Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

STATE OF UTAH COOPERATIVE CONTRACT AMENDMENT

AMENDMENT #: 3

CONTRACT #: AR3109

Starting Date: 7/31/2019

Expiration Date: 9/15/2026

TO BE ATTACHED AND MADE PART OF the specified contract by and between the State of Utah Division of Purchasing and Compulink Management Center, Inc. dba Laserfiche (Referred to as CONTRACTOR).

BOTH PARTIES AGREE TO AMEND THE CONTRACT AS FOLLOWS:

Update to Laserfiche's Privacy Notice, Service Level Agreement, and Data Processing Addendum and added to Attachment E of Master Agreement #AR3109.

Effective Date of Amendment: Upon signatures of both parties.

All other terms and conditions of the contract, including those previously modified, shall remain in full force and effect.

IN WITNESS WHEREOF, the parties sign and cause this contract to be executed.

CONTRACTOR

DocuSigned by:
Wylie Strout
AEC702DEF362467...
Contractor's Signature — Date

Wylie Strout
Contractor's Name (Print)

Chief Legal Officer
Title (Print)

STATE OF UTAH

DocuSigned by:
C38BE9DAC528424...
Director, State of Utah Division of Purchasing — Date: 10/30/2025

For Division of Purchasing Internal Use			
Purchasing Agent	Phone #	E-mail Address	**Contract #**
Keli Lessing	801-957-7167	klessing@utah.gov	AR3109

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

Privacy Notice

NOTICE: This Privacy Notice is effective as of January 10, 2025.

This Privacy Notice ("Notice") describes how Compulink Management Center, Inc. dba Laserfiche, located in the United States, and its various operating subsidiaries located around the world, including Canada and Ireland ("**Laserfiche**", "**we**", "**us**", "**our**") collect, use, disclose, and protect Personal Information and how you can contact us about our privacy practices. This Notice applies to our processing of personal information in connection with the delivery of our website at https://www.laserfiche.com/ (the "**Site**"), and all products and services (including its content and functionality) offered by Laserfiche (collectively, our "**Services**"). We are committed to taking appropriate steps to help protect the privacy of visitors to our Site or users of our Services. "**Personal information**" or "**personal data**" means any information that identifies or relates to a particular individual as more specifically defined under the data protection laws applicable to the particular individual.

Please note, our privacy practices are subject to the applicable laws of the places in which we operate. Thus, in this Privacy Notice, you will see additional legal terms specific to visitors to our Site or users of our Services located in other geographical regions.

Some data protection laws make a distinction between organizations that process personal information for their own purposes (known as "**controllers**" or "**businesses**") and organizations that process personal information on behalf of other organizations (known as "**processors**" or "**service providers**"). Laserfiche may act as either a controller/business or a processor/service provider in respect of your personal information, depending on the circumstances.

Laserfiche is the controller with respect to information you provide through the Site. Laserfiche is located at the address in the section entitled "Contact Us" below.

Sometimes Laserfiche operates as a processor on behalf of its business-to-business clientele (each, a "**Laserfiche client**", "**client**", or "**customer**"). Each Laserfiche client is the data controller over the personal information processed by Laserfiche in connection with the Services provided by Laserfiche to such client and its users. For example, Laserfiche provides cloud services to many of its clients. In doing so, Laserfiche may process personal information stored in Laserfiche Cloud by its clients in order to provide the underlying cloud services. This Notice does not describe the actual processing by each Laserfiche client of such personal data. Please visit the applicable client's privacy policy, privacy notice, or privacy statement on their website ("**privacy notice**") for specific information about such client's privacy practices. Any questions you may have relating to your personal information and rights under applicable data protection law with respect to a Laserfiche client's processing of your personal data should be directed to the Laserfiche client who is the controller of such activity, not to Laserfiche.

Information We Collect

When you visit or use the Site and/or Services, we collect and retain information that you, as a customer or potential customer, provide through the Site or Services, as well as information that is automatically or passively collected from you, your device, or your browser.

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

Laserfiche®

Information You Provide to Us

We collect information that you provide directly to us. For example, when you manage your user profile, participate in interactive features (such as "Contact Us for Your ECM needs", request newsletters or other marketing communications, request customer support, enter login information, or otherwise communicate with us.

The types of information we may collect include:

- Contact and profile information, including your name, email address, company information, postal address (including zip or postal code), and telephone number.
- Account and log-in information, including your username, password, login details, and transaction details.
- Billing information, including your payment instrument number (e.g., credit card or debit card number), expiration date, security code as necessary to process any payments, and transaction details (if applicable).
- Correspondence, for example, reporting a problem or submitting queries, concerns or comments regarding the Site, Services, or their respective content.
- Precise geolocation data, such as latitude/longitude. With your consent, we may get access to precise location technologies on your device (such as GPS or Bluetooth) and collect precise location data. We use precise location data for purposes of labeling where you were when you saved the file to track the file's location.
- Any other content or information you choose to provide, including photos you may upload to the Site or Services.

Information We May Collect Automatically

We automatically collect information about your device and how your device interacts with our Site and the Services for business and commercial purposes. We may use service providers to collect this information. Some examples of information we automatically collect include the following:

- Information about your visits to the Site and use of the Services, the resources you access, any data you download, and information related to the ways in which you interact with the Site or the Services.
- IP addresses, including the general information in such address, such as city, state and zip or postal code, your device's regional settings, unique device identifiers, other information about your mobile phone or other mobile device(s), browser types, and browser language.
- Referral pages and links, URLs, number of clicks, pages viewed, how long you are on a page, your search queries, and results.
- Information about your device, computer and/or browser you use, as well as the device's operating system, such as device hardware model, operating system version, or mobile network information.
- Non-precise location data, including your device's location derived from an IP address or data that indicates a city or zip or postal code.

We use various technologies to collect this information ("**Tracking Technologies**"), as further discussed below under the "Cookies, Other Tracking Technologies, Interest-Based Advertising, And Choices Regarding the Same" heading.

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

Laserfiche®

Information We Collect from Customers

We provide products and services to our customers and collect and process information about individuals (including personal information) (including through Tracking Technologies) at the direction of and on behalf of our customers ("**Customer Data**"). Customer Data has historically included contact data, demographic data, content, service use data, device connectivity and configuration data, and precise and non-precise location data, among other information. Our processing of Customer Data is governed by the terms of our Cloud Subscription Agreement with each customer. To the extent we combine Customer Data with information (including personal information) we have collected about you through the Site, we will treat the combined information in accordance with the practices described in this Notice, plus any additional restrictions imposed by our customers. We are not responsible for how our customers treat the information we collect on their behalf as a processor or service provider. With respect to our customer's use and disclosure of your personal information, we recommend you review the applicable customer's own privacy notice. For more information on your rights and choices regarding your personal information comprised in Customer Data, please see the "Your Privacy Rights" heading below.

Information We Collect From Other Sources

We may obtain information from other third-party sources that we combine with your personal information collected through the Site. These third-party sources vary over time, but include:

- Data brokers from which we purchase demographic data to supplement the data we collect.
- Social networks when you reference our Service or grant permission to Laserfiche to access your data on one or more of these social networks.
- Partners with which we offer co-branded services, sell or distribute our products, or engage in joint marketing activities.
- Publicly available sources, such as open government databases or other data in the public domain.

For example, if you log into a social media website through our Site, we may have access to certain information from that website, in accordance with the procedures and practices of that social media website. You should carefully review the privacy notices and terms of use of these third parties.

Information we Infer

We infer information from other information we collect, including to generate information about your likely preferences or other characteristics.

Sensitive Information

Some of the personal information we collect may be considered sensitive under applicable law. See additional disclosures in your region for details.

How Laserfiche Uses and Discloses the Information We Collect

Use of Information Collected

Laserfiche collects and uses the personal information you provide in connection with our Site and Services for a variety of purposes, in accordance with the practices described in this Notice, which may include:

- **Providing our Services to you:** We use your information to operate and manage our Site and Services, including your registration process and user account.

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

- **Improving and developing our Services and Site:** We may use your information to understand how you use our products, Services, and Site, and how we can improve them, and to obtain insight and analysis. For example, the information collected may assist with customer service improvements and technical improvements to our products.
- **Providing customer and user support:** We may use your information to troubleshoot and diagnose product problems, provide support or technical assistance, investigate security incidents, and to perform services requested by you, such as to respond to your comments, questions, and requests.
- **Sending marketing communications:** Depending on your marketing choices (see the "Your Privacy Rights" heading and the "Cookies, Other Tracking Technologies, Interest-Based Advertising, And Choices Regarding the Same" headings below), we may use your information to keep you informed about Laserfiche and our software and Services and promote certain Services and features that you may be interested in, such as communications about third-party products, updates, special offers, promotions, rewards, and events. We may also contact you for market research and to survey your satisfaction with Laserfiche software and Services, encourage you to participate in our user groups, and invite you to events that may be of interest, including trainings, webinars, and conferences.
- **Sending administrative communications:** We may use your information to send you technical notices, updates, security alerts, information regarding changes to our policies, and other support and administrative messages regarding your account with us.
- **Securing our Services:** We may use your information for maintaining the safety and security of our Services, investigating suspicious activity, detecting, and preventing fraudulent or unauthorized use of the Services, and identifying and troubleshooting any problem.
- **Complying with our legal obligations:** We may process your information in order to cooperate with public and government authorities, courts, or regulators, including to comply with legal orders or judicial proceedings, or to respond to lawful requests and otherwise comply with our legal, regulatory and reporting obligations under applicable laws. Additionally, we may process your information, to protect, defend or exercise our legal rights and to ensure the continuity and integrity of our Services, including where we seek to pursue remedies available to us and or in order to limit damages. We will make reasonable efforts to notify our customers and users of any disclosure of their personal information, unless we are prohibited by law, court order, or exigent circumstances prevent us from doing so.
- **Statistics and analysis:** We may aggregate and/or de-identify your information in such a way as to prevent the information from being reassociated or identified with an account, user, or individual. We may use aggregated and/or de-identified information for a variety of statistical and analytical purposes, which may entail providing this information to an agent acting on Laserfiche's behalf to assist in data analytics.

We also use your personal information for the following purposes:

- Serve personalized advertising tailored to your interests on our Site and/or Service, and third-party Services (where applicable), to the extent it is necessary for our legitimate interest in advertising our Site and Services, or where necessary, to the extent you have provided your prior consent.
- Fulfill any purpose at your direction.
- With your consent, fulfill any other purpose disclosed to you.

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

Laserfiche®

For more information about how we use and disclose your personal information for personalized advertising, please see the "Cookies, Other Tracking Technologies, Interest-Based Advertising, and Choices Regarding the Same" heading below.

We may use publicly available information (as that term is defined by applicable law) or information that does not identify you (including information that has been de-identified or aggregated, as those terms are defined by applicable law), for any purpose without obligation to you except as prohibited by applicable law.

Disclosure of Information Collected

Laserfiche will disclose personal information we have collected about you in accordance with the practices described in this Notice. The types of persons to whom we may disclose your personal information include, but are not limited to, the following:

Disclosing to Service Providers

We will occasionally hire service providers or contract with third-party consultants to provide limited services on our behalf. Laserfiche will only provide those service providers and other third-party consultants your personal information as reasonably needed to deliver services, and, to the extent required by applicable law. Laserfiche service providers and third-party consultants are prohibited from using that information for any other purpose. We may permit these service providers or third-party consultants to use publicly available information (as that term is defined by applicable law) or information that does not identify you (including information that has been de-identified or aggregated, as those terms are defined by applicable law) to the extent permitted by applicable law.

Disclosing to Others

We also disclose personal information about you to the following categories of recipients:

- **Affiliates:** We may disclose your information to our affiliated and related entities including our subsidiaries. For example, we may disclose your information to our affiliates for customer support, marketing, and technical operations.
- **Customers:** We may disclose your information to our customers in connection with us processing your information on their behalf. For example, we may disclose your information to our customers in order to facilitate your orders, maintain and administer your online accounts, respond to your questions and comments, comply with your requests, market, and advertise to you, and otherwise comply with applicable law.
- **Business Partners:** We may disclose your information to our business partners in connection with offering you co-branded services, selling, or distributing our products, or engaging in joint marketing activities. For example, we may disclose information about you to a retailer for purposes of providing you with product support. We may also disclose your information to approved third parties for marketing purposes; this may include our authorized resellers, user group training partners, and cloud solution providers.
- **Promotions:** Our promotions may be jointly sponsored or offered by third parties. If you voluntarily choose to enter a promotion, we may disclose your information to third parties as set forth in the official rules that govern the promotion as well as for administrative purposes and as required by law (e.g., on a winners list). By entering any such promotion, you agree to the official rules that govern that promotion, and may, except where prohibited by applicable law, allow the sponsor and/or other third parties to use your name, voice and/or likeness in advertising or marketing materials.

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

- **User Group, Training, and Events:** Our events may be jointly sponsored or offered by third parties. If you voluntarily sign-up for an event through Laserfiche, we may disclose your contact details or information that you provide to the sponsor, facility, or any other organization who we schedule you to meet with at that event in order to fulfill your event registration and/or inform you of future events organized by the sponsor, which we believe you may be interested in.
- **Tracking Technologies:** Some information about your use of the Site and Services and certain third-party services may be collected using Tracking Technologies across time and Services and used by us and third parties for business and/or commercial purposes such as to associate different devices you use, and deliver relevant ads and/or other content to you on the Site, Services, and certain third-party services, as explained further under the "Cookies, Other Tracking Technologies, Interest-Based Advertising, And Choices Regarding the Same" heading.
- **Third Parties:** We may disclose your information to third parties for the purposes of facilitating your requests (such as when you choose to disclose information with a social network about your activities on the Site or Services) and in connection with tailoring advertisements, measuring, and improving our Service and advertising effectiveness, and enabling other enhancements, subject to your preferences (where applicable).
- **Consent or another lawful purpose:** We may disclose your information for any other lawful purpose and/or with notice to you and with your consent.

We will disclose your personal information to respond to duly authorized requests from governmental authorities as required by law, or in circumstances in which we believe disclosure is necessary or reasonably appropriate to protect the rights, property, or safety of us or others. Please note that Laserfiche is required to disclose personal information in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.

Laserfiche also discloses your personal information when: (a) we are required to do so by law, regulation, warrant, subpoena or court order, (b) we are required in urgent circumstances to protect the personal safety of Laserfiche employees, users of Laserfiche products or services, or members of the public, (c) it is necessary to enforce our Terms of Use, or to exercise, establish or defend our legal rights (including contractual rights), or (d) such disclosure may be part of a sale of all (or substantially all) of the assets of Laserfiche or an affiliated entity where Customer Data might be included among the transferred assets.

Disclosing to third party websites

Some of the hyperlinks on our Site may lead to third-party services that are not controlled by or affiliated with Laserfiche. These links are provided solely as a convenience to you and not as an endorsement by Laserfiche of the content on such third-party services. Third-party services are subject to the terms of use and privacy notices of each applicable third-party entity, including what information they disclose to us, your rights and choices on their services and devices, and whether they store information in the U.S. or elsewhere. For example, Office Online is a Microsoft service and use of Office Online is subject to Microsoft's terms of use and privacy notice. Laserfiche is not responsible for and does not endorse, guarantee or monitor the content, availability, viewpoints, products or services that are offered or expressed through any third-party services and does not make any representations or warranties regarding the content or accuracy of any content on these third-party websites, including third-party privacy policies. We encourage you to familiarize yourself with and consult each applicable third-party entity's terms of use and privacy policies.

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

Laserfiche®

Without limiting the foregoing, in our sole discretion, we may disclose aggregated information which does not identify you or de-identified information (as those terms are defined under applicable law) about you with third parties or affiliates for any legitimate business purpose or with your consent, except as prohibited by applicable law.

How We Respond to Do Not Track Signals

Do-Not-Track ("DNT") is a preference that can be set in your browser to notify websites you visit that you do not want them to collect certain information about you. Laserfiche does not respond to DNT signals at this time and will not do so unless and until the law is interpreted to require such response. As discussed in this Notice, we and third parties may track your visits to our Site or use of our Services for purposes such as to provide Interest-based Advertising. To the extent you have specific rights in your region with respect to certain preference signals, such as Global Privacy Control, please see your region-specific terms for details.

Cookies, Other Tracking Technologies, Interest-Based Advertising, And Choices Regarding the Same

Please see our Cookie Statement for more information about how we use cookies and similar tracking technologies. In addition to the technologies listed in our Cookie Statement, we use the following to collect information:

- **Pixels/Web Beacons:** Pixels or web beacons are code which is embedded in our Site or Services that send information about your use to a server. There are various types of pixels/web beacons, including image pixels (e.g., small graphic images) and JavaScript pixels (e.g., containing JavaScript code). When you access a Service that contains a pixel, the pixel may permit us or a separate entity to drop or read cookies on your browser or collect other information about your visit to our Site or use of our Services. We utilize pixels (some of which are provided by separate entities) that allow us to track our conversions with you, bring you advertising, and provide you with additional functionality with our Site or Services.
- **Device Fingerprinting:** Device fingerprinting is the process of analyzing and combining sets of information elements from your device's browser, such as JavaScript objects and installed fonts, in order to create a "fingerprint" of your device and uniquely identify your device and apps.
- **Precise Geolocation Data**: Precise location data includes latitude and longitude and is used for purposes of labeling where you were when you saved the file to track the file's location. You can stop collection of precise location data through your browser or device settings or by uninstalling the app.

As discussed in our Cookie Statement, we also work with ad serving services, advertisers, and other third parties to serve advertisements on the Site, Services, and/or on third-party services. These third parties may use Tracking Technologies on our Sites, Services, and third-party services (including in emails and advertisements) to track your activities across time and services for purposes of associating the different devices you use and delivering relevant ads and/or other content to you on the Site, Services, and third-party services or third-party devices after you have left the services ("**Interest-based Advertising**"). Some of the third parties that collect information from or about you on the Site or Services in order to provide more relevant advertising to you participate in the Digital Advertising Alliance ("**DAA**") Self-Regulatory Program for Online Behavioral Advertising. This program offers a centralized location where users can make choices about the use of their information for online behavioral advertising. To learn more about the DAA and your opt-out options for their members, please visit (i) for website opt-out, http://www.aboutads.info/choices; and (ii) for mobile app opt-

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

out, http://www.aboutads.info/appchoices. In addition, some of these third parties may be members of the Network Advertising Initiative ("**NAI**"). To learn more about the NAI and your opt-out options for their members, please visit http://www.networkadvertising.org/choices/. Please note that if you opt-out of online behavioral advertising using any of these methods, the opt-out will only apply to the specific browser or device from which you opt-out. Further, opting-out only means that the selected members should no longer deliver certain Interest-based Advertising to you, but does not mean you will no longer receive any targeted content and/or ads (e.g., from other ad networks). We are not responsible for the effectiveness of, or compliance with, any third parties' opt-out options or programs or the accuracy of their statements regarding their programs, content, or services.

Most browsers accept cookies by default. You may instruct your browser, by changing its settings, to decline or delete cookies. If you use multiple browsers on your device, you will need to instruct each browser separately. Your ability to limit cookies is subject to your browser settings and limitations. Please be aware that if you disable or remove Tracking Technologies some parts of the Services may not function correctly.

For further information about the types of Tracking Technologies we use, why, and how you can control such Tracking Technologies, please see our Cookie Statement.

Public Areas (e.g., Bulletin Boards and Chat Rooms

Portions of our Site or Services may allow you to post information that is publicly available to anyone who may have access to that area (e.g., a "bulletin board", "community forum", or interactive "chat room") ("**Public Areas**"). Laserfiche is not responsible for the content users post and share in, or through, Public Areas. If you choose to post information in a Public Area, it becomes available to the public, and Laserfiche has no ability to control or limit the use of information that is available to the public. Laserfiche and its affiliates may utilize any information you post through Public Areas, including in connection with the operation of its business. Laserfiche encourages you not to post any information you consider private or sensitive to, or through, Public Areas. To request removal of your information from Public Areas, please contact us using the contact details provided under the "Contact Us" heading below. In some cases, we may not be able to remove your information, in which case we will let you know if we are unable to and why.

Your Privacy Rights

Your rights

You may have certain rights relating to your personal information, subject to local data protection laws. Depending on the applicable laws these rights may include the right to:

- Access or receive a copy of your personal information held by us;
- Know more about how we process your personal information;
- Rectify inaccurate personal information and, taking into account the purpose of processing the personal information, ensure it is complete;
- Erase or delete your personal information (or right to be forgotten);
- Right to data portability;

Restrict our processing of your personal information. In some jurisdictions, this right is available where one of the following applies: (a) the accuracy of the personal information is contested, (b) the processing is unlawful, and you oppose the erasure of the personal information and request the restriction of its use instead, (c) Laserfiche no longer needs the personal information for the purposes of

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

processing but is required to keep it for the establishment, exercise, or defense of legal claims, or (d) if you have objected to our processing of your personal information and we are verifying whether you have legitimate ground for such objection;

- Transfer your personal information to another controller or business, to the extent possible;
- Object to any processing of your personal information;
- Complain about our processing of your personal information, including to a data protection authority;
- Opt-out of certain disclosures of your personal information to third parties;
- Know what categories of personal information are shared for delivering advertisements on non-Laserfiche websites, applications, and services and the categories of recipients of such personal information;
- Opt-out of the sharing of your personal information for delivering advertisements on non-Laserfiche websites, applications, and services;
-
- Withdraw your consent at any time (to the extent we base processing on consent), without affecting the lawfulness of the processing based on such consent before its withdrawal;
- Where we are processing your personal information on the basis of your consent or pursuant to the performance of a contract with you and such processing is carried out by automated means, you may request to receive your personal information in a commonly used, machine readable format (or have that information transmitted to a third party where technically feasible); and
- Not be discriminated against for exercising your rights as described above.

Where we process your personal information for direct marketing purposes or share it with third parties for their own direct marketing purposes, you can exercise your right to object at any time to such processing without having to provide any specific reason for such objection.

You may also have additional rights based upon your jurisdiction.

How to exercise your rights

To exercise your rights, as may be applicable for your jurisdiction, please contact us by using our online form available here. Your personal information may be processed in responding to these rights. In the request, please specify which right you are seeking to exercise and the scope of the request. We will confirm receipt of your request within 10 business days and try to respond to your request within 45 days. We may require specific information from you to help us verify your identity and process your request. If you are an employee of a Laserfiche client, we recommend you contact your employer's system administrator for assistance in correcting or updating your information.

Your rights relating to Laserfiche Cloud "Customer Data"

As described above, we may also process personal information included in Laserfiche Cloud "Customer Data" which is uploaded by a Laserfiche client in which case, we process such personal information as a processor on behalf of our client (and its affiliates) who is the controller of the personal information. If your personal information has been submitted to us in our role as a processor by or on behalf of a Laserfiche client and you wish to exercise any rights you may have under applicable data protection laws, please inquire with the applicable Laserfiche client directly. Because we may only access a client's data upon their instructions, if you wish to make your request directly to us, please provide us the name of the Laserfiche client who submitted your personal information to us. We will refer your request to that client, and will reasonably support them as needed in responding to your request.

Marketing Communications

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

- If you supply Laserfiche with your postal address online, you may receive periodic mailings from us with information on new products and Services, or upcoming events.
- If you supply us with your telephone number online, you may receive telephone calls from us with information regarding orders and/or requests you have placed online – such as a software demonstration request or general business inquiry.
- If you supply us with your email address, then in accordance with your marketing choices, you may receive email messages for marketing purposes, such as providing information on new products and Services, or upcoming events. We may track when you open our email messages or click on the links contained within them.

You have the right to opt-out of marketing communications from us at any time. You can exercise this right by clicking on the "unsubscribe" or "opt-out" link in the marketing emails we send you, or by emailing us at the email address set forth in the section entitled "Contact Us" below with the word UNSUBSCRIBE in the subject field of your email. Please note this opt-out will not apply to non-promotional emails, such as those about your account, transactions, servicing, or Laserfiche's ongoing business relations.

You can also opt out of receiving calls to your phone number at any time by requesting to opt-out during any call you receive from us or contacting us as set out in the "Contact Us" heading below and specifying you would like to opt-out of calls.

To opt-out of other forms of marketing (such as postal marketing or telemarketing), please contact us using the contact details under the "Contact Us" heading below.

Please note that by opting in to allow Laserfiche and its event sponsors/industry partners to receive your contact information through an event in accordance with this Notice, you will be subject to each event sponsor/industry partner's communications and privacy notice and must opt-out with them directly.

Security Measures

We have implemented and maintain reasonable industry standard controls, intrusion detection network monitoring, and reasonable security measures designed to protect the personal information that you submit through the Services and Site (subject to our disclosure regarding Public Areas). These measures include physical access controls, access authorization controls, and firewalls. We also periodically review our information collection, storage, and processing practices to help prevent loss, misuse, unauthorized access, alteration, or other destruction of personal information we collect. When accessing secure sections of the Site, we use Transport Layer Security (TLS) encryption to secure the communication of personal information passing between your browser and our servers. Additionally, only authorized administrators, Laserfiche employees and third-party contractors have access to systems containing personal information.

Although we take reasonable security measures to protect your personal information, we cannot guarantee the security of your personal information transmitted to the Site. The transmission of information via the internet is never 100% secure, and we cannot ensure or warrant the security of any information (including personal information) you transmit to us. We are not responsible for circumvention of any privacy settings or security measures contained on the Site.

The safety and security of your information (including personal information) also depends on you. Where we have given you (or where you have chosen) a password for access to certain parts of the Site,

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

products, or Services, you are responsible for keeping this password confidential. Please do not share your password with anyone.

International Data Transfers

Laserfiche is headquartered in the United States. Data centers for Laserfiche Cloud Services are located in the United States, Canada, and Ireland, respectively. Operationally, we have on-premises computer facilities in the United States, Canada, Hong Kong and other regions. Our affiliated subsidiaries, third-party service providers, and partners operate around the world. This means that when we collect your personal information, we may process it in any of these jurisdictions. The laws governing our processing of personal information in such jurisdictions may differ from those in the jurisdictions in which you are located. Regardless of where your personal information is processed, we will treat all personal information in accordance with applicable data protection laws and this Notice.

If you are located in the EEA, United Kingdom or Switzerland, we will protect your personal information when it is transferred outside of such locations by processing it in a country that provides an adequate level of protection (click here for a list of countries deemed adequate by the European Commission) or by implementing appropriate safeguards to protect your personal information, including through the use of standard contractual clauses or another lawful transfer mechanisms approved by the European Commission and/or the United Kingdom or Swiss authorities (as applicable). For more information about the lawful transfer mechanisms we rely on, please contact us using the contact details under "**How to Contact Us**" within the "European Economic Area, Switzerland, and United Kingdom" section below.

Laserfiche complies with the EU-U.S. Data Privacy Framework ("**EU-U.S. DPF**"), the UK Extension to the EU-U.S. DPF ("**UK Data Bridge**"), and the Swiss-U.S. Data Privacy Framework ("**Swiss-U.S. DPF**") as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal data transferred from the European Union and Switzerland to the United States. Laserfiche has certified to the U.S. Department of Commerce that it adheres to the EU-U.S. Data Privacy Framework Principles (the "**Principles**") with regard to the processing of personal data received from the European Union in reliance on the EU-U.S. DPF, from the United Kingdom (and Gibraltar) in reliance on the UK Data Bridge, and from Switzerland in reliance on the Swiss-U.S. DPF. If there is any conflict between the terms in this Notice and the Principles, the Principles shall govern personal data processed in reliance of the Data Privacy Framework ("**DPF**"). To learn more about the DPF, and to view our certification, please visit https://www.dataprivacyframework.gov/s/participant-search.

Laserfiche's responsibility for personal data it receives in reliance on the DPF and subsequent transfers of that personal data to third parties is detailed in the Principles. Where Laserfiche relies on the Principles for onward transfers from the EU, UK and Switzerland, including the onward transfer liability provisions, Laserfiche remains responsible under the Principles for third-party agents processing personal data on its behalf.

With respect to personal data received or transferred pursuant to the DPF, we are subject to the regulatory enforcement powers of the U.S. Federal Trade Commission. In certain situations, we may be required to disclose personal data in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.

Laserfiche commits to resolving complaints about your privacy and our collection and use of your personal data in reliance on the DPF within 45 days of receiving your complaint. Individuals with

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

questions or complaints regarding this Notice should first submit inquiries by contacting us using the contact details provided under the "Contact Us" heading below. Laserfiche has further committed to refer unresolved complaints regarding personal data transferred in reliance on the DPF to the American Arbitration Association, an alternative dispute resolution provider located in the United States. If you do not receive timely acknowledgment of your complaint from us, or if we have not resolved your complaint, please contact, or visit the American Arbitration Association for more information or to file a complaint. When filing by mail or email, please complete the appropriate DPF Notice of Arbitration Form located in the link below and forward to the International Centre for Dispute Resolution.
International Centre for Dispute Resolution Case Filing Services
1101 Laurel Oak Road, Suite 100
Voorhees, NJ 08043
United States
Phone: +1.212.484.4181
Email box: casefiling@adr.org

For any questions or for further information about this program, the ICDR's International Arbitration Rules, or for additional language versions of the ICDR's International Arbitration Rules, please contact the International Centre for Dispute Resolution at +1.212.484.4181 or by visiting the website https://www.icdr.org/dpf. The services of the American Arbitration Association are provided at no cost to you.

Under certain limited circumstances, data subjects, as defined by the Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016, of the European Union, may invoke binding arbitration as a last resort if all other forms of dispute resolution have been unsuccessful. To learn more about this method of resolution and its availability to you, please visit https://www.dataprivacyframework.gov/s/.

Privacy of Children
The Site and Services are intended for a general audience and not directed to children under sixteen (16) years of age. We do not market products or services to children, and we do not knowingly collect personal information from children at any time, including as defined by the U.S. Children's Privacy Protection Act ("**COPPA**").

If you are under the age of 16, please do not provide personal information of any kind whatsoever and please do not use the Site or Services or participate in Laserfiche's surveys, contests, events, and other promotions. If you are a parent or guardian and believe Laserfiche has collected such information without parental consent, please contact us as set below in the section entitled "Contact Us" and we will remove personal information to the extent required by COPPA or other applicable law.

Data Retention
We retain personal information we collect from you where we have an ongoing legitimate business need to do so. For example, to provide you with a service you have requested or to comply with applicable legal, tax or accounting requirements.

California Privacy Rights

Notice at Collection

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

Laserfiche®

The California Consumer Privacy Act ("**CCPA**") as amended by the California Privacy Rights Act ("**CPRA**") and implementing regulations (collectively referred to as "**CCPA**") requires that we detail the categories of personal information that we disclose for certain "business purposes," such as to service providers that assist us with securing our services or marketing our products, and to such other entities as described under the "How Laserfiche Uses and Discloses the Information We Collect" heading above in this Notice

- **Collection.** We have collected the following categories of personal information (as that term is defined in the CCPA) in the past 12 months:
    - Identifiers, including your name, postal address, email address, and online identifiers (such as IP address).
    - Consumer records, including your phone number, billing address, and credit or debit card information.
    - Characteristics of protected classifications under California and/or federal law, including your gender.
    - Commercial or transactions information, including records of products or services purchased, obtained, or considered.
    - Internet activity, including browsing your history, search history, and interactions with a website, email, application, or advertisement.
    - Non-precise geolocation data, including your location derived from an IP address.
    - Precise location data
    - Professional, employment or education-related information.
    - Inferences drawn from any of the information identified in this section.

- **Disclosure.** For more details about the personal information Laserfiche collects from you and the sources from which we obtain personal information, please review the section entitled "How Laserfiche Uses and Discloses the Information We Collect" above.
- **Purpose.** We collect, use, and disclose this personal information for the business and commercial purposes set out in the section entitled "How Laserfiche Uses and Discloses the Information We Collect" above. Please see this section above for more details.
- **Sales and Shares.** Laserfiche does not sell personal information as the term "sell" is traditionally understood. However, some of our disclosures of your personal information may be considered a "sale" or a "share" as those terms are defined by the CCPA. A "sale" is broadly defined under the CPRA to include a disclosure for something of value, and a "share" is broadly defined under the CPRA to include a disclosure for cross-context behavioral advertising. We collect, sell, or share the following categories of personal information for commercial purposes: identifiers, characteristics, commercial or transactions information, internet activity, non-precise geolocation data, and inferences drawn. The categories of third parties to whom we sell or share your personal information include, where applicable, vendors and other parties involved in cross-context behavioral advertising. For details about your rights regarding sales and shares, please see the "Do Not Sell or Share My Personal Information " section below. Laserfiche does not knowingly sell or share the personal information of minors under 16 years old who are California residents.

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

- **Sensitive Personal Information.** Some of the personal information we collect may be considered sensitive personal information (as described in the CCPA). For further details of the sensitive personal information we collect (if any) and how we obtain this information, please review the section entitled "Information We Collect" above. We collect, use, and disclose sensitive personal information only for the permissible business purposes for sensitive personal information under the CCPA or without the purpose of inferring characteristics about consumers. Further, we do not "sell" or "share" your sensitive personal information as those terms are defined by the CCPA.
- **Data Retention.** We retain each category of personal information, including sensitive personal information, for the length of time that is reasonably necessary for the purpose for which it was collected, and as necessary to comply with our legal obligations, resolve disputes, prevent fraud, and enforce our agreements.

Privacy Rights

- **Right to Know, Correct, and Delete.**
  - **Know.** You have the right to know certain details about our data practices. In particular, you may request the following from us:
    - The categories of personal information we have collected about you.
    - The categories of sources from which the personal information was collected.
    - The categories of personal information about you that we disclosed for a business purpose or sold or shared.
    - The categories of third parties to whom the personal information was disclosed for a business purpose or sold or shared.
    - The business or commercial purpose for collecting or selling or sharing the personal information.
    - The specific pieces of personal information we have collected about you.
  - **Correct**. You have the right to correct inaccurate personal information we maintain about you.
  - **Delete.** You have the right to delete personal information that we have collected about you.

- These rights are subject to certain exceptions and also apply to sensitive personal information. To exercise any of these rights, California consumers should submit a request through our online form available here or call our toll free number at 800-985-8533.

- **Do Not Sell or Share My Personal Information.** To the extent that using third party cookies and other tracking technologies to serve retargeted or interest-based advertising constitutes a "sale" or "share" of personal information under the CCPA, you may opt-out of such "sales" or "shares" by clicking here to manage your technology preferences or by turning on a recognized opt-out preference signal in your browser or extension such as **Global Privacy Control**. When you submit an opt-out through any method, the opt-out will only apply to sales and shares from the specific browser from which you sent the signal because the connection between your browser identifier and other personal information we have about you is not known to us. If you delete or reset your cookies, or use a different browser or device, you will need to reconfigure your settings. If you want the opt-out to apply to information we have about you in our systems, such

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

as your email address, please also submit a request through our form **here** (specifying the right you wish to exercise).

- **Shine The Light Customer Rights**
  Consumers in the State of California may request a list of categorized third parties and in some cases affiliates to whom we may have disclosed their personal information specifically for those third parties' and/or affiliates' own marketing purposes, as well as the type of personal information disclosed to those parties. If you are a California resident and would like to request this information, please submit a written request to the email or address provided in the section entitled "Contact Us" above. Requests must include "**California Privacy Rights Request**" in the first line of the description and include your name, street address, city, state, and ZIP code. Please note that any response to requests made by means other than through the provided e-mail address or mail address may be seriously delayed.

Exercising Your Privacy Rights (California).
To exercise any rights available under California law regarding your personal information for which Laserfiche is the business, you should submit a request through our online form available here or call our toll free number at 800-985-8533. In the request, please specify which right you are seeking to exercise and the scope of the request. Any requests with respect to personal information for which Laserfiche is a service provider, should be directed to the applicable Laserfiche client that is the applicable business and controller.

Authorized Agent
You may also designate an authorized agent to submit such requests on your behalf. Requests must be submitted through the designated methods listed above. Except for opt-out requests, we will require written proof of the agent's permission to do so and may verify your identity directly.

Additional U.S. States Privacy Rights

Data Practices

This section applies to residents of certain U.S. states which also have an applicable data privacy law currently in effect. Information regarding the collection, use, disclosure, and retention of your personal information are set out above in this Notice.

Some of our disclosures of personal data may be considered a "sale" under applicable law, which is often defined to include a disclosure for something of value. We also may process your personal data for purposes of targeted advertising. We do not process personal data for purposes of profiling in furtherance of decisions that produce legal or similarly significant effects concerning consumers.

Some of the personal data we collect may be considered sensitive personal data under applicable law. We collect sensitive personal data with your consent.

Sales and Targeted Advertising

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

To the extent that using third party cookies and other tracking technologies to serve retargeted or interest-based advertising constitutes a "sale" under certain applicable US state data privacy laws, you have the right to opt-out of us "selling" your personal data or processing your personal data for purposes of targeted advertising. To exercise this right, please submit a request through our online form available here or turn on a recognized opt-out preference signal, such as Global Privacy Control. When you submit an opt-out, the opt-out will only apply to the specific browser from which you sent the signal because the connection between your browser identifier and other personal information we have about you is not known to us. If you want the opt-out to apply to personal information we have about you in our systems, such as your email address, please also submit a request through our form **here** (specifying the right you wish to exercise).

Consent

You have the right to revoke consent previously given to us for the processing of your personal data. To revoke consent, write us at the email or postal address set out in the **Contact Us** section below (specifying the consent you wish to withdraw). If you withdraw consent, you may not be able to receive certain Services related to that consent.

Exercising Your Privacy Rights (US States other than California)

To exercise any rights available under the applicable U.S. state law regarding your personal information for which Laserfiche is the controller, please submit a request through our online form available here. In the request, please specify which right you are seeking to exercise and the scope of the request. Any requests with respect to personal information for which Laserfiche is a service provider, should be directed to the applicable customer that is the controller.

Authorized Agents

You can designate an authorized agent to submit requests on your behalf. Requests must be submitted through the designated methods listed above. Except for opt-out requests, we will require written proof of the agent's permission to do so and may verify your identity directly.

Right to Appeal

If we refuse to take action on your request, you may appeal our decision within a reasonable period of time by contacting us at privacy@laserfiche.com and specifying you wish to appeal. Within 60 days of our receipt of your appeal, we will inform you in writing of any action taken or not taken in response to the appeal, including a written explanation of the reasons for the decisions. If the appeal is denied, you may submit a complaint to your state's attorney general office.

European Economic Area, Switzerland, and United Kingdom

For the purpose of this Notice, "Europe" means the European Economic Area ("**EEA**"), Switzerland, and the United Kingdom.

Legal basis for processing personal information

Our legal bases for processing your personal information include: (a) you have given consent to the processing for one or more specific purposes; (b) processing is necessary for the performance of a contract with you; (c) processing is necessary for compliance with a legal obligation, for example when providing personal information to a law enforcement agency or where we have an accounting or tax

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

obligation; or (d) processing is necessary for the purposes of the legitimate interests pursued by us or a third party, and your interests and fundamental rights and freedoms do not override those interests.

If you are a visitor from Europe, our legal basis for collecting and using the personal information described above will depend on the personal information concerned and the specific context in which we collect it.

In rare situations, we may also need to share your personal information with others to protect your vital interests or those of another person.

If we ask you to provide personal information to comply with a legal requirement or to perform a contract with you, we will make this clear at the relevant time and advise you whether the provision of your personal information is mandatory or not (as well as of the possible consequences if you do not provide your personal information).
Similarly, if we collect and use your personal information in reliance on our legitimate interests (or those of any third party), we will make clear to you at the relevant time what those legitimate interests are.

Please see the "**How Laserfiche Uses and Discloses the Information We Collect**" in this Notice for more details about the purposes for which we process your personal information. More information about the legal basis on which we rely in connection with each of our processing purposes, is set out below.

Purpose and legal basis for processing

Providing our Services to you

- Necessary for our legitimate interests (successful management of our customer and user relationship, and fulfillment of our contractual or other obligations to you).

Improving and developing our Services

- Necessary for our legitimate interests (to improve and develop our Services in order to deliver high quality Services to customers and users, and to ensure the security and efficiency of our Services).

Providing customer and user support

- Necessary for our legitimate interests (successful management of our customer and user relationship, and to promote our business through the delivery of quality Services).

Sending marketing communications

- With your consent, where legally required.
- Necessary for our legitimate interests (promotion of our business and Services to customers and users).

Sending administrative communications

- Necessary for our legitimate interests (continuance of a successful customer and user relationship and to provide quality Services).

Securing our Services

- Necessary for our legitimate interests (providing secure Services, ensuring the security of our networks and systems, and creating trust in our Services).

Complying with our legal obligations

- Necessary for compliance with a legal obligation (such as pursuant to a contract).
- Necessary for our legitimate interests (complying with legal obligations, regulatory, contractual, or other obligations).

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

Laserfiche®

Your European Privacy Rights
Depending on your location and how you interact with Laserfiche, you may have the rights listed under the "Your Privacy Rights" heading above in this Notice subject to applicable data privacy law.

Laserfiche is committed to cooperating and complying with European data protection authorities' advice with respect to any human resources data transferred from Europe in the context of the employment relationship.

Data Retention
We will retain your personal information for only so long as we need it in order to fulfil our processing purposes or where we otherwise need to retain it to comply with our legal obligations. The criteria we use to determine retention periods include the nature of the data, the purpose of processing, and terms of any relevant legal requirements. We regularly review our data retention periods to ensure that we are not keeping personal data longer than necessary.
When we have no ongoing legitimate business need or legal reason to process your personal information, we will either delete or anonymize it or, if this is not possible (for example, because your personal information has been stored in backup archives), then we will securely store your personal information and isolate it from any further processing until deletion is possible.

Exercising Your Privacy Rights (Europe)
To exercise any rights under the applicable laws of Europe with respect to your personal information for which Laserfiche is a controller, please submit a request by filling out this form or contact us as set out in the "How to Contact Us" section below and specify which right you are seeking to exercise. Any requests with respect to personal information for which Laserfiche is a processor, should be directed to the applicable customer that is the controller.

How to Contact Us
If you have any concerns or questions about the information provided in this "European Economic Area, Switzerland, and United Kingdom" section, please do not hesitate to get in touch with us using the following details:
By mail:
Compulink Management Center, Inc. d/b/a Laserfiche
ATTN: Data Protection Officer
3443 Long Beach Blvd.
Long Beach, CA 90807
USA
By email: privacy@laserfiche.com
Data Protection Officer: privacy@laserfiche.com
We are committed to working with you to obtain a resolution of any concern about our privacy practices. If, however, you believe that we have not been able to assist with your concern, you have the right to lodge a complaint with a European data protection authority.

If you are a resident of the European Economic Area, please contact our EU Representative:
By mail:
Laserfiche Ireland Limited

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

Laserfiche®

ATTN: Data Protection Officer
D02 R296
Dublin
Ireland
By email: privacy@laserfiche.com

If you are a resident of the UK, please contact our UK Representative:
By mail:
Laserfiche UK Services Ltd
ATTN: Data Protection Officer
Unit 15B Building 6,
Watford
WD18 8YH
UK
By email: privacy@laserfiche.com

Additional International Jurisdictions

Canada
Laserfiche is committed to collecting, using, and disclosing personal data responsibly in accordance with applicable Canadian privacy regulations, including the Personal Information Protection and Electronic Documents Act (PIPEDA). We collect this information from you, through your interaction with the Laserfiche Site and/or Services, or from third parties. For more information about the personal information we collect, click here. We collect this information for the business and commercial purposes described in the "How Laserfiche Uses and Discloses the Information We Collect" section above.
You have the right to revoke consent previously given to us for the processing of your personal data. To revoke consent, write us at the email or postal address set out in the Contact Us section below (specifying the consent you wish to withdraw). If you withdraw consent, you may not be able to receive certain services related to that consent.

Hong Kong Laserfiche is committed to collecting, using, and disclosing personal information responsibly in accordance with applicable Hong Kong privacy regulations, including the Personal Data Privacy Ordinance. This section applies if the data controller of your personal data is Laserfiche International Limited, which is established in Hong Kong. We collect this information from you, through your interaction with the Laserfiche Site and/or Services, or from third parties. For more information about the personal information we collect, click here. We collect this information for the business and commercial purposes described in the "How Laserfiche Uses and Discloses the Information We Collect" section above. For information about the types of personal information we may collect, please refer to the section "Information We Collect" above. If you are a Hong Kong resident and have questions or wish to exercise your privacy rights, please refer to the Contact Us section of this Notice.

Privacy Notice Changes
Laserfiche may change this Notice from time to time, at Laserfiche's sole discretion. When we update our Notice, we take appropriate measures to inform you, consistent with the significance of the changes we make. If the changes are material, we will notify you or offer you a choice if and to the extent this is required by applicable data protection laws. You can see when this Notice was last updated by checking

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

the “effective” date displayed at the top of this Notice. Laserfiche recommends that you review this Notice regularly for any revisions. Your continued use of the Site or Services after such revisions will constitute your acknowledgement of the amended Notice.

Contact Us

If you have any concerns or questions about the information provided in this Notice, or want to exercise your data protection rights, please contact us using the following details:

By mail:

Compulink Management Center, Inc. d/b/a Laserfiche
ATTN: Data Protection Officer
3443 Long Beach Blvd.
Long Beach, CA 90807
USA

By email: privacy@laserfiche.com

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

Laserfiche®

SERVICE LEVEL AGREEMENT

Your use of the Laserfiche Cloud is subject to and governed by the Cloud Subscription Agreement available here (the "Agreement") and the following Service Level Agreement ("SLA"). This SLA forms a binding agreement between Laserfiche and Subscriber.

1. LASERFICHE CLOUD SERVICE COMMITMENT

During the Service Period of the Agreement, Laserfiche will use commercially reasonable efforts based on industry standards, to make Laserfiche Cloud available subject to the limitations set forth in this SLA. Excluding periods of unavailability described in Section 6(C) below, Laserfiche guarantees that the Laserfiche Cloud will be available 99.9% of the time each calendar month ("Uptime Commitment"). Laserfiche measures Uptime by tracking the availability of certain Laserfiche Cloud systems components. Subscriber may view the status of these components at any time by visiting status.laserfiche.com. "Uptime" means the availability of the Laserfiche Cloud functionality measured over a calendar month notwithstanding the limitations listed in Section 6(A) and 6(B), but excluding periods of unavailability described in Section 6(C), of this SLA.

2. REMEDIES FOR CLOUD SERVICE FAILURE

If Laserfiche Cloud does not achieve the Uptime Commitment described in paragraph 1 ("Failure"), Subscriber may be eligible for a Service Credit. A "Service Credit" is a credit equivalent to the percent of a Subscriber's corresponding monthly Subscription Fees (1/12th of a Subscriber's annual Subscription Fee) for Laserfiche Cloud correlating to Uptime percentage in the following chart:

Uptime Percentage	Service Credit Percentage
Less than 99.9% but more than or equal to 99.5%	10%
Less than 99.5% but more than or equal to 99.0%	20%
Less than 99.0%	30%

Once awarded, a Service Credit will appear on a Subscriber's next month's invoice. Subscriber will have the right to terminate the Agreement if Laserfiche Cloud's Uptime in two or more consecutive months within a calendar year is lower than 85% in each of such months.

3. SERVICE CREDIT REQUEST PROCEDURE

To qualify for a Service Credit:

1. The request must be received by Laserfiche within 15 days of the end of the month for which a credit is sought.
2. Subscriber's account must be in good standing with all invoices paid and up to date.

To receive a Service Credit, Subscriber must submit a claim by emailing orders@laserfiche.com with the following information:

1. "SLA Credit Request" in the subject line;

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

2. Subscriber's name, account ID, administrator's email address and phone number;
3. The date(s) and time(s) of each qualifying incident you are claiming; and
4. Evidence that documents the errors and corroborates your claimed outage (confidential or sensitive information in these logs should be removed and replaced with asterisks).

Failure to provide all the requested information as required will disqualify the Service Credit claim.

4. **ERROR CORRECTION AND RESPONSE TIME FOR CLOUD CLIENT COMPONENTS**

This SLA also covers Error correction support for Cloud Client Components. "Error" means failure of Software to materially conform to its documentation, but excluding any nonconformity resulting from Subscriber's misuse, improper use, or unauthorized change of any Software; or the combining of Software with software not supplied or identified as compatible by Laserfiche. Errors are classified in Table A. Upon identification of an Error, Subscriber will notify their Solution Provider or Laserfiche and provide sufficient information to locate and reproduce the Error. Laserfiche will work with Subscriber's Solution Provider and/or Subscriber to determine the classification of such Error. No Service Credits are awarded in connection with Error corrections. Laserfiche will use all reasonable commercial efforts to attempt to resolve any Errors according to support level within the target times specified in Table A, but failure to meet target times will not constitute a failure to perform a material provision of this SLA. With respect to Subscribers who have Solution Providers, response times below begin upon the Solution Provider's notification to Laserfiche with sufficient information of the Error and are dependent on Solution Provider's continuing collaboration with Laserfiche to resolve the Error.

Table A. Error Classification and Response/Communication Targets

Severity Level	***Definition***	***Initial Response Goals*****	***Updates***
Urgent	Laserfiche Cloud is not operational for all subscribers.	Within 1 business hour	Subscriber will be updated 2x daily on progress via the Status Page at https://status.laserfiche.com/.
Critical	Software functionality is severely impaired even though it is operational at some level affecting multiple subscribers.	Within 4 business hours	Subscriber will be updated daily on progress via the Status Page at https://status.laserfiche.com/
High	A major function in the software is not operational and no acceptable work-around is available, but Subscriber is able to do some production work even though performance and user quality is affected.	Within 8 business hours	Subscriber will be updated weekly on progress via the Status Page at https://status.laserfiche.com/
Medium	There is a loss of a function or resource in software that does not seriously affect Subscriber's operations or schedules.	Within 10 business days	Subscriber will be updated weekly on progress via the Status Page at https://status.laserfiche.com/
Low	All other issues with software.	As needed	Subscriber will be updated as needed

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

Enhancement	New features and functionality not currently existing will be reviewed by Laserfiche's development team and included in future releases if approved.	As needed	Subscriber will be updated as needed

**** Business hours as set forth in the following section.**

5. **ENGINEERING SUPPORT**

Laserfiche will maintain support engineers monitoring Laserfiche's network operations during (1) U.S. PST business hours (except holidays) for the U.S. and Canadian Data Center Regions and (2) GMT business hours (except holidays), for the EU Data Center Region.

6. **LIMITATIONS**

A. The minimum period of Failure eligible for a Service Credit is 10 minutes, and shorter periods will not be aggregated. In the event that multiple periods of Failure overlap in time, Service Credits will not be aggregated, and Subscriber will receive Service Credits only for the longest period of Failure. Laserfiche is not required to issue multiple Service Credits for a single incident.

B. Credits available pursuant to this SLA apply only to future Laserfiche Cloud delivery. Service Credits will not entitle Subscriber to any refunds and are not transferable or assignable. If Subscriber retains a credit balance on termination of the account in question, such credit is forfeited. Notwithstanding the foregoing, credits will not be applied against fees for professional services, bundled support, or setup fees.

C. Notwithstanding any provision to the contrary in this SLA, the following do not constitute Failures: (1) downtime during scheduled maintenance or Emergency Maintenance (as defined below) periods; (2) outages caused by acts or omissions of Subscriber, including its applications, operating system(s), equipment, or facilities, or by any use or user of Laserfiche Cloud authorized by Subscriber, or by Subscriber's use of any other software in its operating system(s); (3) outages caused by hackers, sabotage, viruses, worms, or other third-party wrongful actions; (4) DNS issues outside Laserfiche's control; (5) outages resulting from Internet anomalies; (6) outages resulting from Force Majeure events; and (7) failures during a "beta" period. "Emergency Maintenance" refers to any corrective action intended to remedy conditions likely to cause severe Laserfiche Cloud degradation, as designated by Laserfiche in its sole discretion. Laserfiche will exercise reasonable efforts to inform Subscriber in advance before interrupting Laserfiche Cloud for Emergency Maintenance, but such notice is not guaranteed and failure thereof does not constitute Failure.

D. This SLA does not cover (without limitation): (a) network performance to Subscriber's physical location or Internet access point (such as a local DSL/cable modem) or (b) failures due to denial of service attacks. This SLA does not apply to any feature Laserfiche identifies as "beta" or to any software components made available with Laserfiche Cloud that run outside of the Laserfiche Cloud online service (such as Client Components installed on-premises). IA tools and IA derivatives are excluded from this SLA and are provided "as is" and "as available".

E. Limitations & Warranty Disclaimer. The remedies set forth in this SLA are Subscriber's sole and exclusive remedies for any Failure or other loss of functionality of Laserfiche Cloud, or any Error with the Software, including without limitation for any breach of warranty, except as specifically set forth in the Agreement. The determination of any Failure or categorization of any Error is ultimately in the sole discretion of Laserfiche.

7. **TERMS OF SERVICE/THE AGREEMENT**

Terms defined in the Agreement will have the same meaning when used in this SLA. In the event of any conflict between this SLA and the Agreement, the Agreement will govern.

* * * * *

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

Laserfiche®

Laserfiche Data Processing Addendum

Effective Date: October 15, 2025

This Data Processing Addendum, including its Annexes and the Standard Contractual Clauses (collectively, the "**DPA**" or the "**Addendum**") sets forth the parties obligations with respect to the Processing of Personal Data in connection with Laserfiche's provision of Laserfiche cloud services subscribed by you ("**Cloud Services**") in accordance with the Laserfiche Cloud Subscription Agreement or other agreement under which Laserfiche provides the Cloud Services to you (the "**Laserfiche Cloud Subscription Agreement**" or "**Agreement**") between the party identified as "you" or "Subscriber" in the Agreement and Laserfiche. The term "Laserfiche" and any other capitalized terms utilized in this DPA, but not defined herein, have their respective meanings as set forth in the Laserfiche Cloud Subscription Agreement.

This DPA is incorporated into and forms part of the terms and conditions of the Agreement and will remain in force for the duration of the Subscription Term of the Cloud Services.

By entering into the Agreement, you enter into this DPA on behalf of yourself and, to the extent required under Applicable Data Protection Law, in the name and on behalf of your Permitted Affiliates. For the purposes of this DPA only, and except where indicated otherwise, the terms "you" and "Subscriber" shall include you, Subscriber and such Permitted Affiliates.

1. Definitions

1.1 "**Applicable Data Protection Law**" means all data protection and privacy laws and regulations applicable to the Personal Data in question, including, where applicable, (i) European Data Protection Law and the Swiss DPA, (ii) PIPEDA and any applicable provincial law declared substantially similar to PIPEDA, and (iii) applicable federal and state privacy laws of the United States, including the CCPA and any other similar laws that are in effect or that become effective on or after the Effective Date of this DPA.

1.2 "**CCPA**" means Title 1.81.5. California Consumer Privacy Act of 2018 (California Civil Code §§ 1798.100–1798.199) and its implementing regulations, as amended, superseded or replaced.

1.3 "**Data Privacy Framework**" means (as applicable) the EU-U.S. Data Privacy Framework, the Swiss-U.S. Data Privacy Framework and the UK Extension to the EU-U.S. Data Privacy Framework self-certification programs operated by the U.S. Department of Commerce, and their respective successors.

1.4 "**Data Privacy Framework Principles**" means the Principles and Supplemental Principles contained in the relevant Data Privacy Framework, as amended, superseded or replaced.

1.5 "**Data Subject**" means a data subject, consumer, or identified or identifiable natural person.

1.6 "**European Data Protection Law**" means (i) Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation or "**EU GDPR**"); (ii) the EU GDPR as saved into United Kingdom law by virtue of section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 (the "**UK GDPR**"); (iii) Directive

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector; and (iv) any and all applicable national data protection laws made under, pursuant to or that apply in conjunction with any of (i), (ii) or (iii); (in each case, as may be amended, superseded or replaced from time to time).

1.7 "**Laserfiche Affiliate**" means the subsidiaries of Compulink Management Center, Inc. that may assist in the performance of the Cloud Services in accordance with this DPA.

1.8 "**Permitted Affiliate**" means any Affiliate of Subscriber which: (i) is subject to Applicable Data Protection Law; and (ii) is permitted to use the Cloud Services pursuant to the Agreement, but has not signed its own Agreement with Laserfiche and is not a "Subscriber" as defined under the Agreement.

1.9 "**Personal Data**" means any personal data, personal information or personally identifiable information (as defined under Applicable Data Protection Law) that Laserfiche processes on behalf of Subscriber in connection with the provision of the Cloud Services, as more particularly described in Annex 1 of this DPA.

1.10 "**PIPEDA**" means the Canadian Personal Information Protection and Electronic Documents Act, 2000.

1.11 "**Processing of Personal Data**" has the meaning subscribed to such term under Applicable Data Protection Law as it relates to the processing described in Annex I.

1.12 "**Restricted Transfer**" means: (i) where the EU GDPR applies, a transfer of Personal Data from the European Economic Area to a country outside of the European Economic Area which is not subject to an adequacy determination by the European Commission; (ii) where the UK GDPR applies, a transfer of Personal Data from the United Kingdom to any other country which is not based on adequacy regulations pursuant to Section 17A of the United Kingdom Data Protection Act 2018; and (iii) where the Swiss DPA applies, a transfer of Personal Data from Switzerland to any other country which is not determined to provide adequate protection for personal data by the Federal Data Protection and Information Commission or Federal Council (as applicable).

1.13 "**Standard Contractual Clauses**" means: (i) where the EU GDPR or Swiss DPA applies, the contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council ("**EU SCCs**"); and (ii) where the UK GDPR applies, the "International Data Transfer Addendum to the EU Commission Standard Contractual Clauses" issued by the Information Commissioner under s.119A(1) of the Data Protection Act 2018 ("**UK Addendum**").

1.14 "**Swiss DPA**" means the Swiss Federal Act on Data Protection 1992 (including as amended or superseded).

1.15 "**Subprocessor**" means direct and indirect subcontractors of Laserfiche and Laserfiche Affiliates, which may Process Personal Data in accordance with this DPA, including, without limitation, Laserfiche Solution Providers. For the avoidance of doubt, a Laserfiche employee, independent contractor or consultant is not a Subprocessor.

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

Where applicable, the terms "**controller**," "**business**," "**processor**," "**service provider**," "**data subject**," "**consumer**," "**process**," "**personal data**," "**personal information**," "**sell**," "**share**," "**business purpose**," "**commercial purpose**," "**supervisory authority**," "**deidentified**," "**aggregate consumer information**," (or any equivalent terms) shall have the meaning ascribed to them under Applicable Data Protection Law.

2. Scope and Applicability of this DPA

2.1 This DPA applies where and only to the extent that Laserfiche processes Personal Data that is subject to Applicable Data Protection Law which impose an obligation directly upon Laserfiche as a Processor or a Service Provider (as applicable) by virtue of the specific Processing of Personal Data in the course of providing the Cloud Services in the specific Laserfiche Cloud Data Center Region (as defined below) that you have subscribed to. For the avoidance of doubt, Laserfiche is not responsible for determining the requirements of laws or regulations applicable to your business, or whether the Cloud Services and related processing by Laserfiche meet the requirements of any laws or regulations that may apply to you or to the Processing of Personal Data.

2.2 As between the parties, Subscriber is responsible for the lawfulness of the Processing of Personal Data under this DPA. Subscriber will not use the Cloud Services or request Processing by Laserfiche in a manner that would violate Applicable Data Protection Law.

3. Role and Obligations of the Parties

3.1 You acknowledge and agree that with regard to the Processing of Personal Data under this DPA, Laserfiche is the Processor or the Service Provider (as applicable) and you are the Controller or Business (as applicable) of the Personal Data or you have obtained the authorization of relevant Controller(s) or Business(es) to agree to the Processing of Personal Data by Laserfiche as set forth in this DPA. You are responsible for the lawfulness of the instructions you provide to Laserfiche regarding the Processing of Personal Data and compliance with your obligations as a Controller or a Business (as applicable) under Applicable Data Protection Law and in accordance with the features and functionality of the Cloud Services and the Documentation. You will not use the Cloud Services in conjunction with Personal Data to the extent that doing so would violate Applicable Data Protection Law.

3.2 You warrant that you have all the necessary rights to provide the Personal Data to Laserfiche for the Processing to be performed in relation to the Cloud Services. To the extent required by Applicable Data Protection Law, you are responsible for ensuring that any necessary notices to Data Subjects or Consumers (as applicable) are provided and any necessary Data Subject or Consumer (as applicable) consents to this Processing are obtained, and for ensuring that a record of such consents is maintained. You have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which you acquired Personal Data.

3.3 During the Subscription Term, you appoint Laserfiche as a Processor or a Service Provider (as applicable) with respect to the Personal Data you provide to Laserfiche under the Agreement and consent to the use of Subprocessors by Laserfiche in order to allow Laserfiche to fulfill its contractual obligations under the Agreement, in accordance with Section 5 of this DPA. Laserfiche is responsible for compliance with its obligations under this DPA and for compliance with its obligations as a Processor or a Service Provider (as applicable) under Applicable Data Protection Law.

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

3.4 As a Processor or a Service Provider (as applicable), Laserfiche and any Subprocessors, will Process Personal Data solely for the purpose of (i) providing the Cloud Services in accordance with the Agreement and this DPA, as further described in **Annex I** of this DPA; (ii) complying with your documented written lawful instructions, or (iii) complying with Laserfiche's regulatory or other legal obligations, all in accordance with the terms of this DPA.

3.5 To the extent that any Personal Data is "personal information" subject to the CCPA, Laserfiche shall not further: (i) sell or share the Personal Data, (ii) collect, retain, use, or disclose the Personal Data for any purpose, including a commercial purpose, other than for the specific business purpose of providing the Cloud Services specified in the Agreement or as permitted or required under Applicable Data Protection Law, (iii) retain, use, or disclose the Personal Data outside of the parties' direct business relationship; or (iv) combine Personal Data with personal information that Laserfiche receives from or on behalf of another person, or collects from its own interactions with any other sources, provided that Laserfiche may combine personal information to perform any business purpose as otherwise permitted by the CCPA. Laserfiche certifies that it understands these restrictions and will comply with them. Laserfiche further agrees that: (i) Laserfiche shall comply with applicable obligations under CCPA and provide the same level of privacy protection as is required by CCPA; (ii) you have the right to take reasonable and appropriate steps to help ensure that Laserfiche uses Personal Data in a manner consistent with your obligations under CCPA; (iii) Laserfiche shall notify you if it makes a determination that it can no longer meet its obligations under CCPA; and (iv) you have the right, upon notice, to take reasonable and appropriate steps to stop and remediate unauthorized use of Personal Data.

3.6 Notwithstanding anything to the contrary in this DPA or the Agreement, to the extent any Personal Data becomes "deidentified" or in the "aggregate" as those terms are defined under Applicable Data Protection Law ("**Deidentified Data**"), Laserfiche may use such Deidentified Data for any commercial purpose in accordance with Applicable Data Protection Law, including but not limited to developing analytics, improving the Cloud Services, and other products and offerings, conducting research and development, and similar legitimate and internal business purposes. Laserfiche may retain, use and disclose Deindentified Data for such purpose, without restriction. ~~Laserfiche may also integrate third-party large language models ("Third-Party LLM") into the Cloud Services for the purpose of enhancing functionality, automating tasks, or improving user experience, and may use for such purpose Deidentified Data, such that neither a Subscriber nor any individual can be identified, unless otherwise agreed in writing by the parties. Subscriber agrees that Laserfiche may (i) make Deidentified Data available to third parties including its other customers service providers, contractors and affiliates, in compliance with applicable law, and (ii) use Deidentified Data to produce results for Subscriber, to maintain, test, evaluate, develop and improve the Cloud Services, for product performance analysis and for any other internal business purposes of Laserfiche, and to the extent and in the manner otherwise not prohibited under applicable law. In such case, Laserfiche shall ensure that any Third-Party LLM provider engaged under this provision is contractually obligated to comply with data privacy, security, and confidentiality standards no less protective than those set forth in this DPA.~~

3.7 You warrant that Laserfiche's Processing of Personal Data in accordance with your instructions will not violate or cause Laserfiche to violate Data Protection Law or third-party terms. If Laserfiche reasonably believes that your documented written instructions violate Applicable Data Protection Law, Laserfiche may suspend the performance until you have modified or confirmed the lawfulness of such documented written instructions. If Laserfiche notifies you that either the

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

documented written instructions or the expense for such written instructions are not feasible you may terminate the Cloud Services by providing Laserfiche with a written notice within one month after notification. Laserfiche will refund a prorated portion of any prepaid charges for the period after such termination date. The parties agree that this DPA and the Agreement set out your complete and final instructions to Laserfiche in relation to the Processing of Personal Data and Processing outside the scope of these instructions (if any) shall require prior written agreement between Subscriber and Laserfiche.

4. Cooperation

4.1 **Correspondence.** To the extent permitted by law, Laserfiche will inform you of (i) requests from Data Subjects or Consumers (as applicable) exercising their rights under Applicable Data Protection Law (including requests to access, restrict, receive and transmit, delete or erase, rectify, or object to Processing of specific Personal Data and right to opt-out from the sale of their personal information as applicable) and (ii) any other correspondence, enquiry or complaint received from a Data Subject, Consumer, regulator or other third party addressed to Laserfiche regarding Personal Data processed by Laserfiche in connection with the Cloud Services (collectively "**Correspondence**") but only where Laserfiche is made aware that such Correspondence relates to you as a Controller. You will be responsible for responding to such Correspondence.

4.2 Unless required by applicable law, Laserfiche will not respond directly to any Correspondence and will reasonably assist you in responding to such Correspondence to the extent that you are unable to independently access the relevant Personal Data within the Services Environment. In such case, you may submit a “service request” by emailing privacy@laserfiche.com, and provide detailed written instructions to Laserfiche (including the Personal Data necessary to identify the Data Subject or the Consumer) on how to reasonably assist with such Correspondence in relation to Personal Data held in your Services Environment. To the extent legally permitted, you will be responsible for any costs arising from Laserfiche’s provision of such assistance.

4.3 If a Data Subject, a consumer or a regulator brings a claim directly against Laserfiche for a violation of Data Subject or consumer rights (as applicable) in connection with Laserfiche's Processing of Personal Data in accordance with your documented instructions, you will indemnify Laserfiche for any cost, charge, damages, expenses or loss arising from such a claim.

4.4 **Data Protection Impact Assessments.** To the extent required under Applicable Data Protection Law, Laserfiche shall provide reasonably requested information regarding Laserfiche's Processing of Personal Data under the Agreement to enable you to carry out data protection impact assessments (or risk assessments) or prior consultations with supervisory authorities as required by Applicable Data Protection Law.

4.5 **General cooperation**. Each party will reasonably cooperate with the other in any activities contemplated by this DPA and to enable each party to comply with its respective obligations under Applicable Data Protection Law.

5. Laserfiche Affiliates and Subprocessors

5.1 Subject to terms and restrictions set forth in this DPA, you agree and provide a general prior authorization to Laserfiche to engage Subprocessors (including Laserfiche Affiliates) to Process

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

Personal Data on behalf of Laserfiche and assist in the performance of the Cloud Services, including those Subprocessors listed here (the "**Subprocessor List")**.

6. Sub-processors.

6.1 **Sub-processor Obligations.** Laserfiche will enter into a written agreement with each Subprocessor imposing data protection obligations no less protective of Personal Data as this DPA. Laserfiche remains responsible at all times for and the acts or omissions of its Subprocessors that cause Laserfiche to breach any of its obligations under this DPA.

6.2 **Objection to Sub-processors**. Subscriber may subscribe to notifications of new Subprocessors at the subscriber notification portal, and if Subscriber subscribes, Laserfiche shall notify Subscriber if it makes any changes to the Subprocessor List at least 10 days before such change. Within 5 calendar days of Laserfiche providing such notice to you, you may object to the intended involvement of a Subprocessor in the performance of the Cloud Services, providing, in writing, objective justifiable grounds related to the ability of such Subprocessor or Laserfiche Affiliate to adequately protect Personal Data in accordance with this DPA or European Data Protection Law. You should submit this writing to privacy@laserfiche.com. In the event your objection is justified, you and Laserfiche will work together in good faith to find a mutually acceptable resolution to address your objections, including without limitation reviewing additional documentation supporting the Subprocessors' compliance with this DPA or Applicable Data Protection Law, or delivering the Cloud Services without the involvement of such Subprocessor. To the extent you and Laserfiche do not reach a mutually acceptable resolution within a reasonable timeframe, Laserfiche will, at its sole discretion, either (i) not appoint the Subprocessor; or (ii) permit Subscriber to suspend or terminate the affected portion of the Cloud Services in accordance with the termination provisions in the Agreement without liability to either party (but without prejudice to any fees incurred by Subscriber prior to suspension or termination). In such case, Laserfiche shall refund Subscriber for any prepaid unused portion of the affected portion of the Cloud Services.

7. Security Measures; Confidentiality

7.1 Each party agrees that it has implemented and will maintain appropriate and reasonable technical and organizational measures to ensure a level of security of the Processing of Personal Data appropriate to the risk. These measures will take into account the nature, scope and purposes of Processing as specified in this DPA, as appropriate, and are intended to protect Personal Data against the risks inherent to the Processing of Personal Data in the performance of the Cloud Services, in particular risks from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored or otherwise Processed.

7.2 Laserfiche has specifically implemented system access, data access, transmission and encryption, input, data backup, and security oversight, enforcement and other security controls and measures specified in the Documentation ("**Security Measures**"). The Security Measures shall, at a minimum, include the measures identified in Annex II of this DPA. You are advised to carefully review the applicable Documentation to understand which specific Security Measures and practices apply to the particular Cloud Services ordered by you, and to ensure that these Security Measures and practices are appropriate for the Processing of Personal Data pursuant to this DPA. You hereby instruct Laserfiche to Process Personal Data in accordance with the Documentation.

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

7.3 You acknowledge that the Security Measures are subject to technical progress and development and that Laserfiche may update or modify its Security Measures from time to time, provided that such updates and modifications do not result in the degradation of the overall security of the Cloud Service you have purchased.

7.4 All parties hereto will ensure all such persons or parties, within their respective controls, that may have access to Personal Data subject to this DPA have signed an appropriate confidentiality agreement, are otherwise bound to a duty of confidentiality, or are subject to an appropriate statutory obligation of confidentiality.

8. Audits

8.1 Upon written request, Laserfiche may demonstrate the measures it has taken pursuant to Section 8 in relation to the Personal Data applicable to this DPA. Laserfiche will reasonably contribute to such audits by providing you or your Supervisory Authority with the information and assistance reasonably necessary to conduct the audit. You acknowledge and agree that you shall exercise your audit rights under this DPA (including this Section 8) by instructing Laserfiche to comply with the audit measures described in Section 8.2 below.

8.2 You acknowledge that Laserfiche is periodically audited against recognized data protection and security standards by independent third-party auditors and/or internal auditors respectively. Upon written request, Laserfiche shall supply (on a confidential basis) a summary copy of its most current audit report(s), which is a SOC 2 Type 2 attestation report under the AICPA Statement on Standards for Attestation Engagements (SSAE) 18 standard, ("**Report**") to you, so that you can verify Laserfiche's compliance with the audit standards against which it has been assessed and this DPA. If the Report does not, in your reasonable judgement, provide sufficient information to confirm Laserfiche's compliance with this DPA, then Laserfiche shall also provide written responses (on a confidential basis) to all reasonable requests for information made by you, including responses to information security and audit questionnaires that are necessary to confirm Laserfiche's compliance with this DPA, provided that you shall not exercise this right more than once per calendar year.

8.3 While it is the parties' intention to ordinarily rely on the Report described above to verify Laserfiche's compliance with this DPA, where a Supervisory Authority requires it, you may provide Laserfiche with thirty (30) days' prior written notice requesting that a third party conduct an audit of Laserfiche's facilities, equipment, documents and electronic data relating to the Processing of Personal Data under the Agreement ("**Audit**"), provided that: (a) the Audit shall be conducted at the Subscriber's expense; (b) the parties shall mutually agree upon the third party chosen to conduct the Audit and the scope, timing, duration and confidentiality basis of the Audit; and (c) the Audit shall not unreasonably impact Laserfiche's regular operations.

8.4 You agree to promptly notify Laserfiche with any information in regard to non-compliance during the course of an Audit and will provide Laserfiche any audit reports generated in connection with any Audit, unless prohibited by Applicable Data Protection Law or otherwise instructed by a Supervisory Authority. You may use the audit reports only for the purposes of meeting your regulatory audit requirements and/or confirming compliance with the requirements of this DPA. The audit reports, information and any artifacts to support the audit provided by Laserfiche are Confidential Information of the parties under the terms of the Agreement.

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

9. Incident Notification

9.1 To the extent Laserfiche becomes aware and determines that a security incident qualifies as a breach of security leading to the misappropriation or accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed on Laserfiche systems or the Services Environment that compromises the security, confidentiality or integrity of such Personal Data ("**Incident**"), Laserfiche will inform you of such Incident without undue delay or otherwise in accordance with Applicable Data Protection Law and provide such information as you may reasonably require as required by Applicable Data Protection Law. However, Laserfiche may not have the ability to evaluate or respond to security incidents where your Users are the source of unauthorized access or disclosure of Personal Data and/or the source is a Solution Provider or another agent whom your Users have granted access to Laserfiche systems or the Services Environment.

9.2 In order to address an Incident, Laserfiche defines escalation paths and response teams involving internal functions such as Information Security and the legal department. The goal of Laserfiche's Incident response will be to restore the confidentiality, integrity, and availability of the Services Environment and the Personal Data that may be contained therein, and to establish root causes and remediation steps. Depending on the nature and scope of the Incident and to the extent required by Applicable Data Protection Law, Laserfiche may also involve and work with you and outside law enforcement to respond to the Incident.

10. Return and Deletion of Personal Data upon Termination of Cloud Services. Upon termination of the Cloud Services or upon expiry of the retrieval period following termination of the Cloud Services (if available), Laserfiche will as soon as reasonably practicable delete all Personal Data (including copies) from the Services Environment by rendering such Personal Data unrecoverable, except as may be required by law and the Agreement. Laserfiche may retain Personal Data where necessary for you to comply with applicable law or legal obligations or protect its rights or those of a third party.

11. International Transfers

11.1 **Data Center Region**. Unless separately agreed to by the parties in writing, Laserfiche will host your Subscription to Laserfiche Cloud from AWS data centers located in the region(s) as specified here (such regions, the "**Laserfiche Cloud Data Center Regions**", and such list, the "**Laserfiche Cloud Data Center Regions List**". Laserfiche may offer hosting from data centers of a different hosting provider or in new regions in the future by amending the Laserfiche Cloud Data Center Regions List. Subscriber is solely responsible for the regions from which its Users upload or access Personal Data and for any transfer or sharing of Personal Data by Subscriber or its Users.

11.2 **Cross-Border Data Transfers.** You acknowledge and agree that Laserfiche may transfer and Process Personal Data to and in the United States and other countries in which Laserfiche, its Affiliates or Subprocessors maintain data processing operations. You and Laserfiche shall at all times ensure such transfers are made in compliance with the requirements of Applicable Data Protection Law.

11.3 **Data Privacy Framework.**

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

11.3.1 Laserfiche is self-certified under the Privacy Shield Framework, now superseded by the Data Privacy Framework, as administered by the U.S. Department of Commerce, in order to implement appropriate safeguards for transfers of Personal Data to the United States pursuant to Article 46 of the GDPR. To the extent the Data Privacy Framework can be used to lawfully transfer Personal Data to the United States, and for as long as Laserfiche is self-certified to the Data Privacy Framework, Laserfiche will adhere to the Data Privacy Framework Principles, including by: (a) processing such Personal Data only for the limited and specified purposes set out in the Agreement, including this DPA; (b) providing at least the same level of privacy protection to the Personal Data as is required by the Data Privacy Framework Principles; (c) promptly notifying you if it makes a determination that it can no longer meet its obligation under (b) above, and in such event, promptly taking reasonable and appropriate steps to stop and remediate any processing until such time as the processing meets the level of protection as is required by the Data Privacy Framework Principles; and (d) at your sole election, ceasing the processing of the Personal Data if, in your reasonable discretion, Laserfiche is not providing the same level of protection to the Personal Data as is required by the Data Privacy Framework Principles. Laserfiche intends to remain self-certified under the Data Privacy Framework as long as the Data Privacy Framework is recognized as a valid transfer mechanism under Applicable Data Protection Law. Details about Laserfiche's self-certification to the Data Privacy Framework are available at: https://www.dataprivacyframework.gov/s/participant-search/participant-detail?id=a2zt00000008RnHAAU&status=Active

11.3.2 You acknowledge that Laserfiche may disclose this DPA and any relevant privacy provisions in the Agreement to the US Department of Commerce, the Federal Trade Commission, a relevant European supervisory authority or other public or regulatory authority, court or tribunal, upon their request.

11.3.3 If Laserfiche is unable to comply with this Clause 11.3, Clause 11.4 shall apply.

11.4 **Restricted transfers.** The parties agree that when the transfer of Personal Data from Subscriber to Laserfiche is a Restricted Transfer it shall be subject to the appropriate Standard Contractual Clauses as follows:

11.4.1 in relation to Personal Data that is protected by the EU GDPR, the EU Standard Contractual Clauses will apply completed as follows:

a) Module Two will apply;

b) in Clause 7, the optional docking clause will apply;

c) in Clause 9, Option 2 will apply, and the time period for prior notice of subprocessor changes shall be as set out in Section 6 of this DPA;

d) in Clause 11, the optional language will not apply;

e) in Clause 17, Option 1 will apply, and the EU SCCs will be governed by the Republic of Ireland law;

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

f) in Clause 18(b), disputes shall be resolved before the courts of the Republic of Ireland;

g) Annex I of the EU SCCs shall be deemed completed with the information set out in Annex I to this DPA; and

h) Annex II of the EU SCCs shall be deemed completed with the information set out in Annex II to this DPA.

11.4.2 in relation to Personal Data that is protected by the UK GDPR, the UK Addendum will apply completed as follows:

a) The EU SCCs, completed as set out above in Section 11.3.1 of this DPA shall also apply to transfers of such Personal Data, subject to sub-section (b) below; and

b) Tables 1 to 3 of the UK Addendum shall be deemed completed with relevant information from the EU SCCs, completed as set out above, and the options "neither party" shall be deemed checked in Table 4. The start date of the UK Addendum (as set out in Table 1) shall be the date of this DPA.

11.4.3 In relation to Personal Data that is protected by the Swiss DPA, the EU SCCs will apply as set out in Section 11.4.1 amended as follows:

a) references to 'Regulation (EU) 2016/679' in the EU SCCs will be deemed to refer to the Swiss DPA;

b) references to specific articles of 'Regulation (EU) 2016/679' will be deemed replaced with the equivalent article or section of the Swiss DPA;

c) references to 'EU', 'Union' and 'Member State' will be deemed replaced with 'Switzerland';

d) references to the 'competent supervisory authority' and 'competent courts' are replaced with the 'Swiss Federal Data Protection Information Commissioner' and 'applicable courts of Switzerland' (as applicable);

e) in Clause 17, the EU SCCs will be governed by the laws of Switzerland; and

f) in Clause 18(b), disputes shall be resolved before the competent courts of Switzerland.

11.5 **Onward transfers.** Laserfiche shall not participate in (nor permit any Subprocessor to participate in) any other Restricted Transfers (whether as an exporter or an importer of the Personal Data) unless the Restricted Transfer is made in full compliance with Applicable Data Protection Law.

11.6 **Alternative Transfer Arrangements**. To the extent Laserfiche adopts an alternative data export mechanism (for Restricted Transfer not described in this DPA ("**Alternative Transfer**

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

Mechanism"), the Alternative Transfer Mechanism shall apply instead of any applicable transfer mechanism described in this DPA (but only to the extent such Alternative Transfer Mechanism complies with European Data Protection Law and extends to the territories to which Personal Data is transferred) and you agree to execute such other and further documents and take such other and further actions as may be reasonably necessary to give legal effect such Alternative Transfer Mechanism. In addition, if and to the extent that a court of competent jurisdiction or a Supervisory Authority with binding authority orders or determines (for whatever reason) that the measures described in this DPA cannot be relied on to lawfully transfer such Personal Data, you acknowledge and agree that Laserfiche may implement any additional measures or safeguards that may be reasonably required to enable the lawful transfer of such Personal Data.

12. Limitation of Liability. Each party's liability (and each of its Affiliate's liability) taken together in the aggregate, arising out of or related to this DPA (including the Standard Contractual Clauses) whether in contract, tort, or under any other theory of liability, is subject to the limitation of liability provisions of the Agreement. Any reference in such limitation of liability provisions to the liability of a party means the aggregate liability of that party and all of its Affiliates (including Subscriber Affiliates) under the Agreement and this DPA (including the Standard Contractual Clauses), taken together.

13. Miscellaneous

13.1 Except for the changes made by this DPA, the Agreement remains unchanged and in full force and effect. If there is any conflict or inconsistency between this DPA and the Agreement, the provisions of the following documents (in order of precedence) shall prevail: (a) Standard Contractual Clauses (where applicable); then (b) this DPA; and then (c) the main body of the Agreement.

13.2 Notwithstanding anything to the contrary in the Agreement (including this DPA), Laserfiche shall have a right to collect, use and disclose data relating to the use, support and/or operation of the Cloud Services ("**Service Data**") in connection with its legitimate interests, such as billing, account management, technical support, and product development. To the extent any such Service Data is considered personal data under Applicable Data Protection Law, Laserfiche shall be responsible for and shall Process such data in accordance with the Laserfiche Privacy Notice located at https://www.laserfiche.com/legal/privacy/ (as updated from time to time) and Applicable Data Protection Law. Subscriber shall make a copy of Laserfiche's Privacy Notice available to any data subjects whose Personal Data is provided by the Subscriber to Laserfiche in connection with the Cloud Services. For the avoidance of doubt and except for this Section 13.2, the terms of this DPA shall not apply to Service Data.

13.3 Subscriber acknowledges that Laserfiche may disclose this DPA (including the Standard Contractual Clauses) and any relevant privacy provisions in the Agreement to the US Department of Commerce, the Federal Trade Commission, a supervisory authority, or any other Canadian, US or European judicial or regulatory body upon their request.

13.4 Notwithstanding anything else to the contrary in the Agreement and without prejudice to Section 3 (Roles and Obligations of the Parties), Laserfiche may periodically make modification to this DPA as may be required to comply with Applicable Data Protection Law.

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

13.5 This DPA shall be governed by and construed in accordance with governing law and jurisdiction provisions in the Agreement, unless required otherwise by Applicable Data Protection Law.

Annex I

Data Processing Description

This Annex I forms part of the DPA and describes the processing that the processor will perform on behalf of the controller.

A. LIST OF PARTIES

Controller(s) / Data exporter(s): *Identity and contact details of the controller(s) /data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union*

1.	Name:	The party identified as the "Subscriber" in the Agreement and this DPA
	Address:	The address provided in the Agreement
	Contact person's name, position and contact details:	As set out in the Agreement
	Activities relevant to the data transferred under these Clauses:	See B. below
	Signature and date:	Executed as per Agreement
	Role (controller/processor):	Controller

Processor(s) / Data importer(s):

1.	Name:	The party identified as "Laserfiche" in the Agreement and this DPA
	Address:	As set out in the Agreement
	Contact person's name, position and contact details:	Wylie Strout, Chief Legal Officer and DPO
	Activities relevant to the data transferred under these Clauses:	See B. below
	Signature and date:	Executed as per Agreement
	Role (controller/processor):	Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred:	Subscriber may submit Personal Data to the Cloud Services, the extent of which is determined and controlled by Subscriber in its sole discretion, and which may include, but is not limited to, Personal Data relating to the following categories of data subjects:

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

	• Employees, contractors or job applicants of Subscriber; • Individuals authorized to use the Cloud Services by Subscriber; • Current and potential customers, business partners or vendors of Subscriber; and • Any other data subjects whose data may be processed from time to time pursuant to the Agreement and this DPA.
Categories of personal data transferred:	The categories of Personal Data processed by Laserfiche are determined and controlled by Subscriber in its sole discretion and may include, but are not limited to the following categories of Personal Data: • Contact data (name, title, email address, telephone number, mailing address); • Account credentials; and • IP address.
Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures:	Subscriber, or third parties acting on their behalf, or through their subscription may submit Personal Data that contains special categories of data to Laserfiche in connection with the Cloud Service, the nature and extent of which is exclusively determined and controlled by Subscriber. See Annex II for the restrictions and safeguards applied.
The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis):	Continuous
Nature of the processing:	Providing the Cloud Services to Subscriber. Personal Data transferred will be processed in accordance with the Agreement and may be subject to the following processing activities: (A) storage and other processing necessary to provide, maintain, and improve the Cloud Services, as applicable, provided to Subscriber; and/or (B) disclosures in accordance with the Agreement and/or as compelled by applicable laws.
Purpose(s) of the data transfer and further processing:	Processing (a) to perform any steps necessary for the performance of the Agreement; (b) to provide

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

	the Cloud Services in accordance with the Agreement; (c) initiated by users in their use of the Cloud Services; (d) to comply with other reasonable instructions provided by Subscriber that are consistent with the terms of the Agreement and this DPA; and (e) to comply with any legal obligations under applicable law, including Applicable Data Protection Law.
The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:	The duration of the Agreement plus the period from the expiry of the Agreement until deletion of the Personal Data by Customer in accordance with the Agreement.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance (e.g. in accordance with Clause 13 SCCs)	The competent supervisory authority, in accordance with Clause 13 of the EU SCCs, is either (i) the supervisory authority applicable to the data exporter in its EEA country of establishment or, (ii) where the data exporter is not established in the EEA, the supervisory authority applicable in the EEA country where the data exporter's EU representative has been appointed pursuant to Article 27(1) of the GDPR, or (iii) where the data exporter is not obliged to appoint a representative, the supervisory authority applicable to the EEA country where the data subjects relevant to the transfer are located. With respect to personal data regulated by the UK GDPR, the competent supervisory authority is the Information Commissioners Office. With respect to the processing of Personal Data to which the Swiss DPA applies, the competent supervisory authority is the Swiss Federal Data Protection and Information Commissioner. With respect to the processing of Personal Data to which PIPEDA applies, the competent supervisory authority is the Office of the Privacy Commissioner of Canada.

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

Annex II

Technical and Organizational Security Measures

Description of the technical and organizational measures implemented by the processor(s) / data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Measure	Description
Measures of pseudonymisation and encryption of personal data	• Data that resides in Amazon Web Services (AWS) is encrypted at rest using AES-256 as stated in AWS' documentation and whitepapers. • Encryption keys are secured against unauthorized access during generation, storage, use and destruction. • Customer interfaces to Laserfiche Cloud is encrypted using TLS encryption. • Backup databases are stored in encrypted EBS snapshots.
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	• Access controls are implemented to enforce confidentiality, integrity and availability. • Access to in-scope systems requires a user ID plus SSH Keys and/or password authentication. Where passwords are used, password parameters enforce minimum length, password age and complexity requirements. • Privileged access to Laserfiche Cloud systems is restricted to appropriate personnel. • Access to Laserfiche Cloud production systems is logically and physically segregated from the Laserfiche network. • Antivirus software is used to protect Laserfiche workstations used to access the Laserfiche Cloud system from malicious code or viruses. • Laserfiche employees are prohibited from accessing customer data without prior customer request and authorization.
Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident	• Customer databases are backed up at regular intervals throughout the day by an automated process. • Backup restorations are tested ona quarterly basis. • Backups are configured to be retained for at least seven days. Laserfiche generally does not support restoring a customer repository or specific data from backups, as Laserfiche Cloud backups are solely intended for recovering the multitenant SaaS platform from a systemwide outage event. The Laserfiche data backup system is not meant as a backup solution for individual accounts with restore points.

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

	Customers are responsible for their own data backups for content stored in the Laserfiche Cloud repository. • Services requiring high availability are deployed across multiple availability zones within an AWS region. • Services that are not deployed across multiple availability zones are monitored and will trigger alerts to manually restore services in alternate availability zones.
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing	• A global independent accounting and advisory firm performs annual testing of Laserfiche Cloud controls via inquiry, observation, and inspection, and provides an attestation report under the AICPA Statement on Standards for Attestation Engagements (SSAE) 18 standard. • Laserfiche uses a third-party security firm to conduct annual external penetration testing of the Laserfiche Cloud systems. • Laserfiche performs periodic network vulnerability scans and addresses critical issues using a risk-based approach. • Security incident response plans are tested annually, and plans are updated, if necessary. • Laserfiche assesses the effectiveness of its security awareness program through quarterly employee simulated phishing campaigns.
Measures for user identification and authorisation	• Access to Laserfiche Cloud operational and production environments is controlled by user IDs, passwords, role-based access and least privilege principle. Multi-factor authentication (MFA) is made available to customers to further enhance security and restrict access to their data. • Identity and access management processes for Laserfiche user account provisioning, de-provisioning and changes are enforced.
Measures for the protection of data during transmission	• Customer interfaces to Laserfiche Cloud is encrypted using TLS encryption.
Measures for the protection of data during storage	• Access controls restrict access to customer data. • Customer databases and backup databases in Laserfiche Cloud are encrypted. • Customer data is logically segregated on its own database and customer files are segregated on its own virtual disk. • Endpoint security software is used to protect workstations used to access the Laserfiche Cloud system from malicious code or viruses.
Measures for ensuring physical security of locations at which	• Laserfiche utilizes AWS for its production environments. The physical and environmental controls related to the facilities housing the production environments are managed by the subservice organization.

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

personal data are processed	• The subservice organization SOC reports are reviewed on an annual basis in accordance with Laserfiche's security standards.
Measures for ensuring events logging	• An IDS is deployed to monitor for potential security incidents that are reviewed, escalated and tracked through resolution by Laserfiche.
Measures for ensuring system configuration, including default configuration	• Laserfiche has a change management policy to manage configuration changes. • Any changes made to the Laserfiche Cloud production environment are logged in the ticketing system and are reviewed and approved by authorized individuals prior to deployment.
Measures for internal IT and IT security governance and management	• Laserfiche has established an Information Security Management System (ISMS) in accordance with the ISO 27001. • Laserfiche has a documented Information Security Policy, which is approved by the Laserfiche Board of Directors. • The Laserfiche Board of Directors and management provide oversight over the Information Security program through periodic updates on risk assessments, third-party attack and penetration studies, and compliance with information security policies. • The Laserfiche CEO is accountable for the security, availability and confidentiality of information assets. The CTO has overall responsibilities over the software development life cycle and security for Laserfiche products. The CIO provides IT and security governance, along with the Information Security Officer. • The Laserfiche Board of Directors has authorized the CIO and Information Security Officer to enforce Laserfiche Cloud and information security policies. • A formal security awareness program is in place to make all employees aware of the company's security policy, standards, and obligations of users. • Employees are required to read and sign company policies, confidentiality agreements, and code of conduct upon hire.
Measures for certification/assurance of processes and products	• A global CPA firm performs annual testing of Laserfiche Cloud controls via inquiry, observation, and inspection, and provides an attestation report under the AICPA Statement on Standards for Attestation Engagements (SSAE) 18 standard. • Laserfiche has aligned its information security program to ISO 27001. • Laserfiche has a Laserfiche Gold, Platinum and Administration certification training programs that are available to a Subscriber, Solution Providers and other third parties. `

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

Measures for ensuring data minimisation	• Laserfiche policies limit data collection to the purposes of processing (or the data that the Subscriber chooses to provide). • Security measures are implemented to provide Laserfiche employees with only the minimum amount of access necessary to perform required functions.
Measures for ensuring data quality	• Laserfiche has a process that allows individuals to exercise their privacy rights, including a right to amend and update information, as described in Laserfiche's Privacy Notice available at https://www.laserfiche.com/legal/privacy/. • Laserfiche has a quality assurance team that is responsible for data quality for Laserfiche products.
Measures for ensuring limited data retention	• Database backups are retained to support Laserfiche Cloud system recovery operations in the event of a disaster or other contingency. Laserfiche does not make specific Subscriber commitments for data retention. • Data for provisional customers and subscription customers is removed after the end of the trial period and upon written notice by the customer, respectively.
Measures for ensuring accountability	• Security responsibilities are included in Laserfiche job descriptions for administrators. • Laserfiche Information Security Policy, Laserfiche AI Governance and Usage Policy and Employee Handbook contain employee sanctions on noncompliance with policies. • Laserfiche policies require violations of information security policies to be reported to People Operations and/or Information Security. • Laserfiche has agreements with its Solution Providers that includes requirements to comply with all applicable laws, perform in an ethical manner, and adhere to a data processing agreement.
Measures for allowing data portability and ensuring erasure	• Laserfiche has a process that allows individuals to exercise their privacy rights, including a right of erasure or a right to data portability, as described in Laserfiche's Privacy Notice available at https://www.laserfiche.com/legal/privacy/. • Subscribers have ownership and control over their data in Laserfiche Cloud.

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

STATE OF UTAH COOPERATIVE CONTRACT AMENDMENT

AMENDMENT #: 2

CONTRACT #: AR3109

Starting Date: Unchanged

Expiration Date: Unchanged

TO BE ATTACHED AND MADE PART OF the specified contract by and between the State of Utah Division of Purchasing and Compulink Management Center, Inc. dba Laserfiche (Referred to as CONTRACTOR).

BOTH PARTIES AGREE TO AMEND THE CONTRACT AS FOLLOWS:

The attached, updated Laserfiche Privacy Notice is amended and added to Attachment E of Master Agreement #AR3109.

Effective Date of Amendment: As of the last signature date below.

All other terms and conditions of the contract, including those previously modified, shall remain in full force and effect.

IN WITNESS WHEREOF, the parties sign and cause this contract to be executed.

CONTRACTOR

DocuSigned by:
Peter Wayman
D8A46824A026490...
Contractor's Signature — 9/28/2023 Date

Peter Wayman
Contractor's Name (Print)

President
Title (Print)

STATE OF UTAH

DocuSigned by:
C38BE9DAC528424...
Director, State of Utah Division of Purchasing — 9/29/2023 Date

For Division of Purchasing Internal Use			
Purchasing Agent	Phone #	E-mail Address	**Contract #**
Blake Theo Porter	801-957-7136	btporter@utah.gov	AR3109

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

Laserfiche®

Privacy Notice

NOTICE: This Privacy Notice is effective as of August 24, 2023.

Compulink Management Center, Inc. operating as Laserfiche and its affiliates ("**Laserfiche**", "**we**", "**us**", "**our**") respect your privacy and understand that you care about how your personal information is collected and used. This Privacy Notice ("**Notice**") describes the types of personal information that we process about you, how we use it, how we disclose it, your rights and choices, and how you can contact us about our privacy practices. This Notice applies to our processing of personal information in connection with the delivery of our website at https://www.laserfiche.com/ (the "**Site**"), and all products and services (including its content and functionality) offered by Laserfiche (collectively, our "**Services**"). We are committed to taking appropriate steps to help protect the privacy of visitors to our Site or users of our Services.

Some data protection laws make a distinction between organizations that process personal data for their own purposes (known as "**controllers**" or "**businesses**") and organizations that process personal data on behalf of other organizations (known as "**processors**" or "**service providers**"). Laserfiche may act as either a controller/business or a processor/service provider in respect of your personal data, depending on the circumstances.

Laserfiche is the controller with respect to information you provide through the Site and is located at the address in the section entitled "Contact Us" below.

Sometimes Laserfiche operates as a processor or service provider on behalf of a customer (a separate legal entity), which is the data controller or business. For example, Laserfiche provides cloud services to its customers and may process personal data on each customer's behalf to provide those services. This Notice does not describe the processing of such data. We invite you to visit the applicable customer's privacy notice for information about their privacy practices. Any questions that you may have relating to such personal data and your rights under data protection law should be directed to the customer as the controller or business, not to Laserfiche.

For personal data transferred from the United Kingdom, the European Union, and Switzerland, we will provide appropriate safeguards, such as through use of standard contractual clauses. For more information, please see our "International Transfers" heading below.

You may also have additional rights based upon your jurisdiction. For more information, please see the relevant jurisdiction headings at the end of this Notice or please click on the links for your jurisdiction listed below:

- California

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

- Nevada
- Colorado, Connecticut, Utah, and Virginia
- European Economic Area, Switzerland, or United Kingdom

1. Information We Collect

When you visit or use the Site and/or Services, we collect and retain information that you, as a customer or potential customer, provide through the Site or Services, as well as information that is automatically or passively collected from you, your device, or your browser.

Information You Provide to Us

We collect information that you provide directly to us. For example, when you manage your user profile, participate in interactive features (such as the Contact Us page), request newsletters or other marketing communications, request customer support, provide other information in connection with a job opening, enter login information, or otherwise communicate with us.

The types of information we may collect include:

- Contact and profile information, including your name, email address, company information, postal address (including zip or postal code), and telephone number.
- Account and log-in information, including your username, password, login details, and transaction details.
- Billing information, including your payment instrument number (e.g., credit card or debit card number), expiration date, security code as necessary to process any payments, and transaction details (if applicable).
- Correspondence, for example, reporting a problem or submitting queries, concerns or comments regarding the Site or its content.
- Job application information, including your resume and related data as necessary to consider you for a job opening if you submit an application to us, including your employment history, transcript, writing samples, and references.
- Any other content or information you choose to provide, including photos you may upload.

If you post information on the Site, including on a bulletin board, in a chat room, or community forum, it becomes generally available to the public. Laserfiche does not control or limit the use by visitors of the Site. By posting information on the Site, you understand that Laserfiche may use the information in connection with its business. Therefore, you should not post any information you consider private or sensitive.

Information We May Collect Automatically

We automatically collect information for business and commercial purposes about your device and how your device interacts with our Site and the Services. We may use service providers to collect this information. Some examples of information we automatically collect include the following:

- Information about your visits to the Site and use of the Services, the resources you access, any data you download, and information related to the ways in which you interact with the Site or the Services.

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

- IP addresses, including the general information in such address, such as city, state and zip or postal code, your device's regional settings, unique device identifiers, other information about your mobile phone or other mobile device(s), browser types, and browser language.
- Referral pages and links, URLs, number of clicks, pages viewed, how long you're on a page, your search queries, and results.
- Information about your device, computer and/or browser you use, as well as the device's operating system, such as device hardware model, operating system version, or mobile network information.
- Non-precise location data, including your device's location derived from an IP address or data that indicates a city or zip or postal code.

We use various technologies to collect this information ("**Tracking Technologies**"), as further discussed below under the "**Cookies, Other Tracking Technologies, Interest-Based Advertising, And Choices Regarding the Same**" heading.

Information We Collect from Customers

We provide products and services for our customers and collect and process information about individuals (including through Tracking Technologies) at the direction of and on behalf of our customers ("**Customer Data**"). Customer Data has historically included contact data, demographic data, content, service use data, device connectivity and configuration data, and non-precise location data, among other information. Our processing of Customer Data is governed by the terms of our Cloud Subscription Agreement with each customer. To the extent we combine Customer Data with information we have collected about you through the Site, we will treat the combined information in accordance with the practices described in this Notice, plus any additional restrictions imposed by our customers. We are not responsible for how our customers treat the information we collect on their behalf as a processor or service provider, and we recommend you review each customer's own privacy notice. For more information on your rights and choices regarding Customer Data, please see the "**Your Privacy Rights**" heading below.

Information We Collect From Other Sources

We may obtain information from other third-party sources that we combine with information collected through the Site. These third-party sources vary over time, but include:

- Data brokers from which we purchase demographic data to supplement the data we collect.
- Social networks when you reference our Service or grant permission to Laserfiche to access your data on one or more of these social networks.
- Partners with which we offer co-branded services, sell or distribute our products, or engage in joint marketing activities.
- Publicly available sources, such as open government databases or other data in the public domain.

For example, if you log into a social media website through our Site, we may have access to certain information from that website, in accordance with the procedures and practices of that social media website. You should carefully review the privacy policies and terms of use of these third parties.

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

2. How Laserfiche Uses and Discloses the Information We Collect

Use of Information Collected

Laserfiche collects and uses the information you provide in connection with our Site and Services for a variety of purposes, in accordance with the practices described in this Notice, which may include:

- **Providing our Services to you:** We use your information to operate and manage our Site and Services, including your registration process and user account.
- **Improving and developing our Services and Site:** We may use your information to understand how you use our products, Services, and Site, and how we can improve them, and to obtain insight and analysis. For example, the information collected may assist with customer service improvements and technical improvements to our products.
- **Providing customer and user support:** We may use your information to troubleshoot and diagnose product problems, provide support or technical assistance, investigate security incidents, and to perform services requested by you, such as to respond to your comments, questions, and requests.
- **Sending marketing communications:** Depending on your marketing choices, we may use your information to keep you informed about Laserfiche and our software and Services and promote certain Services and features that you may be interested in, such as communications about third-party products, updates, special offers, promotions, rewards, and events. We may also contact you for market research and to survey your satisfaction with Laserfiche software and Services, encourage you to participate in our user groups, and invite you to events that may be of interest, including trainings, webinars, and conferences.
- **Sending administrative communications:** We may use your information to send you technical notices, updates, security alerts, information regarding changes to our policies, and other support and administrative messages regarding your account with us.
- **Securing our Services:** We may use your information for maintaining the safety and security of our Services, investigating suspicious activity, detecting, and preventing fraudulent or unauthorized use of the Services, and identifying and troubleshooting any problem.
- **Complying with our legal obligations:** We may process your information in order to cooperate with public and government authorities, courts, or regulators, including to comply with legal orders or judicial proceedings, or to respond to lawful requests and otherwise comply with our legal, regulatory and reporting obligations under applicable laws. Additionally, we may process your information, to protect, defend or exercise our legal rights and to ensure the continuity and integrity of our Services, including where we seek to pursue remedies available to us and or in order to limit damages. We will make reasonable efforts to notify our customers and users of any disclosure of their information, unless we are prohibited by law, court order, or exigent circumstances prevent us from doing so.
- **Statistics and analysis:** We may aggregate and anonymize your information in such a way as to prevent the information from being reassociated or identified with an account, user, or individual. We may use aggregated and anonymized information for a variety of statistical and analytical purposes, which may entail providing this information to an agent acting on Laserfiche's behalf to assist in data analytics.

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

We also use information about you for the following purposes:

- Serve personalized advertising tailored to your interests on our Site and/or Service, and third-party Services (where applicable), to the extent it is necessary for our legitimate interest in advertising our Site and Services, or where necessary, to the extent you have provided your prior consent.
- Fulfill any purpose at your direction.
- With your consent, fulfill any other purpose disclosed to you.

For more information about how we use and disclose your information for personalized advertising, please see the "**Cookies, Other Tracking Technologies, Interest-Based Advertising, and Choices Regarding the Same**" heading below.

We may use publicly available information (as that term is defined by applicable law) or information that does not identify you (including information that has been de-identified or aggregated, as those terms are defined by applicable law), for any purpose without obligation to you except as prohibited by applicable law.

Disclosure of Information Collected

Laserfiche will disclose information we have collected about you in accordance with the practices described in this Notice. The types of persons to whom we disclose information include, but are not limited to, the following:

Disclosing to Service Providers

We will occasionally hire service providers or contract with third-party consultants to provide limited services on our behalf. Laserfiche will only provide those service providers and other third-party consultants the information they need to deliver services, and, to the extent required by law. They are prohibited from using that information for any other purpose. We may permit these service providers or third-party consultants to use publicly available information (as that term is defined by applicable law) or information that does not identify you (including information that has been de-identified or aggregated, as those terms are defined by applicable law) to the extent permitted by applicable law.

Disclosing to Others

We also disclose information about you to the following categories of recipients:

- **Affiliates**: We may disclose your information to our affiliated and related entities including our subsidiaries. For example, we may disclose your information to our affiliates for customer support, marketing, and technical operations.
- **Customers**: We may disclose your information to our customers in connection with us processing your information on their behalf. For example, we may disclose your information to our customers in order to facilitate your orders, maintain and administer your online accounts, respond to your questions and comments, comply with your requests, market, and advertise to you, and otherwise comply with applicable law.
- **Business Partners**: We may disclose your information to our business partners in connection with offering you co-branded services, selling, or distributing our products, or engaging in joint marketing activities. For example, we may disclose information about you to a retailer for purposes of providing you with product support. We may also disclose your

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

information to approved third parties for marketing purposes; this may include our authorized resellers, user group training partners, and cloud solution providers.

- **Promotions**: Our promotions may be jointly sponsored or offered by third parties. If you voluntarily choose to enter a promotion, we may disclose your information to third parties as set forth in the official rules that govern the promotion as well as for administrative purposes and as required by law (e.g., on a winners list). By entering any such promotion, you agree to the official rules that govern that promotion, and may, except where prohibited by applicable law, allow the sponsor and/or other third parties to use your name, voice and/or likeness in advertising or marketing materials.
- **User Group, Training, and Events**: Our events may be jointly sponsored or offered by third parties. If you voluntarily sign-up for an event through Laserfiche, we may disclose your contact details or information that you provide to the sponsor, facility, or any other organization who we schedule you to meet with at that event in order to fulfill your event registration and/or inform you of future events organized by the sponsor, which we believe you may be interested in.
- **Tracking Technologies**: Some information about your use of the Site and Services and certain third-party services may be collected using Tracking Technologies across time and services and used by us and third parties for business and/or commercial purposes such as to associate different devices you use, and deliver relevant ads and/or other content to you on the Site, Services, and certain third-party services, as explained further under the "**Cookies, Other Tracking Technologies, Interest-Based Advertising, And Choices Regarding the Same**" heading.
- **Third Parties:** We may disclose your information to third parties for the purposes of facilitating your requests (such as when you choose to disclose information with a social network about your activities on the Site or Services) and in connection with tailoring advertisements, measuring, and improving our Service and advertising effectiveness, and enabling other enhancements, subject to your preferences (where applicable).
- **Consent or another lawful purpose**: We may disclose your information for any other lawful purpose and/or with notice to you and with your consent.

We will disclose your information to respond to duly authorized requests from governmental authorities as required by law, or in circumstances in which we believe disclosure is necessary or reasonably appropriate to protect the rights, property, or safety of us or others. Please note that Laserfiche is required to disclose personal information in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.

Laserfiche also discloses your personal information when: (a) we are required to do so by law, regulation, warrant, subpoena or court order, (b) we are required in urgent circumstances to protect the personal safety of Laserfiche employees, users of Laserfiche products or services, or members of the public, (c) it is necessary to enforce our Terms of Use, or to exercise, establish or defend our legal rights, or (d) such disclosure may be part of a sale of all (or substantially all) of the assets of Laserfiche or an affiliated entity where customer information might be included among the transferred assets.

Disclosing to third party websites

Some of the hyperlinks on our Site may lead to third-party services that are not controlled by or affiliated with Laserfiche. These links are provided solely as a convenience to you and not as an

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

endorsement by Laserfiche of the content on such third-party services. Third-party services are subject to the terms of use and privacy policies of each applicable third-party entity, including what information they disclose with us, your rights and choices on their services and devices, and whether they store information in the U.S. or elsewhere. For example, Office Online is a Microsoft service and use of Office Online is subject to Microsoft's terms of use and privacy policy. Laserfiche is not responsible for and does not endorse, guarantee or monitor the content, availability, viewpoints, products or services that are offered or expressed through any third-party services and does not make any representations or warranties regarding the content or accuracy of any content on these third-party websites, including third-party privacy policies. We encourage you to familiarize yourself with and consult each applicable third-party entity's terms of use and privacy policies.

Without limiting the foregoing, in our sole discretion, we may disclose aggregated information which does not identify you or de-identified information (as those terms are defined under applicable law) about you with third parties or affiliates for any legitimate business purpose or with your consent, except as prohibited by applicable law.

3. How We Respond to Do Not Track Signals

Do-Not-Track ("**DNT**") is a preference that can be set in your browser to notify websites you visit that you do not want them to collect certain information about you. Laserfiche does not respond to DNT signals at this time and will not do so unless and until the law is interpreted to require such response. As discussed in this Notice, we and third parties may track your visits to our Site or use of our Services for purposes such as to provide Interest-based Advertising. To the extent you have specific rights in your region with respect to certain preference signals, such as **Global Privacy Control**, please see your region-specific terms for details.

4. Cookies, Other Tracking Technologies, Interest-Based Advertising, And Choices Regarding the Same

Please see our **Cookie Statement** for more information about how we use cookies and similar tracking technologies. In addition to the technologies listed in our **Cookie Statement**, we use the following to collect information:

- **Pixels/Web Beacons**: Pixels or web beacons are code which is embedded in our Site or Services that send information about your use to a server. There are various types of pixels/web beacons, including image pixels (e.g., small graphic images) and JavaScript pixels (e.g., containing JavaScript code). When you access a service that contains a pixel, the pixel may permit us or a separate entity to drop or read cookies on your browser or collect other information about your visit to our Site or use of our Services. We utilize pixels (some of which are provided by separate entities) that allow us to track our conversions with you, bring you advertising, and provide you with additional functionality with our Site or Services.
- **Device Fingerprinting**: Device fingerprinting is the process of analyzing and combining sets of information elements from your device's browser, such as JavaScript objects and installed fonts, in order to create a "fingerprint" of your device and uniquely identify your device and apps.

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

As discussed in our **Cookie Statement**, we also work with ad serving services, advertisers, and other third parties to serve advertisements on the Site, Services, and/or on third-party services. These third parties may use Tracking Technologies on our Sites, Services, and third-party services (including in emails and advertisements) to track your activities across time and services for purposes of associating the different devices you use and delivering relevant ads and/or other content to you on the Site, Services, and third-party services or third-party devices after you have left the Services ("**Interest-based Advertising**").

Some of the third parties that collect information from or about you on the Site or Services in order to provide more relevant advertising to you participate in the Digital Advertising Alliance ("**DAA**") Self-Regulatory Program for Online Behavioral Advertising. This program offers a centralized location where users can make choices about the use of their information for online behavioral advertising. To learn more about the DAA and your opt-out options for their members, please visit (i) for website opt-out, http://www.aboutads.info/choices; and (ii) for mobile app opt-out, http://www.aboutads.info/appchoices. In addition, some of these third parties may be members of the Network Advertising Initiative ("**NAI**"). To learn more about the NAI and your opt-out options for their members, please visit http://www.networkadvertising.org/choices/. Please note that if you opt-out of online behavioral advertising using any of these methods, the opt-out will only apply to the specific browser or device from which you opt-out. Further, opting-out only means that the selected members should no longer deliver certain Interest-based Advertising to you, but does not mean you will no longer receive any targeted content and/or ads (e.g., from other ad networks). We are not responsible for effectiveness of, or compliance with, any third parties' opt-out options or programs or the accuracy of their statements regarding their programs.

Most browsers accept cookies by default. You may instruct your browser, by changing its settings, to decline or delete cookies. If you use multiple browsers on your device, you will need to instruct each browser separately. Your ability to limit cookies is subject to your browser settings and limitations.

Please be aware that if you disable or remove Tracking Technologies some parts of the Services may not function correctly.

For further information about the types of Tracking Technologies we use, why, and how you can control such Tracking Technologies, please see our **Cookie Statement**.

5. Bulletin Boards and Chat Rooms

Occasionally, portions of the Site may allow you to post information that other visitors to the Site will be able to access (i.e., a "bulletin board" or interactive "chat"). If you choose to post information on a bulletin board or through a chat session, it becomes available to the public, and Laserfiche has no ability to control or limit the use of information that is available to the public. Laserfiche and its affiliates will utilize any information you post through the Site in connection with the operation of its business. Laserfiche encourages you not to post any information you consider private or sensitive on the Site. To request removal of your information from such bulletin boards or chat sessions, please contact us using the contact details provided under the "**Contact Us**" heading below. In some cases, we may not be able to remove your information, in which case we will let you know if we are unable to and why.

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

Laserfiche®

6. Your Privacy Rights

- **Jurisdictional Rights**

Consumers in California, Nevada, Colorado, Connecticut, Utah, and Virginia, and data subjects in the European Economic Area, Switzerland or United Kingdom may have additional rights as set forth in the sections entitled "**California Privacy Rights**," "**Nevada Privacy Rights**," "Colorado, Connecticut, Utah, and **Virginia Privacy Rights**," and "**European Privacy Rights**" below. For more information about choices regarding Tracking Technologies, see the section on "**Cookies, Other Tracking Technologies, Interest-Based Advertising, and Choices Regarding the Same**" above.

Your information may be transferred to, and processed in, countries other than the country in which you are resident. These countries may have data protection laws that are different to the laws of your country. Please see the "**International Transfers**" section below for more information.

- **Marketing Communications**
  - If you supply Laserfiche with your postal address online, you may receive periodic mailings from us with information on new products and Services, or upcoming events.
  - If you supply us with your telephone number online, you may receive telephone calls from us with information regarding orders and/or requests you have placed online – such as a software demonstration request or general business inquiry.
  - If you supply us with your email address, then in accordance with your marketing choices, you may receive email messages for marketing purposes, such as providing information on new products and Services, or upcoming events. We may track when you open our email messages or click on the links contained within them.

You have the right to opt-out of marketing communications from us at any time. You can exercise this right by clicking on the "unsubscribe" or "opt-out" link in the marketing emails we send you, or by emailing us at the email address set forth in the section entitled "**Contact Us**" below with the word UNSUBSCRIBE in the subject field of your email. Please note that you cannot opt-out of non-promotional emails, such as those about your account, transactions, servicing, or Laserfiche's ongoing business relations.

You can also opt out of receiving calls to your phone number at any time by requesting to opt-out during any call you receive from us or contacting us as set out in the "**Contact Us**" heading below and specifying you would like to opt-out of calls.

To opt-out of other forms of marketing (such as postal marketing or telemarketing), please contact us using the contact details under the "**Contact Us**" heading below.

Please note that by opting in to allow Laserfiche and its event sponsors/industry partners to receive your contact information through an event in accordance with this Notice, you will be

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

subject to each event sponsor/industry partner's communications and privacy policy and must opt-out with them directly.

7. Security Measures

We have implemented and maintain reasonable industry standard controls, intrusion detection network monitoring, and reasonable security measures designed to protect the personal information that you submit through the Services and Site. These measures include physical access controls, access authorization controls, and firewalls. We also periodically review our information collection, storage, and processing practices to help prevent loss, misuse, unauthorized access, alteration, or other destruction of information we collect. When accessing secure sections of the Site, we use Transport Layer Security (TLS) encryption to secure the communication of information passing between your browser and our servers. Additionally, only authorized administrators, Laserfiche employees and third-party contractors have access to systems containing such information.

Although we take reasonable security measures to protect your information, we cannot guarantee the security of your personal information transmitted to the Site. The transmission of information via the internet is never 100% secure, and we cannot ensure or warrant the security of any information you transmit to us. We are not responsible for circumvention of any privacy settings or security measures contained on the Site.

The safety and security of your information also depends on you. Where we have given you (or where you have chosen) a password for access to certain parts of the Site, products, or Services, you are responsible for keeping this password confidential. Please do not share your password with anyone.

8. International Data Transfers

Laserfiche is headquartered in the United States. Data centers for Laserfiche Cloud Services are located in the United States, Canada, and Ireland, respectively. Operationally, we have on-premises computer facilities in the United States, Canada, Hong Kong and other regions. Our affiliated subsidiaries, third-party service providers, and partners operate around the world. This means that when we collect your personal information, we may process it in any of these jurisdictions. The laws governing our processing of personal information in such jurisdictions may differ from those in the jurisdictions in which you are located. Regardless of where your personal information is processed, we will treat all personal information in accordance with applicable data protection laws and this Notice.

If you are located in the EEA, United Kingdom or Switzerland, we will protect your personal information when it is transferred outside of such locations by processing it in a country that provides an adequate level of protection (click here for a list of countries deemed adequate by the European Commission) or by implementing appropriate safeguards to protect your personal information, including through the use of standard contractual clauses or another lawful transfer mechanisms approved by the European Commission and/or the United Kingdom or Swiss authorities (as applicable). For more information about

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

the lawful transfer mechanisms we rely on, please contact us using the contact details under "**How to Contact Us**" within the **"European Economic Area, Switzerland, and United Kingdom**" section below.

Laserfiche complies with the EU-U.S. Data Privacy Framework ("**EU-U.S. DPF**"), the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework ("**Swiss-U.S. DPF**") as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal data transferred from the European Union and Switzerland to the United States. Laserfiche has certified to the U.S. Department of Commerce that it adheres to the EU-U.S. Data Privacy Framework Principles ("**EU-U.S. DPF Principles**") with regard to the processing of personal data received from the European Union in reliance on the EU-U.S. DPF, from the United Kingdom (and Gibraltar) in reliance on the UK Extension to the EU-U.S. DPF, and from Switzerland in reliance on the Swiss-U.S. DPF. If there is any conflict between the terms in this Notice and the Principles, the Principles shall govern personal data processed in reliance of the Data Privacy Framework ("**DPF**"). To learn more about the DPF, and to view our certification, please visit https://www.dataprivacyframework.gov/s/participant-search.

Laserfiche's responsibility for personal data it receives in reliance on the DPF and subsequent transfers of that personal data to third parties is detailed in the Principles. Where Laserfiche relies on the Principles for onward transfers from the EU and Switzerland, including the onward transfer liability provisions, Laserfiche remains responsible under the Principles for third-party agents processing personal data on its behalf.

With respect to personal data received or transferred pursuant to the DPF, we are subject to the regulatory enforcement powers of the U.S. Federal Trade Commission. In certain situations, we may be required to disclose personal data in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.

Laserfiche commits to resolving complaints about your privacy and our collection and use of your personal data in reliance on the DPF within 45 days of receiving your complaint. Individuals with questions or complaints regarding this Notice should first submit inquiries by contacting us using the contact details provided under the "**Contact Us**" heading below. Laserfiche has further committed to refer unresolved complaints regarding personal data transferred in reliance on the DPF to the American Arbitration Association, an alternative dispute resolution provider located in the United States. If you do not receive timely acknowledgment of your complaint from us, or if we have not resolved your complaint, please contact, or visit the American Arbitration Association for more information or to file a complaint. When filing by mail or email, please complete the appropriate DPF Notice of Arbitration Form located in the link below and forward to the International Centre for Dispute Resolution.

International Centre for Dispute Resolution Case Filing Services
1101 Laurel Oak Road, Suite 100
Voorhees, NJ 08043
United States
Phone: +1.212.484.4181
Email box: casefiling@adr.org

For any questions or for further information about this program, the ICDR's International Arbitration Rules, or with additional language versions of the ICDR's International Arbitration Rules, please contact the International Centre for Dispute Resolution at +1.212.484.4181 or by visiting the

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

website https://www.icdr.org/dpf. The services of the American Arbitration Association are provided at no cost to you.

Under certain limited circumstances, data subjects, as defined by the Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016, of the European Union, may invoke binding arbitration as a last resort if all other forms of dispute resolution have been unsuccessful. To learn more about this method of resolution and its availability to you, please visit https://www.dataprivacyframework.gov/s/.

9. Privacy of Children

The Site and Services are intended for a general audience and not directed to children under sixteen (16) years of age. We do not market products or services to children, and we do not knowingly collect personal information from children any time, including as defined by the U.S. Children's Privacy Protection Act ("**COPPA**").

If you are under the age of 16, please do not provide personal information of any kind whatsoever and please do not use Laserfiche Site and Services or participate in Laserfiche's surveys, contests, events, and other promotions. If you are a parent or guardian and believe Laserfiche has collected such information without parental consent, please contact us as set below in the section entitled "**Contact Us**" and we will remove such data to the extent required by COPPA or other applicable law.

10. Data Retention

We retain personal information we collect from you where we have an ongoing legitimate business need to do so. For example, to provide you with a service you have requested or to comply with applicable legal, tax or accounting requirements.

11. Privacy Notice Changes

Laserfiche may change this Notice from time to time, at Laserfiche's sole discretion. When we update our Notice, we take appropriate measures to inform you, consistent with the significance of the changes we make. If the changes are material, we will notify you or offer you choice if and to the extent this is required by applicable data protection laws. You can see when this Notice was last updated by checking the "effective" date displayed at the top of this Notice. Laserfiche recommends that you review this Notice regularly for any revisions. Your continued use of the Site or Services after such revisions will constitute your acknowledgement of the amended Notice.

12. Contact Us

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

Laserfiche®

If you have any concerns or questions about the information provided in this Notice, or want to exercise your data protection rights, please contact us using the following details:

By mail:

Compulink Management Center, Inc. d/b/a Laserfiche
Attention: Data Protection Officer
3443 Long Beach Blvd.
Long Beach, CA 90807
USA

By email: notices@laserfiche.com

13. California Privacy Rights

California provides additional rights to California residents, including rights through the California Consumer Privacy Act as replaced by the California Privacy Rights Act ("**CPRA**"). This section addresses those additional rights and only applies to California residents.

Additionally, we acknowledge that you may have rights under California law in connection with the personal information we process on behalf of our customers. If personal information about you has been processed by us as a service provider on behalf of a customer and you wish to exercise any rights you have with such personal information, please inquire with our customer directly. If you wish to make your request directly to us, please provide the name of our customer on whose behalf we processed your personal information. We will refer your request to that customer and will support them to the extent required by applicable law in responding to your request.

- **Shine The Light Consumer Rights**

Consumers in the State of California may request a list of categorized third parties and in some cases affiliates to whom we may have disclosed their personal information specifically for those third parties' and/or affiliates' own marketing purposes, as well as the type of personal information disclosed to those parties. If you are a California resident and would like to request this information, please submit a written request to the email or address provided in the section entitled "**Contact Us**" above. Requests must include "***California Privacy Rights Request***" in the first line of the description and include your name, street address, city, state, and ZIP code. Please note that we are not required to respond to requests made by means other than through the provided e-mail address or mail address.

- **California Consumer Rights Under The CPRA**

Notice of Collection.

We have collected the following categories of personal information (as that term is defined in the CPRA) in the past 12 months:

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

- Identifiers, including your name, postal address, email address, and online identifiers (such as IP address).
- Consumer records, including your phone number, billing address, and credit or debit card information.
- Characteristics of protected classifications under California and/or federal law, including your gender.
- Commercial or transactions information, including records of products or services purchased, obtained, or considered.
- Internet activity, including browsing your history, search history, and interactions with a website, email, application, or advertisement.
- Non-precise geolocation data, including your location derived from an IP address.
- Professional, employment or education-related information.
- Inferences drawn from any of the information identified in this section.

For more details about the personal information Laserfiche collects from you and the sources from which we obtain personal information, please review the section entitled "**How Laserfiche Uses and Discloses the Information We Collect**" above.

Additionally, we collect, use, and disclose this personal information for the business and commercial purposes set out in the section entitled "**How Laserfiche Uses and Discloses the Information We Collect**" above. Please see this section above for more details.

Laserfiche does not sell personal information as the term "sell" is traditionally understood. However, some of our disclosures of your personal information may be considered a "sale" or a "share" as those terms are defined by the CPRA. A "sale" is broadly defined under the CPRA to include a disclosure for something of value, and a "share" is broadly defined under the CPRA to include a disclosure for cross-context behavioral advertising. We collect, sell, or share the following categories of personal information for commercial purposes: identifiers, characteristics, commercial or transactions information, internet activity, non-precise geolocation data, and inferences drawn. The categories of third parties to whom we sell or share your personal information include, where applicable, vendors and other parties involved in cross-context behavioral advertising. For details about your rights regarding sales and shares, please see the "**Do Not Sell or Share My Personal Information**" section below.

Laserfiche does not knowingly sell or share the personal information of minors under 16 years old who are California residents.

Sensitive Personal Information.

Some of the personal information we collect may be considered sensitive personal information (as described in the CCPA). For further details of the sensitive personal information we collect (if any) and how we obtain this information, please review the section entitled "**Information We Collect**" above.

We collect, use, and disclose sensitive personal information only for the permissible business purposes for sensitive personal information under the CPRA or without the purpose of inferring

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

characteristics about consumers. Further, we do not "sell" or "share" your sensitive personal information as those terms are defined by the CPRA.

Data Retention.

We retain each category of personal information, including sensitive personal information, for the length of time that is reasonably necessary for the purpose for which it was collected, and as necessary to comply with our legal obligations, resolve disputes, prevent fraud, and enforce our agreements.

Right to Know, Correct, and Delete.

You have the right to know certain details about our data practices. In particular, you may request the following from us:

- The categories of personal information we have collected about you.
- The categories of sources from which the personal information was collected.
- The categories of personal information about you that we disclosed for a business purpose or sold or shared.
- The categories of third parties to whom the personal information was disclosed for a business purpose or sold or shared.
- The business or commercial purpose for collecting or selling or sharing the personal information.
- The specific pieces of personal information we have collected about you.

In addition, you have the right to correct or delete the personal information we have collected from you. These rights are subject to certain exceptions and also apply to sensitive personal information.

To exercise any of these rights, California consumers should submit a request through our online form available here or call our toll free number at 800-985-8533. In the request, please specify which right you are seeking to exercise and the scope of the request. We will confirm receipt of your request within 10 business days. We may require specific information from you to help us verify your identity and process your request. If we are unable to verify your identity, we may deny your requests to know, correct, or delete.

Do Not Sell or Share My Personal Information.

To the extent that using third party cookies and other tracking technologies to serve retargeted or interest-based advertising constitutes a "sale" or "share" of personal information under the CPRA, you may opt-out of such "sales" or "shares" by visiting our cookie consent platform at the button below and opting out of any third party advertising cookies, or by clicking on the "**Do Not Sell or Share My Personal Information**" button below.

[Do Not Sell or Share My Personal Information]

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

You may also submit a request by turning on a recognized opt-out preference signal in your browser or extension. At this time, we recognize the **Global Privacy Control** signal. When you submit an opt-out, the opt-out will only apply to sales and shares from the specific browser from which you sent the signal because the connection between your browser identifier and other personal information we have about you is not known to us.

Authorized Agent

You may also designate an authorized agent to submit such requests on your behalf. Requests must be submitted through the designated methods listed above. Except for opt-out requests, we will require written proof of the agent's permission to do so and may verify your identity directly.

Right to Non-Discrimination

You have the right not to receive discriminatory treatment by us for the exercise of any of your rights.

14. Nevada Privacy Rights

Nevada law (NRS 603A.340) requires each business to establish a designated request address where Nevada consumers may submit requests directing the business not to sell certain kinds of personal information that the business has collected or will collect about the consumer. A sale under Nevada law is the exchange of personal information for monetary consideration by the business to a third party for the third party to license or sell the personal information to other third parties. If you are a Nevada consumer and wish to submit a request relating to our compliance with Nevada law, please submit a request through our online form available here.

15. Colorado, Connecticut, Utah, and Virginia Privacy Rights

These additional rights and disclosures apply only to residents of Colorado, Connecticut, Utah, and Virginia. Terms have the meaning ascribed to them in the Colorado Privacy Act ("**CPA**"), the Connecticut Data Privacy Act ("**CTDPA**"), the Utah Consumer Privacy Act ("**UCPA**"), and the Virginia Consumer Data Protection Act ("**VCDPA**"), as applicable.

You have the following rights under applicable law:

- To confirm whether or not we are processing your personal data.
- To access your personal data.
- To correct inaccuracies in your personal data.
- To delete your personal data.
- To obtain a copy of your personal data that you previously provided to us in a portable and readily usable format.

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

- To opt out of the processing of personal data for purposes of targeted advertising, the sale of personal data, or profiling in furtherance of decisions that produce legal or similarly significant effects concerning you.

To exercise any of these rights, please submit a request through our online form available here. Please note these rights are subject to exceptions. We will respond to your request within 45 days. We may require specific information from you to help us confirm your identity and process your request. If personal data about you has been processed by us as a processor on behalf of a customer and you wish to exercise any rights you have with such personal data, please inquire with our customer directly. If you wish to make your request directly to us, please provide the name of our customer on whose behalf we processed your personal data. We will refer your request to that customer and will support them to the extent required by applicable law in responding to your request.

You also may have the right to opt-out of the processing of personal data for purposes of targeted advertising or the sale of personal data through a recognized opt-out preference signal, such as **Global Privacy Control**. When you submit an opt-out, the opt-out will only apply to the specific browser from which you sent the signal because the connection between your browser identifier and other personal information we have about you is not known to us.

You can designate an authorized agent to submit requests on your behalf. Requests must be submitted through the designated methods listed above. Except for opt-out requests, we will require written proof of the agent's permission to do so and may verify your identity directly.

If we refuse to take action on your request, you may appeal our decision within a reasonable period of time by contacting us at notices@laserfiche.com and specifying you wish to appeal. Within 60 days of our receipt of your appeal, we will inform you in writing of any action taken or not taken in response to the appeal, including a written explanation of the reasons for the decisions. If the appeal is denied, you may submit a complaint as follows:

- For Colorado residents, to the Colorado AG at https://coag.gov/file-complaint/
- For Connecticut residents, to the Connecticut AG at https://www.dir.ct.gov/ag/complaint/
- For Utah residents, to the Utah AG at https://www.attorneygeneral.utah.gov/contact/complaint-form/
- For Virginia residents, to the AG at https://www.oag.state.va.us/consumercomplaintform

16. European Economic Area, Switzerland, and United Kingdom

For the purpose of this Notice, "Europe" means the European Economic Area ("**EEA**"), Switzerland, and the United Kingdom.

Legal basis for processing personal information

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

Laserfiche®

Please see the "How Laserfiche Uses and Discloses the Information We Collect" section above for more details about the purposes for which we process your personal information.

Data protection laws in Europe require a legal basis for processing personal information. Our legal bases include: (a) you have given consent to the processing for one or more specific purposes; (b) processing is necessary for the performance of a contract with you; (c) processing is necessary for compliance with a legal obligation, for example when providing personal information to a law enforcement agency or where we have an accounting or tax obligation; or (d) processing is necessary for the purposes of the legitimate interests pursued by us or a third party, and your interests and fundamental rights and freedoms do not override those interests.

If you are a visitor from Europe, our legal basis for collecting and using the personal information described above will depend on the personal information concerned and the specific context in which we collect it. In rare situations, we may also need to share your personal information with others to protect your vital interests or those of another person.

If we ask you to provide personal information to comply with a legal requirement or to perform a contract with you, we will make this clear at the relevant time and advise you whether the provision of your personal information is mandatory or not (as well as of the possible consequences if you do not provide your personal information).

Similarly, if we collect and use your personal information in reliance on our legitimate interests (or those of any third party), we will make clear to you at the relevant time what those legitimate interests are.

More information about the legal basis on which we rely in connection with each of our processing purposes (described in the section "How Laserfiche Uses and Discloses the Information We Collect" above), is set out below.

Purpose and legal basis for processing

Providing our Services to you

- Necessary for our legitimate interests (successful management of our customer and user relationship, and fulfillment of our contractual or other obligations to you).

Improving and developing our Services

- Necessary for our legitimate interests (to improve and develop our Services in order to deliver high quality Services to customers and users, and to ensure the security and efficiency of our Services).

Providing customer and user support

- Necessary for our legitimate interests (successful management of our customer and user relationship, and to promote our business through the delivery of quality Services).

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

Sending marketing communications

- With your consent, where legally required.
- Necessary for our legitimate interests (promotion of our business and Services to customers and users).

Sending administrative communications

- Necessary for our legitimate interests (continuance of a successful customer and user relationship and to provide quality Services).

Securing our Services

- Necessary for our legitimate interests (providing secure Services, ensuring the security of our networks and systems, and creating trust in our Services).

Complying with our legal obligations

- Necessary for compliance with a legal obligation.
- Necessary for our legitimate interests (complying with legal obligations, regulatory, contractual, or other obligations).

If you have questions or need further information concerning the legal basis on which we collect and use your personal information, please contact us using the contact details provided under the "**How to Contact Us**" heading below.

Your European Privacy Rights

Depending on your location and how you interact with Laserfiche, you may have the following rights regarding the personal information we collect and use about you on our Site and Services:

- **Right of Access**: You have the right to know what personal Information we hold about you, and to obtain a copy of such personal information.
- **Right to Correct**: If you find out that your personal information is inaccurate or incomplete, you can request that we correct it.
- **Right to be forgotten**: You may require that we erase your personal information where certain grounds apply (including where we no longer require the personal information for the purpose for which it was collected or where we relied upon your consent to process the personal information and you have withdrawn that consent, among other things).
- **Right to Restrict**: You have the right to request that we suspend our processing of your personal information if:
    - The accuracy of the personal information is contested;
    - The processing is unlawful, and you oppose the erasure of the personal information and request the restriction of its use instead;
    - Laserfiche no longer needs the personal information for the purposes of processing but is required to keep it for the establishment, exercise, or defense of legal claims; or
    - You have objected to our processing of your personal information (see below) and we are verifying whether you have legitimate ground for such objection.

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

- **Right to complain**: You can contact us at any time if you wish to make a complaint about our processing of your personal information. Additionally, you have the right to complain to a data protection authority.
- **Right to withdraw consent**: Where we process your personal information on the basis of your consent, you may withdraw such consent at any time, and we will no longer process your personal information. Such withdrawal of consent shall not affect the lawfulness of our processing prior to the time that such withdrawal was made but can affect the ability you have to receive our Services (or services provided by third parties) going forward.
- **Right to object**: Where we process your personal information on the basis of legitimate interests you may object to our processing based on grounds relating to your situation. Where we process your personal information for direct marketing purposes you may object at any time, and we will cease our processing for such purposes.
- **Right to data portability**: Where we are processing your personal information on the basis of your consent or pursuant to the performance of a contract with you and such processing is carried out by automated means, you may request to receive your personal information in a commonly used, machine readable format (or have that information transmitted to a third party where technically feasible).

Laserfiche is committed to cooperating and complying with European data protection authorities' advice with respect to any human resources data transferred from Europe in the context of the employment relationship.

To exercise any of these rights, please fill out **this form** or contact us as set out in the "**How to Contact Us**" section below and specify which right you are seeking to exercise. We will respond to your request within a month of receipt of your request. If we require more time, we will inform you of the reason and extension period in writing. We may require additional information from you to allow us to confirm your identity and process your request.

If personal information about you has been processed by us as a processor on behalf of a customer (acting as a controller) and you wish to exercise any rights you have in connection with such personal information, please inquire with our customer directly. If you wish to make your request directly to us, please provide the name of the customer on whose behalf we processed your personal information. We will refer your request to that customer and will support them to the extent required by applicable law in responding to your request.

Data Retention

We will retain your personal information for only so long as we need it in order to fulfil our processing purposes or where we otherwise need to retain it to comply with our legal obligations.

When we have no ongoing legitimate business need or legal reason to process your personal information, we will either delete or anonymize it or, if this is not possible (for example, because your personal information has been stored in backup archives), then we will securely store your personal information and isolate it from any further processing until deletion is possible.

How to Contact Us

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

Laserfiche®

If you have any concerns or questions about the information provided in this "European Economic Area, Switzerland, and United Kingdom" section, please do not hesitate to get in touch with us using the following details:

By mail:

Compulink Management Center, Inc. d/b/a Laserfiche
ATTN: Data Protection Officer
3443 Long Beach Blvd.
Long Beach, CA 90807
USA

By email: notices@laserfiche.com

Data Protection Officer: privacy@laserfiche.com

We are committed to working with you to obtain a resolution of any concern about our privacy practices. If, however, you believe that we have not been able to assist with your concern, you have the right to lodge a complaint with a European data protection authority.

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

STATE OF UTAH COOPERATIVE CONTRACT AMENDMENT

AMENDMENT #: 1

CONTRACT #: AR3109

Starting Date: Unchanged

Expiration Date: Unchanged

TO BE ATTACHED AND MADE PART OF the specified contract by and between the State of Utah Division of Purchasing and Compulink Management Center, Inc. dba Laserfiche (Referred to as CONTRACTOR).

BOTH PARTIES AGREE TO AMEND THE CONTRACT AS FOLLOWS:

The attached Laserfiche Privacy Policy is amended into Attachment E.

Effective Date of Amendment: As of the last signature date below.

All other terms and conditions of the contract, including those previously modified, shall remain in full force and effect.

IN WITNESS WHEREOF, the parties sign and cause this contract to be executed.

CONTRACTOR

DocuSigned by:
Peter Wayman
55434A302F9F438...

1/20/2020

Contractor's Signature — Date

Peter Wayman

Contractor's Name (Print)

Executive Vice Prsident

Title (Print)

STATE OF UTAH

Jan 21, 2020

Director, State of Utah Division of Purchasing — Date

For Division of Purchasing Internal Use			
Purchasing Agent	Phone #	E-mail Address	**Contract #**
Solomon Kingston	801-538-3228	skingston@utah.gov	AR3109

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

Laserfiche Privacy Policy

NOTICE: This Privacy Policy is effective as of January 1, 2020.

Welcome to the Laserfiche.com website (the "Site"). This Site is operated by Compulink Management Center, Inc. doing business as Laserfiche and its affiliates ("Laserfiche", "we", "us", "our"). This Privacy Policy ("Policy") explains how information is collected and used by Laserfiche and how to exercise your privacy rights. We refer to all products and services offered by Laserfiche and the Site, including its content and functionality, as the "Services." We are committed to taking appropriate steps to help protect the privacy of visitors to our Site or users of our Services.

You represent and warrant that you will only provide information and use the Sites and Services acting in your capacity as an employee, owner, director, officer, or contractor of a company, partnership, sole proprietorship, nonprofit or other legal entity, and that your communications and transactions with Laserfiche (on and off the Sites) occur solely within the context of Laserfiche providing the Sites and Services to the company, partnership, sole proprietorship, nonprofit or other legal entity that you represent.

EU data protection law makes a distinction between organizations that process personal data for their own purposes (known as "controllers") and organizations that process personal data on behalf of other organizations (known as "processors"). Laserfiche may act as either a controller or a processor in respect of your personal data, depending on the circumstances.

Laserfiche, located at the address in the section entitled "Contact Us" below, is the controller with respect to information you provide through the Site.

Sometimes Laserfiche operates as a processor on behalf of a customer, a separate legal entity, which is the data controller. For example, Laserfiche provides cloud services to its customers and processes personal data on their behalf to provide those services. This Policy does not describe the processing of such data and we invite you to visit the applicable customer's privacy policy for information about their privacy practices. Any questions that you may have relating to such personal data and your rights under data protection law should therefore be directed to the customer as the controller, not to Laserfiche.

Laserfiche is located in the United States and is certified with the EU-U.S. and Swiss-U.S. Privacy Shield Framework regarding the collection, use, and retention of personal information from the EU and Switzerland in the United States. For more information, please see our "International Transfers and E.U./U.S. Privacy Shield Framework Compliance" heading below.

1. Information We Collect

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

When you visit or use the Site and/or Services, we collect and retain information that you, as a customer or potential customer, provide through the Site or Services, as well as information that is automatically or passively collected from you, your device or your browser.

Information You Provide to Us

We collect information that you provide directly to us for business purposes. For example, when you manage your user profile, participate in interactive features (such as the Contact Us page), request newsletters or other marketing communications, request customer support, provide other information in connection with a job opening, enter login information, or otherwise communicate with us.

The types of information we may collect includes:

- Contact and profile information, including your name, email address, company information, postal address (including zip code), and telephone number;
- Account and log-in information, including your username, password, login details, transaction details;
- Credit card information and transaction details (if applicable);
- Communications to us, for example, reporting a problem or submitting queries, concerns or comments regarding the Site or its content;
- Resume and related data as necessary to consider you for a job opening if you submit an application to us, including your employment history, transcript, writing samples, and references; and
- Any other content or information you choose to provide, including photos you may upload.

If you post information on the Site, including on a bulletin board, or in a chat room or community forum, it becomes generally available to the public. Laserfiche does not control or limit the use by visitors of the Site. By posting information on the Site, you understand that Laserfiche may use the information in connection with its business. Therefore, you should not post any information you consider private or sensitive.

Information We May Collect Automatically

We automatically collect information for business and commercial purposes about your device and how your device interacts with our Site and the Services. We may use Service Providers to collect this information. Some examples of information we collect include the following:

- Information about your visits to the Site and use of the Services, the resources you access, any data you download, and information related to the ways in which you interact with the Site or the Services;
- IP addresses, including the general information in such address, such as city, state and zip code, unique device identifiers, other information about your mobile phone or other mobile device(s), browser types, and browser language;

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

- Referral pages and links, URLs, number of clicks, pages viewed, how long you're on a page, your search queries and results;
- Information about your device, computer and/or browser you use, as well as the device's operating system, such as device hardware model, operating system version, or mobile network information; and
- Data about your device's location, which can be precise (e.g., latitude/longitude data) or imprecise (e.g., location derived from an IP address or data that indicates a city or postal code level).

We use various current – and later – developed technologies to collect this information ("Tracking Technologies"), as further discussed below under the "Cookies and Other Tracking Technologies And Choices Regarding the Same" heading.

Information We Collect from Customers

We provide products and services for our customers, and collect and process information about individuals (including through Tracking Technologies) for business purposes at the direction of our customers ("Customer Data"). Customer Data has historically included contact data, demographic data, content, service use data, device connectivity and configuration data, and location data, among other information. Our processing of Customer Data is governed by the terms of our Cloud Service Agreements with our customers. To the extent we combine Customer Data with information we have collected about you through the Site, we will treat the combined information in accordance with the practices described in this Privacy Policy, plus any additional restrictions imposed by our customers. We are not responsible for how our customers treat the information we collect on their behalf, and we recommend you review their own privacy policies.

Information We Collect From Other Sources

We may obtain information from other third-party sources that we combine with information collected through the Site for business and commercial purposes. These third-party sources vary over time, but have included:

- Data brokers from which we purchase demographic data to supplement the data we collect.
- Social networks when you reference our Service or grant permission to Laserfiche to access your data on one or more of these services.
- Partners with which we offer co-branded services, sell or distribute our products, or engage in joint marketing activities.
- Publicly-available sources such as open government databases or other data in the public domain.

For example, if you log into a social media website through our Site, we may have access to certain information from that website, in accordance with the procedures and practices of that social media site.

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

You should carefully review the privacy policies and terms of use of these third parties.

2. How Laserfiche Uses and Shares the Information We Collect

Laserfiche collects and uses the information you provide in connection with our Site and Services for our business purposes, including to:

- Manage our Site and Services, including your registration and account;
- Perform services requested by you, such as to respond to your comments, questions, and requests, and provide customer service;
- Send you technical notices, updates, security alerts, information regarding changes to our policies, and support and administrative messages;
- Prevent and address fraud, breach of policies or terms, and threats or harm;
- Keep you informed regarding Laserfiche and our software and services;
- Develop and send you direct marketing, including advertisements and communications about our and third-party products, updates, special offers, promotions, rewards, events, and services;
- Help Laserfiche enhance products and services;
- Contact you for market research and to survey your satisfaction with Laserfiche software and services;
- Encourage you to participate in our user groups and invite you to events that may be of interest, including trainings, webinars, and conferences;
- Improve our Site; and
- Analyze information for trends and statistics, which may entail providing this information to an agent acting on Laserfiche's behalf to assist in data analytics.

If you supply Laserfiche with your postal address online, you may receive periodic mailings from us with information on new products and services or upcoming events. If you supply us with your telephone number online, you may receive telephone calls from us with information regarding orders and/or requests you have placed online – such as a software demonstration request or general business inquiry.

If you supply Laserfiche with your email address, you may receive email messages from us for marketing purposes such as providing information on new products and services or upcoming events. We may track when you open our e-mail messages or click on the links contained within them.

You have the right to opt-out of marketing communications we send you at any time. You can exercise this right by clicking on the "unsubscribe" or "opt-out" link in the marketing e-mails we send you. To opt-out of other forms of marketing (such as postal marketing or telemarketing), please contact us using the contact details provided under the "Contact Us" heading below.

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

We also use information about you for commercial purposes with your consent, including to:

- Serve advertising tailored to your interests on our Service and Third-Party Services; and
- Fulfill any other purpose disclosed to you and with your consent.

We may use information that does not identify you (including information that has been de-identified) without obligation to you except as prohibited by applicable law.

Subject to recent changes in the law, which may include a different definition of "sell" from those previously used in this Policy (further discussed below), Laserfiche generally does not sell or rent your information. Laserfiche will disclose information it has about you for our business purposes including, but not limited to, those described as follows:

Sharing with Service Providers

We will occasionally hire other companies or contract with third-party consultants to provide limited services on our behalf. Laserfiche will only provide those companies the information they need to deliver services, and they are prohibited from using that information for any other purpose.

Sharing with Others

We also share information about you as follows:

- Affiliates for Business Purposes. We may share your information with our related entities including our parent and sister companies. For example, we may share your information with our affiliates for customer support, marketing, and technical operations.
- Customers for Business Purposes. We share your information with our customers in connection with us processing your information on their behalf. For example, we share your information with our customers in order to facilitate your orders, maintain and administer your online accounts, respond to your questions and comments, comply with your requests, market and advertise to you, and otherwise comply with applicable law.
- Business Partners for Business and/or Commercial Purposes. We may share your information with our business partners in connection with offering you co-branded services, selling or distributing our products, or engaging in joint marketing activities. For example, we may share information about you with a retailer for purposes of providing you with product support. We may also share your information with approved third parties for marketing purposes; this may include our authorized resellers, user group training partners, and cloud solution providers. We may also share your information with third parties who provide services to assist us with our business activities.
- Promotions. Our promotions may be jointly sponsored or offered by third parties. If you voluntarily choose to enter a promotion, we may share your information with third parties for those commercial purposes as set forth in the official rules that govern the promotion as well as for administrative purposes and as required by law (e.g., on a winners list).

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

- User Group, Training, and Events. Our events may be jointly sponsored or offered by third parties. If you voluntarily sign-up for an event through Laserfiche, we may share your contact details or information that you provide with the sponsor, facility, or any other organization who we schedule you to meet with at that event for commercial purposes in order to fulfill your event registration and/or inform you of future events organized by the sponsor, which we believe you may be interested in.
- Some information about your use of the Site and Services and certain Third Party Services may be collected using Tracking Technologies across time and services and used by us and third parties for business and/or commercial purposes such as to associate different devices you use, and deliver relevant ads and/or other content to you on the Site, Services, and certain Third Party Services, as explained further under the "Cookies and Other Tracking Technologies And Choices Regarding the Same" heading.
- Third Parties. We may share your information with third parties for business purposes of facilitating your requests (such as when you choose to share information with a social network about your activities on the Site or Services) and for commercial purposes in connection with tailoring advertisements, measuring and improving our Service and advertising effectiveness, and enabling other enhancements, subject to your preferences (where applicable).
- Consent or another lawful purpose. We may share your information for any other lawful purpose and/or with your consent.

We will share your information to respond to duly authorized requests from governmental authorities as required by law, or in circumstances in which we believe disclosure is necessary or reasonably appropriate to protect the rights, property, or safety of us or others. Please note that Laserfiche is required to disclose personal information in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.

Some of the hyperlinks on our Site may lead to third-party websites that are not controlled by or affiliated with Laserfiche ("Third Party Services"). These links are provided solely as a convenience to you and not as an endorsement by Laserfiche of the content on such third-party websites. If you use our Services, which include third-party integration(s), such Services are also subject to the terms of use and privacy policy of each applicable third-party entity. For example, Office Online is a Microsoft service and use of Office Online is subject to Microsoft's terms of use and privacy policy. Laserfiche is not responsible for and does not endorse, guarantee or monitor the content, availability, viewpoints, products or services that are offered or expressed on such third-party websites and does not make any representations or warranties regarding the content or accuracy of any content on these third-party websites, including third-party privacy policies. Without limiting the foregoing, in our sole discretion, we may share aggregated information which does not identify you or de-identified information about you with third parties or affiliates for any purpose except as prohibited by applicable law.

Laserfiche also discloses your personal information when: (a) we are required to do so by law, regulation, warrant, subpoena or court order, (b) we are required in urgent circumstances to protect the personal safety of Laserfiche employees, users of Laserfiche products or services, or members of the public, (c) it is necessary to enforce the Terms of Use, or to exercise, establish or defend our legal rights, or (d) such disclosure is part of a sale of all (or substantially all) of the assets of one or more divisions or affiliates of Laserfiche where customer information might be included among the transferred assets.

Laserfiche does not generally sell personal information as the term "sell" is traditionally understood. However, to the extent the California Consumer Privacy Act ("CCPA") is interpreted to include advertising technology activities such as those disclosed below in the Section entitled "Cookies and Other Tracking Technologies And Choices Regarding the Same" as a "sale," Laserfiche will comply with applicable law as to such activity. For more information about how to opt-out of sale of personal information, see the Section below entitled "California Privacy Rights."

3. How We Respond to Do Not Track Signals

Do-Not-Track ("DNT") is a preference that can be set in your browser to notify websites you visit that you do not want them to collect certain information about you. Laserfiche does not respond to DNT signals at this time and will not do so unless and until the law is interpreted to require such response. As discussed in this Policy, we and third parties may track your visits to our Site to provide targeted advertising.

4. Cookies, Other Tracking Technologies, Interest-Based Advertising, And Choices Regarding the Same

Please see our Cookie Statement for information about how we use cookies and similar tracking technologies. In addition to the technologies listed in our Cookie Statement, we use the following to collect information:

- Device Fingerprinting. Device fingerprinting is the process of analyzing and combining sets of information elements from your device's browser, such as JavaScript objects and installed fonts, in order to create a "fingerprint" of your device and uniquely identify your device and apps.

- App Technologies. There are a variety of tracking technologies that may be included in our apps, and these are not browser-based like cookies and cannot be controlled by browser settings. For example, our apps may include third party SDKs, which is code that sends information about your use to a server, and is in effect the app version of a pixel. These SDKs allow us to track our conversions, bring you advertising both on and off the Service, and provide you with additional functionality, such as the ability to connect our Service with your social media account.

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

- Location-Identifying Technologies. GPS, WiFi, Bluetooth, and other location-aware technologies may be used to collect precise location data when you enable location-based services through your device. Location data may be used for purposes such as verifying your device's location and delivering or restricting relevant content and advertising based on that location.

As discussed in our Cookie Statement, we also work with ad serving services, advertisers, and other third parties to serve advertisements on the Site, Services, and/or on Third Party Services. These third parties may use Tracking Technologies on our Sites, Services, and Third Party Services (including in e-mails and advertisements) to track your activities across time and services for purposes of associating the different devices you use, and delivering relevant ads and/or other content to you on the Site, Services, and Third Party Services or third party devices after you have left the Service ("Interest-based Advertising").

We serve ads on and through Third Party Services, such as Facebook, LinkedIn and Google, that are targeted to reach people (or people similar to people) who have visited our Site or are identified in one or more of our databases ("Matched Ads"). This is done by us uploading a customer list to the Third-Party Service or incorporating a pixel from the Third-Party Service on our Site, and the Third-Party Service matching common factors between our data and their data. To opt-out of receiving Matched Ads, please contact the applicable Third-Party Service. If we use Facebook Custom Audiences to serve Matched Ads on Facebook services, you should be able to hover over the box in the right corner of such Facebook ads and find out how to opt-out. We are not responsible for such Third-Party Service's failure to comply with your opt-out instructions.

You can reset your device advertising ID at any time through your device settings, which is designed to allow you to limit the use of information collected about you. For information on how to do this on Apple devices, visit Apple.com. For information on how to do this on Android devices, visit Google.com. You can stop all collection of information via an app by uninstalling the app.

The location data collected through an app depends on your device settings and app permissions. You can exercise choice over the location data collected through our apps by (i) for GPS data, disabling location in your device settings or disabling location permissions to that app; (ii) for Bluetooth data, disabling Bluetooth and any Bluetooth scanning option in your device settings; or (iii) for WiFi data, disabling WiFi and any WiFi scanning option in your device settings. You can stop collection of all location data via an app by uninstalling the app.

Some of the third parties that collect information from or about you on the Site or Services in order to provide more relevant advertising to you participate in the Digital Advertising Alliance ("DAA") Self-Regulatory Program for Online Behavioral Advertising. This program offers a centralized location where users can make choices about the use of their information for online behavioral advertising. To learn more about the DAA and your opt-out options for their members,

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

please visit (i) for website opt-out, http://www.aboutads.info/choices; and (ii) for mobile app opt-out, http://www.aboutads.info/appchoices. In addition, some of these third parties may be members of the Network Advertising Initiative ("NAI"). To learn more about the NAI and your opt-out options for their members, please visit http://www.networkadvertising.org/choices/. Please note that if you opt-out of online behavioral advertising using any of these methods, the opt-out will only apply to the specific browser or device from which you opt-out. Further, opting-out only means that the selected members should no longer deliver certain Interest-based Advertising to you, but does not mean you will no longer receive any targeted content and/or ads (e.g., from other ad networks). We are not responsible for effectiveness of, or compliance with, any third-parties' opt-out options or programs or the accuracy of their statements regarding their programs.

You may also limit our use of information collected from or about your mobile device for purposes of serving online behavioral advertising to you by going to your device settings and selecting "Limit Ad Tracking" (for iOS devices) or "Opt Out of Interest-Based Ads" (for Android devices).

Please be aware that if you disable or remove Tracking Technologies some parts of the Service may not function correctly.

Laserfiche has always considered our advertising technology partners to be Service Providers. However, regulators may interpret newer data protection laws such as the CCPA as characterizing certain kinds of digital advertising activities as "sales." In such an event, Laserfiche will comply with applicable laws in connection with its use of such advertising technology services on its Services.

For further information about the types of Tracking Technologies we use, why, and how you can control such Tracking Technologies, please see our Cookie Statement.

5. Bulletin Boards and Chat Rooms

Occasionally, portions of the Site may allow you to post information that other visitors to the Site will be able to access (i.e., a "bulletin board" or interactive "chat"). If you choose to post information on a bulletin board or through a chat session, it becomes available to the public, and Laserfiche has no ability to control or limit the use of information that is available to the public. Laserfiche and its affiliates will utilize any information you post through the Site in connection with the operation of its business. Laserfiche encourages you not to post any information you consider private or sensitive on the Site. To request removal of your information from such bulletin boards or chat sessions, please contact us using the contact details provided under the "Contact Us" heading below. In some cases, we may not be able to remove your information, in which case we will let you know if we are unable to and why.

6. Your Privacy Rights: Controlling Your Personal Information (Access and Removal)

- You can opt-out of receiving promotional e-mails from us at any time by following the instructions as provided in e-mails to click on the unsubscribe link, or e-mailing us at the e-mail address set forth in the section entitled "Contact Us" below with the word UNSUBSCRIBE in the subject field of the e-mail. Please note that you cannot opt-out of non-promotional e-mails, such as those about your account, transactions, servicing, or Laserfiche's ongoing business relations. To opt-out of other forms of marketing (such as postal marketing or telemarketing), please contact us using the contact details provided under the "Contact Us" heading below.

If you have opted-in to receive push notification on your device, you can opt-out at any time by adjusting the permissions in your device or uninstalling our app.

Please note that your opt-out is limited to the e-mail address, device, and phone number used and will not affect subsequent subscriptions.

California consumers, Nevada consumers, and data subjects in Europe may have additional rights as set forth in the sections entitled "California Privacy Rights," "Nevada Privacy Rights," and "European Privacy Rights" below. For more information about choices regarding Tracking Technologies, see the section on "Cookies and Other Tracking Technologies and Choices Regarding the Same" above.

7. California Privacy Rights

- ### Shine The Light Customer Rights

  Customers in the State of California may request a list of categorized third parties and in some cases affiliates to whom we may have disclosed their personal information specifically for those third parties' and/or affiliates' own marketing purposes, as well as the type of personal information disclosed to those parties. If you are a California resident and would like to request this information, please submit a written request to the email or address provided below. Requests must include "California Privacy Rights Request" in the first line of the description and include your name, street address, city, state, and ZIP code. Please note that we are not required to respond to requests made by means other than through the provided e-mail address or mail address.

- ### California Consumer Rights Under The CCPA

  Right to Know and Delete.

  Consumers who are California residents (and not representatives of businesses, whether those businesses are our customers or others) have the right to know certain information about our data practices in the preceding 12 months. In particular, they have the right to request the following from us:

- The categories of personal information we have collected about them;
- The categories of sources from which the personal information was collected;
- The categories of personal information about them that we disclosed for a business purpose or sold;
- The categories of third parties to whom the personal information was disclosed for a business purpose or sold; and
- The business or commercial purpose for collecting or selling the personal information.

In addition, in certain circumstances California consumers have the right to delete the personal information we have collected from them.

To exercise any of these rights, California consumers should submit a request through our online form available at https://secure1.laserfiche.com/Forms/CCPARequest, email us at privacy@laserfiche.com, or call us at 800-985-8533. In the request, please specify which right you are seeking to exercise and the scope of the request. We will confirm receipt of your request within 10 days. We may require specific information from you to help us verify your identity and process your request. If we are unable to verify your identity, we may deny your requests to know or delete.

If we have processed personal information about you as a service provider on behalf of a customer and you wish to exercise any rights you have with such personal information, please inquire with our customer directly. If you wish to make your request directly to us, please provide the name of our customer on whose behalf we processed your personal information. We will refer your request to that customer, and will support them to the extent required by applicable law in responding to your request.

Do Not Sell My Personal Information.

Laserfiche will always seek your affirmative direction/consent to intentionally disclose personal information to third parties in ways that might otherwise be construed to be a "sale" under the CCPA.

8. Nevada Privacy Rights

Nevada law (NRS 603A.340) requires each business to establish a designated request address where Nevada consumers may submit requests directing the business not to sell certain kinds of personal information that the business has collected or will collect about the consumer. A sale under Nevada law is the exchange of personal information for monetary consideration by the business to a third party for the third party to license or sell the personal information to other third parties. If you are a Nevada consumer and wish to submit a request relating to our compliance with Nevada law, please contact us at Nevadarequests@laserfiche.com.

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

9. European Privacy Rights

If you are a data subject located in the European Economic Area ("EEA"), you may have the right to access, rectify, or erase personal data we have collected about you through the Site or Services. You may also have the right to data portability and the right to restrict or object to our processing of personal data we have collected about you through the Site or Services. In addition, you have the right to ask us not to process your personal data (or provide it to third parties to process) for marketing purposes or purposes materially different than for which it was originally collected or subsequently authorized by you. You may withdraw your consent at any time for any data processing we do based on consent you have provided to us. Withdrawing your consent will not affect the lawfulness of any processing we conducted prior to your withdrawal, nor will it affect processing of your personal information conducted in reliance on lawful processing grounds other than consent.

To exercise any of these rights, contact us as set forth in the section entitled "Contact Us" below and specify which right you intend to exercise. We will respond to your request within 30 days. We may require additional information from you to allow us to confirm your identity.

If your information has been processed by us on behalf of a customer and you wish to exercise any rights you have with such information, please inquire with our customer directly.

If you have any issues with our compliance, you have the right to lodge a complaint with a European supervisory authority.

10. Legal Basis For Processing Personal Information (EEA visitors only)

If you are a visitor from the EEA, our legal basis for collecting and using the personal information described above will depend on the personal information concerned and the specific context in which we collect it.

However, we will normally collect personal information from you only where we have your consent to do so, where we need the personal information to perform a contract with you, or where the processing is in our legitimate interests and not overridden by your data protection interests or fundamental rights and freedoms. In some cases, we may also have a legal obligation to process personal data about you, for example when providing personal data to a law enforcement agency or where we have an accounting or tax obligation. In rare situations, we may also need to share your personal data with others to protect your vital interests or those of another person.

If we ask you to provide personal information to comply with a legal requirement or to perform a contract with you, we will make this clear at the relevant time and advise you whether the provision of your personal information is mandatory or not (as well as of the possible consequences if you do not provide your personal information).

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

Similarly, if we collect and use your personal information in reliance on our legitimate interests (or those of any third party), we will make clear to you at the relevant time what those legitimate interests are.

If you have questions about or need further information concerning the legal basis on which we collect and use your personal information, please contact us using the contact details provided under the "Contact Us" heading below.

11. International Transfers and E.U./U.S. Privacy Shield Framework Compliance

Your personal information may be transferred to, and processed in, countries other than the country in which you are resident. These countries may have data protection laws that are different to the laws of your country.

Specifically, Laserfiche is headquartered in the USA, our data centers are located in the USA and Canada, and our group companies and third-party service providers and partners operate around the world. This means that when we collect your personal information we may process it in any of these countries.

However, we have taken appropriate safeguards to require that your personal information will remain protected in accordance with this Policy. These include certifying with the Privacy Shield Framework discussed below.

Laserfiche complies with the EU-U.S. Privacy Shield Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information transferred from the European Union to the United States. Laserfiche has certified to the Department of Commerce that it adheres to the Privacy Shield Principles ("Principles"). If there is any conflict between the terms in this Policy and the Privacy Shield Principles, the Privacy Shield Principles shall govern. To learn more about the Privacy Shield program, and to view our certification, please visit https://www.privacyshield.gov/.

Laserfiche's responsibility for data it receives pursuant to the Privacy Shield and subsequent transfers of that data to third parties is detailed in the Privacy Shield Principles. Laserfiche complies with the Principles for all onward transfers from the EU, including the onward transfer liability provisions. Laserfiche remains responsible under the Principles for third-party agents processing personal data on its behalf.

With respect to personal information received or transferred pursuant to the Privacy Shield Frameworks, we are subject to the regulatory enforcement powers of the U.S. Federal Trade Commission. In certain situations, we may be required to disclose personal information in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

Laserfiche commits to resolving complaints about your privacy and our collection and use of your personal information within 45 days of receiving your complaint. Individuals with questions or complaints regarding this Privacy Policy should first submit inquiries by contacting us using the contact details provided under the "Contact Us" heading below. Laserfiche has further committed to refer unresolved Privacy Shield complaints to the American Arbitration Association, an alternative dispute resolution provider located in the United States. If you do not receive timely acknowledgment of your complaint from us, or if we have not resolved your complaint, please contact or visit the American Arbitration Association for more information or to file a complaint. When filing by mail or email, please complete the appropriate Privacy Shield Program Notice of Arbitration Form located in the link below and forward to the International Centre for Dispute Resolution.

International Centre for Dispute Resolution Case Filing Services
1101 Laurel Oak Road, Suite 100
Voorhees, NJ 08043
United States
Phone: +1.212.484.4181
Email box: casefiling@adr.org

For any questions or for further information about this program, the ICDR's International Arbitration Rules, or with additional language versions of the ICDR's International Arbitration Rules, please contact the International Centre for Dispute Resolution at +1.212.484.4181 or by visiting the website http://go.adr.org/privacyshield.html. The services of the American Arbitration Association are provided at no cost to you.

Under certain limited circumstances, data subjects, as defined by the Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016, of the European Union, may invoke binding Privacy Shield arbitration as a last resort if all other forms of dispute resolution have been unsuccessful. To learn more about this method of resolution and its availability to you, please visit https://www.privacyshield.gov/.

12. Security Measures

We have implemented industry standard controls, intrusion detection network monitoring, and reasonable security measures designed to protect the personal information that you submit through the Services and Site. These measures include physical access controls, access authorization controls, and firewalls. We also periodically review our information collection, storage, and processing practices to help prevent loss, misuse, unauthorized access, alteration or other destruction of information we collect. When accessing secure sections of the Site, we use Transport Layer Security (TLS) encryption to secure the communication of information passing between your browser and our servers. Additionally, only authorized administrators, Laserfiche employees and third-party contractors have access to systems containing such information.

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

Nevertheless, transmission via the internet is not completely secure and we cannot guarantee the security of your information.

13. Privacy of Children

The Site and Services are intended for a general audience and not directed to children under sixteen (16) years of age. We do not market products or services to children, and we do not knowingly collect personal information from children at any time, including as defined by the U.S. Children's Privacy Protection Act ("COPPA") or personal information as defined under the CCPA from anyone under the age of 16 without verification of consent. If you are under the age of 16, please do not provide personal information of any kind whatsoever and please do not use Laserfiche Site and Services or participate in Laserfiche's surveys, contests, events, and other promotions. If you are a parent or guardian and believe Laserfiche has collected such information without parental consent, please contact us as set forth in the section entitled "Contact Us" below and we will remove such data to the extent required by COPPA or other applicable law.

14. Data Retention

We retain personal information we collect from you where we have an ongoing legitimate business need to do so (for example, to provide you with a service you have requested or to comply with applicable legal, tax or accounting requirements).

15. Privacy Policy Changes

Laserfiche may change this Privacy Policy at any time. When we update this Policy, we take appropriate measures to inform you, consistent with the significance of the changes we make. We will obtain your consent to any material changes if and where this is required by applicable data protection laws. You can see when this Policy was last updated by checking the "effective" date displayed at the top of this Policy. Laserfiche recommends that you review this Privacy Policy regularly for any revisions. Your continued use of the Site or Services after such revisions will constitute your acknowledgement of the amended Policy.

16. Contact Us

If you have any comments or questions regarding our Privacy Policy, or want to exercise your data protection rights, please send a message to:

Compulink Management Center, Inc. d/b/a Laserfiche
ATTN: Data Protection Officer
3545 Long Beach Blvd.
Long Beach, CA 90807
USA
notices@laserfiche.com

For EU-specific requests, you can reach our Data Protection Officer ("DPO") at privacy@laserfiche.com.

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

Contract #: AR3109

STATE OF UTAH COOPERATIVE CONTRACT

1. CONTRACTING PARTIES: This contract is between the Utah Division of Purchasing and the following Contractor:

Compulink Management Center, Inc. dba Laserfiche
Name

3545 Long Beach Blvd
Street Address

Long Beach	CA	90807
City	*State*	*Zip*

Vendor # VC226574 Commodity Code #: 920-05 Legal Status of Contractor: For-Profit Corporation

Contact *Name:* Brigitte Meiselman *Phone Number:* 1-562-988-1688 ext. 138 *Email:* brigitte.meiselman@laserfiche.com

2. CONTRACT PORTFOLIO NAME: Cloud Solutions.

3. GENERAL PURPOSE OF CONTRACT: Provide Cloud Solutions under the service models awarded in Attachment B.

4. PROCUREMENT: This contract is entered into as a result of the procurement process on FY2018, Solicitation# SK18008

5. CONTRACT PERIOD: Effective Date: Wednesday, July 31, 2019. Termination Date: Tuesday, September 15, 2026 unless terminated early or extended in accordance with the terms and conditions of this contract.

6. Administrative Fee: Contractor shall pay to NASPO ValuePoint, or its assignee, a NASPO ValuePoint Administrative Fee of one-quarter of one percent (0.25% or 0.0025) of contract sales no later than 60 days following the end of each calendar quarter. The NASPO ValuePoint Administrative Fee shall be submitted quarterly and is based on sales of the Services.

7. ATTACHMENT A: NASPO ValuePoint Master Terms and Conditions, including the attached Exhibits
ATTACHMENT B: Scope of Services Awarded to Contractor
ATTACHMENT C: Pricing Discounts and Schedule
ATTACHMENT D: Contractor's Response to Solicitation # SK18008
ATTACHMENT E: Service Offering EULAs, SLAs

Any conflicts between Attachment A and the other Attachments will be resolved in favor of Attachment A.

9. DOCUMENTS INCORPORATED INTO THIS CONTRACT BY REFERENCE BUT NOT ATTACHED:
a. All other governmental laws, regulations, or actions applicable to the goods and/or services authorized by this contract.
b. Utah Procurement Code, Procurement Rules, and Contractor's response to solicitation #SK18008.

10. Each signatory below represents that he or she has the requisite authority to enter into this contract.

IN WITNESS WHEREOF, the parties sign and cause this contract to be executed. Notwithstanding verbal or other representations by the parties, the "Effective Date" of this Contract shall be the date provided within Section 5 above.

CONTRACTOR

Contractor's signature — Date: 8/1/2019

PETER WAYMAN, E.V.P.
Type or Print Name and Title

DIVISION OF PURCHASING

Director, Division of Purchasing — Date: Aug 5, 2019

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

Note: Exceptions negotiated on sections 2, 8, 13, 25, 26, 46, 47, and 48.



Attachment A: NASPO ValuePoint Master Agreement Terms and Conditions

1. Master Agreement Order of Precedence

a. Any Order placed under this Master Agreement shall consist of the following documents:

(1) A Participating Entity's Participating Addendum[1] ("PA");
(2) NASPO ValuePoint Master Agreement Terms & Conditions, including the applicable Exhibits[2] to the Master Agreement;
(3) The Solicitation;
(4) Contractor's response to the Solicitation, as revised (if permitted) and accepted by the Lead State; and
(5) A Service Level Agreement issued against the Participating Addendum.

b. These documents shall be read to be consistent and complementary. Any conflict among these documents shall be resolved by giving priority to these documents in the order listed above. Contractor terms and conditions that apply to this Master Agreement are only those that are expressly accepted by the Lead State and must be in writing and attached to this Master Agreement as an Exhibit or Attachment.

2. Definitions - Unless otherwise provided in this Master Agreement, capitalized terms will have the meanings given to those terms in this Section.

Confidential Information means any and all information of any form that is marked as confidential or would by its nature be deemed confidential obtained by Contractor, Purchasing Entity, or any of their respective employees or agents in the performance of this Master Agreement, including, but not necessarily limited to (1) any Purchasing Entity's records, (2) personnel records, (3) information concerning individuals, is confidential information of Purchasing Entity, and (4) any proprietary information of Contractor utilized in procuring, maintaining or providing the Product.

Contractor means the person or entity providing solutions under the terms and conditions set forth in this Master Agreement. Contractor also includes its employees, subcontractors, agents and affiliates who are providing the services agreed to under the Master Agreement.

[1] A Sample Participating Addendum will be published after the contracts have been awarded.
[2] The Exhibits comprise the terms and conditions for the service models: PaaS, IaaS, and PaaS.

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

Data means all information, whether in oral or written (including electronic) form, created by or in any way originating with a Participating Entity or Purchasing Entity, and all information that is the output of any computer processing, or other electronic manipulation, of any information that was created by or in any way originating with a Participating Entity or Purchasing Entity, in the course of using and configuring the Services provided under this Agreement.

Data Breach means any actual or reasonably suspected non-authorized access to or acquisition of computerized Non-Public Data or Personal Data that compromises the security, confidentiality, or integrity of the Non-Public Data or Personal Data, or the ability of Purchasing Entity to access the Non-Public Data or Personal Data.

Data Categorization means the process of risk assessment of Data. See also “High Risk Data”, “Moderate Risk Data” and “Low Risk Data”.

Disabling Code means computer instructions or programs, subroutines, code, instructions, data or functions, (including but not limited to viruses, worms, date bombs or time bombs), including but not limited to other programs, data storage, computer libraries and programs that self-replicate without manual intervention, instructions programmed to activate at a predetermined time or upon a specified event, and/or programs purporting to do a meaningful function but designed for a different function, that alter, destroy, inhibit, damage, interrupt, interfere with or hinder the operation of the Purchasing Entity’s’ software, applications and/or its end users processing environment, the system in which it resides, or any other software or data on such system or any other system with which it is capable of communicating.

Fulfillment Partner means a third-party contractor qualified and authorized by Contractor, and approved by the Participating State under a Participating Addendum, who may, to the extent authorized by Contractor, fulfill any of the requirements of this Master Agreement including but not limited to providing Services under this Master Agreement and billing Customers directly for such Services. Contractor may, upon written notice to the Participating State, add or delete authorized Fulfillment Partners as necessary at any time during the contract term. Fulfillment Partner has no authority to amend this Master Agreement or to bind Contractor to any additional terms and conditions.

High Risk Data is as defined in FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems (“High Impact Data”).

Infrastructure as a Service (IaaS) as used in this Master Agreement is defined the capability provided to the consumer to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications; and possibly limited

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

control of select networking components (e.g., host firewalls).

Intellectual Property means any and all patents, copyrights, service marks, trademarks, trade secrets, trade names, patentable inventions, or other similar proprietary rights, in tangible or intangible form, and all rights, title, and interest therein.

Lead State means the State centrally administering the solicitation and any resulting Master Agreement(s).

Low Risk Data is as defined in FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems ("Low Impact Data").

Master Agreement means this agreement executed by and between the Lead State, acting on behalf of NASPO ValuePoint, and the Contractor, as now or hereafter amended.

Moderate Risk Data is as defined in FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems ("Moderate Impact Data").

NASPO ValuePoint is the NASPO ValuePoint Cooperative Purchasing Program, facilitated by the NASPO Cooperative Purchasing Organization LLC, a 501(c)(3) limited liability company (doing business as NASPO ValuePoint) is a subsidiary organization the National Association of State Procurement Officials (NASPO), the sole member of NASPO ValuePoint. The NASPO ValuePoint Cooperative Purchasing Organization facilitates administration of the cooperative group contracting consortium of state chief procurement officials for the benefit of state departments, institutions, agencies, and political subdivisions and other eligible entities (i.e., colleges, school districts, counties, cities, some nonprofit organizations, etc.) for all states and the District of Columbia. The NASPO ValuePoint Cooperative Development Team is identified in the Master Agreement as the recipient of reports and may be performing contract administration functions as assigned by the Lead State.

Non-Public Data means High Risk Data and Moderate Risk Data that is not subject to distribution to the public as public information. It is deemed to be sensitive and confidential by the Purchasing Entity because it contains information that is exempt by statute, ordinance or administrative rule from access by the general public as public information.

Participating Addendum means a bilateral agreement executed by a Contractor and a Participating Entity incorporating this Master Agreement and any other additional Participating Entity specific language or other requirements, e.g. ordering procedures specific to the Participating Entity, other terms and conditions.

Participating Entity means a state, or other legal entity, properly authorized to enter into a Participating Addendum.

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

Participating State means a state, the District of Columbia, or one of the territories of the United States that is listed in the Request for Proposal as intending to participate. Upon execution of the Participating Addendum, a Participating State becomes a Participating Entity.

Personal Data means data alone or in combination that includes information relating to an individual that identifies the individual by name, identifying number, mark or description can be readily associated with a particular individual and which is not a public record. Personal Information may include the following personally identifiable information (PII): government-issued identification numbers (e.g., Social Security, driver's license, passport); financial account information, including account number, credit or debit card numbers; or Protected Health Information (PHI) relating to a person.

Platform as a Service (PaaS) as used in this Master Agreement is defined as the capability provided to the consumer to deploy onto the cloud infrastructure consumer-created or -acquired applications created using programming languages and tools supported by the provider. This capability does not necessarily preclude the use of compatible programming languages, libraries, services, and tools from other sources. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.

Product means any deliverable under this Master Agreement, including Services, software, and any incidental tangible goods.

Protected Health Information (PHI) means individually identifiable health information transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium. PHI excludes education records covered by the Family Educational Rights and Privacy Act (FERPA), as amended, 20 U.S.C. 1232g, records described at 20 U.S.C. 1232g(a)(4)(B)(iv) and employment records held by a covered entity in its role as employer. PHI may also include information that is a subset of health information, including demographic information collected from an individual, and (1) is created or received by a health care provider, health plan, employer or health care clearinghouse; and (2) relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and (a) that identifies the individual; or (b) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Purchasing Entity means a state, city, county, district, other political subdivision of a State, and a nonprofit organization under the laws of some states if authorized by a Participating Addendum, who issues a Purchase Order against the Master Agreement and becomes financially committed to the purchase.

Services mean any of the specifications described in the Scope of Services that are supplied or created by the Contractor pursuant to this Master Agreement.

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

Security Incident means the possible or actual unauthorized access to a Purchasing Entity's Non-Public Data and Personal Data the Contractor believes could reasonably result in the use, disclosure or theft of a Purchasing Entity's Non-Public Data within the possession or control of the Contractor. A Security Incident also includes a major security breach to the Contractor's system, regardless if Contractor is aware of unauthorized access to a Purchasing Entity's Non-Public Data. A Security Incident may or may not turn into a Data Breach.

Service Level Agreement (SLA) means a written agreement between both the Purchasing Entity and the Contractor that is subject to the terms and conditions in this Master Agreement and relevant Participating Addendum unless otherwise expressly agreed in writing between the Purchasing Entity and the Contractor. SLAs should include: (1) the technical service level performance promises, (i.e. metrics for performance and intervals for measure), (2) description of service quality, (3) identification of roles and responsibilities, (4) remedies, such as credits, and (5) an explanation of how remedies or credits are calculated and issued.

Software as a Service (SaaS) as used in this Master Agreement is defined as the capability provided to the consumer to use the Contractor's applications running on a Contractor's infrastructure (commonly referred to as 'cloud infrastructure). The applications are accessible from various client devices through a thin client interface such as a Web browser (e.g., Web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

Solicitation means the documents used by the State of Utah, as the Lead State, to obtain Contractor's Proposal.

Statement of Work means a written statement in a solicitation document or contract that describes the Purchasing Entity's service needs and expectations.

3. Term of the Master Agreement: Unless otherwise specified as a shorter term in a Participating Addendum, the term of the Master Agreement will run from contract execution to September 15, 2026.

4. Amendments: The terms of this Master Agreement shall not be waived, altered, modified, supplemented or amended in any manner whatsoever without prior written approval of the Lead State and Contractor.

5. Assignment/Subcontracts: Contractor shall not assign, sell, transfer, or sublet rights, or delegate responsibilities under this Master Agreement, in whole or in part, without the prior written approval of the Lead State.

The Lead State reserves the right to assign any rights or duties, including written assignment of contract administration duties to the NASPO Cooperative Purchasing

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

Organization LLC, doing business as NASPO ValuePoint.

6. Discount Guarantee Period: All discounts must be guaranteed for the entire term of the Master Agreement. Participating Entities and Purchasing Entities shall receive the immediate benefit of price or rate reduction of the services provided under this Master Agreement. A price or rate reduction will apply automatically to the Master Agreement and an amendment is not necessary.

7. Termination: Unless otherwise stated, this Master Agreement may be terminated by either party upon 60 days written notice prior to the effective date of the termination. Further, any Participating Entity may terminate its participation upon 30 days written notice, unless otherwise limited or stated in the Participating Addendum. Termination may be in whole or in part. Any termination under this provision shall not affect the rights and obligations attending orders outstanding at the time of termination, including any right of any Purchasing Entity to indemnification by the Contractor, rights of payment for Services delivered and accepted, data ownership, Contractor obligations regarding Purchasing Entity Data, rights attending default in performance an applicable Service Level of Agreement in association with any Order, Contractor obligations under Termination and Suspension of Service, and any responsibilities arising out of a Security Incident or Data Breach. Termination of the Master Agreement due to Contractor default may be immediate.

8. Confidentiality, Non-Disclosure, and Injunctive Relief

a. Confidentiality. Each of Contractor and Purchasing Entity acknowledges that it and any of their respective employees or agents may, in the course of providing a Product under this Master Agreement, be exposed to or acquire information that is confidential to Purchasing Entity's or Purchasing Entity's clients or to Contractor. For purposes of this Agreement, "Discloser" refers to the party that discloses Confidential Information to the other party, and "Recipient" refers to the party that receives the information. Any reports or other documents or items (including software) that result from the use of the Confidential Information by Contractor or Purchasing Entity shall be treated in the same manner as the Confidential Information. Confidential Information does not include information that (1) is or becomes (other than by disclosure by Discloser) publicly known; (2) is furnished by Discloser to others without restrictions similar to those imposed by this Master Agreement; (3) is rightfully in Recipient's possession without the obligation of nondisclosure prior to the time of its disclosure under this Master Agreement; (4) is obtained from a source other than Discloser without the obligation of confidentiality, (5) is disclosed with the written consent of Discloser or; (6) is independently developed by employees, agents or subcontractors of Recipient who can be shown to have had no access to the Confidential Information.

b. Non-Disclosure. Contractor and Purchasing Entity shall hold Confidential Information in confidence, using at least the industry standard of confidentiality, and shall not copy, reproduce, sell, assign, license, market, transfer or otherwise dispose of, give, or disclose Confidential Information to third parties or use Confidential Information for any purposes whatsoever other than what is necessary to the performance of Orders placed under this Master Agreement. Contractor and Purchasing Entity shall advise each of its

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

employees and agents of their obligations to keep Confidential Information confidential. Contractor shall use commercially reasonable efforts to assist Discloser in identifying and preventing any unauthorized use or disclosure of any Confidential Information. Without limiting the generality of the foregoing, Recipient shall advise Discloser, applicable Participating Entity, and the Lead State immediately if Recipient learns or has reason to believe that any person who has had access to Confidential Information has violated or intends to violate the terms of this Master Agreement, and Recipient shall at its expense cooperate with Discloser in seeking injunctive or other equitable relief in the name of Discloser or Recipient against any such person. Except as directed by Discloser, Recipient will not at any time during or after the term of this Master Agreement disclose, directly or indirectly, any Confidential Information to any person, except in accordance with this Master Agreement, and that upon Discloser's request, Recipient shall turn over to Discloser all documents, papers, and other matter in Recipient's possession that embody Confidential Information. Notwithstanding the foregoing, Recipient may keep one copy of such Confidential Information necessary for quality assurance, audits and evidence of the performance of this Master Agreement.

c. Injunctive Relief. Contractor and Purchasing Entity acknowledge that breach of this section, including disclosure of any Confidential Information, will cause irreparable injury to Discloser that is inadequately compensable in damages. Accordingly, Discloser may seek and obtain injunctive relief against the breach or threatened breach of the foregoing undertakings, in addition to any other legal remedies that may be available. Recipient acknowledges and agrees that the covenants contained herein are necessary for the protection of the legitimate business interests of Discloser and are reasonable in scope and content.

d. Purchasing Entity Law. These provisions shall be applicable only to extent they are not in conflict with the applicable public disclosure laws of any Purchasing Entity.

9. Right to Publish: Throughout the duration of this Master Agreement, Contractor must secure prior approval from the Lead State or Participating Entity for the release of any information that pertains to the potential work or activities covered by the Master Agreement , including but not limited to reference to or use of the Lead State or a Participating Entity's name, Great Seal of the State, Coat of Arms, any Agency or other subunits of the State government, or any State official or employee, for commercial promotion which is strictly prohibited. News releases or release of broadcast e-mails pertaining to this Master Agreement or Participating Addendum shall not be made without prior written approval of the Lead State or a Participating Entity.

The Contractor shall not make any representations of NASPO ValuePoint's opinion or position as to the quality or effectiveness of the services that are the subject of this Master Agreement without prior written consent. Failure to adhere to this requirement may result in termination of the Master Agreement for cause.

10. Defaults and Remedies

a. The occurrence of any of the following events shall be an event of default under this Master Agreement:

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

(1) Nonperformance of contractual requirements; or

(2) A material breach of any term or condition of this Master Agreement; or

(3) Any certification, representation or warranty by Contractor in response to the solicitation or in this Master Agreement that proves to be untrue or materially misleading; or

(4) Institution of proceedings under any bankruptcy, insolvency, reorganization or similar law, by or against Contractor, or the appointment of a receiver or similar officer for Contractor or any of its property, which is not vacated or fully stayed within thirty (30) calendar days after the institution or occurrence thereof; or

(5) Any default specified in another section of this Master Agreement.

b. Upon the occurrence of an event of default, Lead State shall issue a written notice of default, identifying the nature of the default, and providing a period of 30 calendar days in which Contractor shall have an opportunity to cure the default. The Lead State shall not be required to provide advance written notice or a cure period and may immediately terminate this Master Agreement in whole or in part if the Lead State, in its sole discretion, determines that it is reasonably necessary to preserve public safety or prevent immediate public crisis. Time allowed for cure shall not diminish or eliminate Contractor's liability for damages.

c. If Contractor is afforded an opportunity to cure and fails to cure the default within the period specified in the written notice of default, Contractor shall be in breach of its obligations under this Master Agreement and Lead State shall have the right to exercise any or all of the following remedies:

(1) Exercise any remedy provided by law; and

(2) Terminate this Master Agreement and any related Contracts or portions thereof; and

(3) Suspend Contractor from being able to respond to future bid solicitations; and

(4) Suspend Contractor's performance; and

(5) Withhold payment until the default is remedied.

d. Unless otherwise specified in the Participating Addendum, in the event of a default under a Participating Addendum, a Participating Entity shall provide a written notice of default as described in this section and have all of the rights and remedies under this paragraph regarding its participation in the Master Agreement, in addition to those set forth in its Participating Addendum. Nothing in these Master Agreement Terms and Conditions shall be construed to limit the rights and remedies available to a Purchasing Entity under the applicable commercial code.

11. Changes in Contractor Representation: The Contractor must notify the Lead State of changes in the Contractor's key administrative personnel, in writing within 10 calendar days of the change. The Lead State reserves the right to approve changes in key personnel, as identified in the Contractor's proposal. The Contractor agrees to propose replacement key personnel having substantially equal or better education, training, and

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

experience as was possessed by the key person proposed and evaluated in the Contractor's proposal.

12. Force Majeure: Neither party shall be in default by reason of any failure in performance of this Contract in accordance with reasonable control and without fault or negligence on their part. Such causes may include, but are not restricted to, acts of nature or the public enemy, acts of the government in either its sovereign or contractual capacity, fires, floods, epidemics, quarantine restrictions, strikes, freight embargoes and unusually severe weather, but in every case the failure to perform such must be beyond the reasonable control and without the fault or negligence of the party.

13. Indemnification

a. The Contractor shall defend, indemnify and hold harmless NASPO, NASPO ValuePoint, the Lead State, Participating Entities, and Purchasing Entities, along with their officers, agents, and employees as well as any person or entity for which they may be liable, from and against claims, damages or causes of action including reasonable attorneys' fees and related costs for any death, injury, or damage to property arising directly or indirectly from act(s), error(s), or omission(s) of the Contractor, its employees or subcontractors or volunteers, at any tier, relating to the performance under the Master Agreement.

b. Indemnification – Intellectual Property. The Contractor shall defend, indemnify and hold harmless NASPO, NASPO ValuePoint, the Lead State, Participating Entities, Purchasing Entities, along with their officers, agents, and employees as well as any person or entity for which they may be liable ("Indemnified Party"), from and against claims, damages or causes of action including reasonable attorneys' fees and related costs arising out of the claim that the Product or its use, infringes Intellectual Property rights ("Intellectual Property Claim") of another person or entity based on the following terms and conditions:

(1) The Contractor's obligations under this section shall not extend to any claims arising from the combination, modification, alteration, integration or reconfiguration of the Product with any other product, system or method, unless the Product, system or method is:

(a) provided and installed by the Contractor or the Contractor's subsidiaries or affiliates;

(b) specified by the Contractor in writing to work with the Product; or

(c) reasonably required, in order to use the Product in its intended manner, and the infringement could not have been avoided by substituting another reasonably available product, system or method capable of performing the same function.

.

(2) The Contractor's obligations under this section shall also not extend to any

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

claims arising from:

(a) Indemnified Party's breach of the Master Agreement or any Participating Addendum; or

(b) any conduct, act or omission by non-Contractor employees that is not authorized or approved by Contractor; or

(c) Participating Entity's Data, or the incorporation or interaction of such Data in or with the Product if the claim would not have arisen but for Participating Entity's Data or the incorporation or interaction of such Data in or with the Product.

(3) The Indemnified Party shall notify the Contractor within a reasonable time after receiving notice of an Intellectual Property Claim. Even if the Indemnified Party fails to provide reasonable notice, the Contractor shall not be relieved from its obligations unless the Contractor can demonstrate that it was prejudiced in defending the Intellectual Property Claim resulting in increased expenses or loss to the Contractor and then only to the extent of the prejudice or expenses. If the Contractor promptly and reasonably investigates and defends any Intellectual Property Claim, it shall have control over the defense and settlement of it. However, the Indemnified Party must consent in writing for any money damages or obligations for which it may be responsible. The Indemnified Party shall furnish, at the Contractor's reasonable request and expense, information and assistance necessary for such defense. If the Contractor fails to vigorously pursue the defense or settlement of the Intellectual Property Claim, the Indemnified Party may assume the defense or settlement of it and the Contractor shall be liable for all costs and expenses, including reasonable attorneys' fees and related costs, incurred by the Indemnified Party in the pursuit of the Intellectual Property Claim. Unless otherwise agreed in writing, this section is not subject to any limitations of liability in this Master Agreement or in any other document executed in conjunction with this Master Agreement.

(4) If the Product becomes, or in Contractor's opinion is likely to become, the subject of an infringement claim, or if Contractor is enjoined or, in Contractor's opinion is likely to be enjoined, from making available any Product, Contractor may, at its option and expense, either (a) procure for Participating Entity the right to continue exercising the rights licensed hereunder with respect to the Product; (b) replace or modify the Product so that it becomes non-infringing; (c) refund to Participating Entity any fees paid in advance by it for any unused portion of the then-current subscription term for the Product, whereupon Contractor may terminate the applicable subscription upon writtten notice to Participating Entity. Section 13(b) states Contractor's entire liability and Participating Entity's sole and exclusive remedy for infringement claims and actions.

c. If Contractor is only partially responsible for, or the cause of, a loss for which Contractor demands indemnification, Contractor's obligation to indemnify and defend Indemnified Party will be based on principles of comparative equitable indemnification.

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

Therefore, the loss will be equitably apportioned to Contractor based on Contractor's proportionate share of responsibility for the total loss suffered by the injured party.

14. Independent Contractor: The Contractor shall be an independent contractor. Contractor shall have no authorization, express or implied, to bind the Lead State, Participating States, other Participating Entities, or Purchasing Entities to any agreements, settlements, liability or understanding whatsoever, and agrees not to hold itself out as agent except as expressly set forth herein or as expressly agreed in any Participating Addendum.

15. Individual Customers: Except to the extent modified by a Participating Addendum, each Purchasing Entity shall follow the terms and conditions of the Master Agreement and applicable Participating Addendum and will have the same rights and responsibilities for their purchases as the Lead State has in the Master Agreement, including but not limited to, any indemnity or right to recover any costs as such right is defined in the Master Agreement and applicable Participating Addendum for their purchases. Each Purchasing Entity will be responsible for its own charges, fees, and liabilities. The Contractor will apply the charges and invoice each Purchasing Entity individually.

16. Insurance

a. Unless otherwise agreed in a Participating Addendum, Contractor shall, during the term of this Master Agreement, maintain in full force and effect, the insurance described in this section. Contractor shall acquire such insurance from an insurance carrier or carriers licensed to conduct business in each Participating Entity's state and having a rating of A-, Class VII or better, in the most recently published edition of Best's Reports. Failure to buy and maintain the required insurance may result in this Master Agreement's termination or, at a Participating Entity's option, result in termination of its Participating Addendum.

b. Coverage shall be written on an occurrence basis. The minimum acceptable limits shall be as indicated below, with no deductible for each of the following categories:

(1) Commercial General Liability covering premises operations, independent contractors, products and completed operations, blanket contractual liability, personal injury (including death), advertising liability, and property damage, with a limit of not less than $1 million per occurrence/$3 million general aggregate;

(2) CLOUD MINIMUM INSURANCE COVERAGE:

Level of Risk	**Data Breach and Privacy/Cyber Liability including Technology Errors and Omissions** Minimum Insurance Coverage
Low Risk Data	$2,000,000
Moderate Risk Data	$5,000,000
High Risk Data	$10,000,000

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

(3) Contractor must comply with any applicable State Workers Compensation or Employers Liability Insurance requirements.

(4) Professional Liability. As applicable, Professional Liability Insurance Policy in the minimum amount of $1,000,000 per occurrence and $1,000,000 in the aggregate, written on an occurrence form that provides coverage for its work undertaken pursuant to each Participating Addendum.

c. Contractor shall pay premiums on all insurance policies. Such policies shall also reference this Master Agreement and shall have a condition that they not be revoked by the insurer until thirty (30) calendar days after notice of intended revocation thereof shall have been given to Purchasing Entity and Participating Entity by the Contractor.

d. Prior to commencement of performance, Contractor shall provide to the Lead State a written endorsement to the Contractor's general liability insurance policy or other documentary evidence acceptable to the Lead State that (1) names the Participating States identified in the Request for Proposal as additional insureds, (2) provides that no material alteration, cancellation, non-renewal, or expiration of the coverage contained in such policy shall have effect unless the named Participating State has been given at least thirty (30) days prior written notice, and (3) provides that the Contractor's liability insurance policy shall be primary, with any liability insurance of any Participating State as secondary and noncontributory. Unless otherwise agreed in any Participating Addendum, the Participating Entity's rights and Contractor's obligations are the same as those specified in the first sentence of this subsection. Before performance of any Purchase Order issued after execution of a Participating Addendum authorizing it, the Contractor shall provide to a Purchasing Entity or Participating Entity who requests it the same information described in this subsection.

e. Contractor shall furnish to the Lead State, Participating Entity, and, on request, the Purchasing Entity copies of certificates of all required insurance within thirty (30) calendar days of the execution of this Master Agreement, the execution of a Participating Addendum, or the Purchase Order's effective date and prior to performing any work. The insurance certificate shall provide the following information: the name and address of the insured; name, address, telephone number and signature of the authorized agent; name of the insurance company (authorized to operate in all states); a description of coverage in detailed standard terminology (including policy period, policy number, limits of liability, exclusions and endorsements); and an acknowledgment of the requirement for notice of cancellation. Copies of renewal certificates of all required insurance shall be furnished within thirty (30) days after any renewal date. These certificates of insurance must expressly indicate compliance with each and every insurance requirement specified in this section. Failure to provide evidence of coverage may, at sole option of the Lead State, or any Participating Entity, result in this Master Agreement's termination or the termination of any Participating Addendum.

f. Coverage and limits shall not limit Contractor's liability and obligations under this

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

Master Agreement, any Participating Addendum, or any Purchase Order.

17. Laws and Regulations: Any and all Services offered and furnished shall comply fully with all applicable Federal and State laws and regulations.

18. No Waiver of Sovereign Immunity: In no event shall this Master Agreement, any Participating Addendum or any contract or any Purchase Order issued thereunder, or any act of a Lead State, a Participating Entity, or a Purchasing Entity be a waiver of any form of defense or immunity, whether sovereign immunity, governmental immunity, immunity based on the Eleventh Amendment to the Constitution of the United States or otherwise, from any claim or from the jurisdiction of any court.

This section applies to a claim brought against the Participating State only to the extent Congress has appropriately abrogated the Participating State's sovereign immunity and is not consent by the Participating State to be sued in federal court. This section is also not a waiver by the Participating State of any form of immunity, including but not limited to sovereign immunity and immunity based on the Eleventh Amendment to the Constitution of the United States.

19. Ordering

a. Master Agreement order and purchase order numbers shall be clearly shown on all acknowledgments, shipping labels, packing slips, invoices, and on all correspondence.

b. This Master Agreement permits Purchasing Entities to define project-specific requirements and informally compete the requirement among other firms having a Master Agreement on an "as needed" basis. This procedure may also be used when requirements are aggregated or other firm commitments may be made to achieve reductions in pricing. This procedure may be modified in Participating Addenda and adapted to Purchasing Entity rules and policies. The Purchasing Entity may in its sole discretion determine which firms should be solicited for a quote. The Purchasing Entity may select the quote that it considers most advantageous, cost and other factors considered.

c. Each Purchasing Entity will identify and utilize its own appropriate purchasing procedure and documentation. Contractor is expected to become familiar with the Purchasing Entities' rules, policies, and procedures regarding the ordering of supplies and/or services contemplated by this Master Agreement.

d. Contractor shall not begin providing Services without a valid Service Level Agreement or other appropriate commitment document compliant with the law of the Purchasing Entity.

e. Orders may be placed consistent with the terms of this Master Agreement during the term of the Master Agreement.

f. All Orders pursuant to this Master Agreement, at a minimum, shall include:

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

(1) The services or supplies being delivered;
(2) The place and requested time of delivery;
(3) A billing address;
(4) The name, phone number, and address of the Purchasing Entity representative;
(5) The price per unit or other pricing elements consistent with this Master Agreement and the contractor's proposal;
(6) A ceiling amount of the order for services being ordered; and
(7) The Master Agreement identifier and the Participating State contract identifier.

g. All communications concerning administration of Orders placed shall be furnished solely to the authorized purchasing agent within the Purchasing Entity's purchasing office, or to such other individual identified in writing in the Order.

h. Orders must be placed pursuant to this Master Agreement prior to the termination date of this Master Agreement. Contractor is reminded that financial obligations of Purchasing Entities payable after the current applicable fiscal year are contingent upon agency funds for that purpose being appropriated, budgeted, and otherwise made available.

i. Notwithstanding the expiration or termination of this Master Agreement, Contractor agrees to perform in accordance with the terms of any Orders then outstanding at the time of such expiration or termination. Contractor shall not honor any Orders placed after the expiration or termination of this Master Agreement. Orders from any separate indefinite quantity, task orders, or other form of indefinite delivery order arrangement priced against this Master Agreement may not be placed after the expiration or termination of this Master Agreement, notwithstanding the term of any such indefinite delivery order agreement.

20. Participants and Scope

a. Contractor may not deliver Services under this Master Agreement until a Participating Addendum acceptable to the Participating Entity and Contractor is executed. The NASPO ValuePoint Master Agreement Terms and Conditions are applicable to any Order by a Participating Entity (and other Purchasing Entities covered by their Participating Addendum), except to the extent altered, modified, supplemented or amended by a Participating Addendum. By way of illustration and not limitation, this authority may apply to unique delivery and invoicing requirements, confidentiality requirements, defaults on Orders, governing law and venue relating to Orders by a Participating Entity, indemnification, and insurance requirements. Statutory or constitutional requirements relating to availability of funds may require specific language in some Participating Addenda in order to comply with applicable law. The expectation is that these alterations, modifications, supplements, or amendments will be addressed in the Participating Addendum or, with the consent of the Purchasing Entity and Contractor, may be included in the ordering document (e.g. purchase order or contract) used by the Purchasing Entity to place the Order.

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

b. Subject to subsection 20c and a Participating Entity's Participating Addendum, the use of specific NASPO ValuePoint cooperative Master Agreements by state agencies, political subdivisions and other Participating Entities (including cooperatives) authorized by individual state's statutes to use state contracts is subject to the approval of the respective State Chief Procurement Official.

c. Unless otherwise stipulated in a Participating Entity's Participating Addendum, specific services accessed through the NASPO ValuePoint cooperative Master Agreements for Cloud Services by state executive branch agencies, as required by a Participating Entity's statutes, are subject to the authority and approval of the Participating Entity's Chief Information Officer's Office[3].

d. Obligations under this Master Agreement are limited to those Participating Entities who have signed a Participating Addendum and Purchasing Entities within the scope of those Participating Addenda. States or other entities permitted to participate may use an informal competitive process to determine which Master Agreements to participate in through execution of a Participating Addendum. Financial obligations of Participating States are limited to the orders placed by the departments or other state agencies and institutions having available funds. Participating States incur no financial obligations on behalf of political subdivisions.

e. NASPO ValuePoint is not a party to the Master Agreement. It is a nonprofit cooperative purchasing organization assisting states in administering the NASPO ValuePoint cooperative purchasing program for state government departments, institutions, agencies and political subdivisions (e.g., colleges, school districts, counties, cities, etc.) for all 50 states, the District of Columbia and the territories of the United States.

f. Participating Addenda shall not be construed to amend the terms of this Master Agreement between the Lead State and Contractor.

g. Participating Entities who are not states may under some circumstances sign their own Participating Addendum, subject to the approval of participation by the Chief Procurement Official of the state where the Participating Entity is located. Coordinate requests for such participation through NASPO ValuePoint. Any permission to participate through execution of a Participating Addendum is not a determination that procurement authority exists in the Participating Entity; they must ensure that they have the requisite procurement authority to execute a Participating Addendum.

h. Resale. Subject to any explicit permission in a Participating Addendum, Purchasing Entities may not resell goods, software, or Services obtained under this Master Agreement. This limitation does not prohibit: payments by employees of a Purchasing Entity as explicitly permitted under this agreement; sales of goods to the general public as surplus property; and fees associated with inventory transactions with other

[3] Chief Information Officer means the individual designated by the Governor with Executive Branch, enterprise-wide responsibility for the leadership and management of information technology resources of a state.

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

governmental or nonprofit entities under cooperative agreements and consistent with a Purchasing Entity's laws and regulations. Any sale or transfer permitted by this subsection must be consistent with license rights granted for use of intellectual property.

21. Payment: Orders under this Master Agreement are fixed-price or fixed-rate orders, not cost reimbursement contracts. Unless otherwise stipulated in the Participating Addendum, Payment is normally made within 30 days following the date of a correct invoice is received. Purchasing Entities reserve the right to withhold payment of a portion (including all if applicable) of disputed amount of an invoice. After 45 days the Contractor may assess overdue account charges up to a maximum rate of one percent per month on the outstanding balance. Payments will be remitted by mail. Payments may be made via a State or political subdivision "Purchasing Card" with no additional charge.

22. Data Access Controls: Contractor will provide access to Purchasing Entity's Data only to those Contractor employees, contractors and subcontractors ("Contractor Staff") who need to access the Data to fulfill Contractor's obligations under this Agreement. Contractor shall not access a Purchasing Entity's user accounts or Data, except on the course of data center operations, response to service or technical issues, as required by the express terms of this Master Agreement, or at a Purchasing Entity's written request.

Contractor may not share a Purchasing Entity's Data with its parent corporation, other affiliates, or any other third party without the Purchasing Entity's express written consent.

Contractor will ensure that, prior to being granted access to the Data, Contractor Staff who perform work under this Agreement have successfully completed annual instruction of a nature sufficient to enable them to effectively comply with all Data protection provisions of this Agreement; and possess all qualifications appropriate to the nature of the employees' duties and the sensitivity of the Data they will be handling.

23. Operations Management: Contractor shall maintain the administrative, physical, technical, and procedural infrastructure associated with the provision of the Product in a manner that is, at all times during the term of this Master Agreement, at a level equal to or more stringent than those specified in the Solicitation.

24. Public Information: This Master Agreement and all related documents are subject to disclosure pursuant to the Purchasing Entity's public information laws.

25. Purchasing Entity Data: Purchasing Entity retains full right and title to Data provided by it and any Data derived therefrom, including metadata.
Contractor shall not collect, access, or use user-specific Purchasing Entity Data except as strictly necessary to provide Service to the Purchasing Entity. No information regarding Purchasing Entity's use of the Service may be disclosed, provided, rented or sold to any third party for any reason unless required by law or regulation or by an order of a court of competent jurisdiction. The obligation shall extend beyond the term of this Master Agreement in perpetuity.

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

Contractor shall not use any information collected in connection with this Master Agreement, including Purchasing Entity Data, for any purpose other than fulfilling its obligations under this Master Agreement.

Notwithstanding the foregoing, Contractor may (i) compile statistical and other information related to the performance, operation and use of the Service, and (ii) use Data from the Service in aggregated form for security and operations management, to create statistical analyses, and for research and development purposes (clauses i and ii are collectively referred to as "Service Analyses"). Contractor retains all intellectual property rights in Service Analyses.

26. Records Administration and Audit.

a. The Contractor shall maintain books, records, documents, and other evidence pertaining to this Master Agreement and orders placed by Purchasing Entities under it to the extent and in such detail as shall adequately reflect performance and administration of payments and fees. Contractor shall permit the Lead State, a Participating Entity, a Purchasing Entity, the federal government (including its grant awarding entities and the U.S. Comptroller General), and any other duly authorized agent of a governmental agency, to audit, inspect, examine, copy and/or transcribe Contractor's books, documents, papers and records directly pertinent to this Master Agreement or orders placed by a Purchasing Entity under it for the purpose of making audits, examinations, excerpts, and transcriptions. This right shall survive for a period of six (6) years following termination of this Agreement or final payment for any order placed by a Purchasing Entity against this Agreement, whichever is later, to assure compliance with the terms hereof or to evaluate performance hereunder.

b. Without limiting any other remedy available to any governmental entity, the Contractor shall reimburse the applicable Lead State, Participating Entity, or Purchasing Entity for any overpayments inconsistent with the terms of the Master Agreement or orders or underpayment of fees found as a result of the examination of the Contractor's records.

c. The rights and obligations herein exist in addition to any quality assurance obligation in the Master Agreement requiring the Contractor to self-audit contract obligations and that permits the Lead State to review compliance with those obligations.

d. The Contractor shall allow the Purchasing Entity to audit information directly related to conformance to the Master Agreement and applicable Participating Addendum terms. All audits will be conducted during regular business hours, and no more frequently than once in any 12 month period, and in a manner that does not unreasonably interfere with Contractor's business operations. The Purchasing Entity may perform this audit or contract with a third party bound by written confidentiality and restricted use obligations at least as protective of Confidential Information as the terms set forth in Section 8, at its discretion and at the Purchasing Entity's expense.

27. Administrative Fees: The Contractor shall pay to NASPO ValuePoint, or its

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

assignee, a NASPO ValuePoint Administrative Fee of one-quarter of one percent (0.25% or 0.0025) no later than 60 days following the end of each calendar quarter. The NASPO ValuePoint Administrative Fee shall be submitted quarterly and is based on sales of the Services. The NASPO ValuePoint Administrative Fee is not negotiable. This fee is to be included as part of the pricing submitted with proposal.

Additionally, some states may require an additional administrative fee be paid directly to the state on purchases made by Purchasing Entities within that state. For all such requests, the fee level, payment method and schedule for such reports and payments will be incorporated into the Participating Addendum that is made a part of the Master Agreement. The Contractor may adjust the Master Agreement pricing accordingly for purchases made by Purchasing Entities within the jurisdiction of the state. All such agreements shall not affect the NASPO ValuePoint Administrative Fee percentage or the prices paid by the Purchasing Entities outside the jurisdiction of the state requesting the additional fee. The NASPO ValuePoint Administrative Fee shall be based on the gross amount of all sales at the adjusted prices (if any) in Participating Addenda.

28. System Failure or Damage: In the event of system failure or damage caused by Contractor or its Services, the Contractor agrees to use its best efforts to restore or assist in restoring the system to operational capacity.

29. Title to Product: If access to the Product requires an application program interface (API), Contractor shall convey to Purchasing Entity an irrevocable and perpetual license to use the API.

30. Data Privacy: The Contractor must comply with all applicable laws related to data privacy and security, including IRS Pub 1075. Prior to entering into a SLA with a Purchasing Entity, the Contractor and Purchasing Entity must cooperate and hold a meeting to determine the Data Categorization to determine whether the Contractor will hold, store, or process High Risk Data, Moderate Risk Data and Low Risk Data. The Contractor must document the Data Categorization in the SLA or Statement of Work.

31. Warranty: At a minimum the Contractor must warrant the following:

a. Contractor has acquired any and all rights, grants, assignments, conveyances, licenses, permissions, and authorization for the Contractor to provide the Services described in this Master Agreement.

b. Contractor will perform materially as described in this Master Agreement, SLA, Statement of Work, including any performance representations contained in the Contractor's response to the Solicitation by the Lead State.

c. Contractor represents and warrants that the representations contained in its response to the Solicitation by the Lead State.

d. The Contractor will not interfere with a Purchasing Entity's access to and use of the

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

Services it acquires from this Master Agreement.

e. The Services provided by the Contractor are compatible with and will operate successfully with any environment (including web browser and operating system) specified by the Contractor in its response to the Solicitation by the Lead State.

f. The Contractor warrants that the Products it provides under this Master Agreement are free of malware. The Contractor must use industry-leading technology to detect and remove worms, Trojans, rootkits, rogues, dialers, spyware, etc.

32. Transition Assistance:

a. The Contractor shall reasonably cooperate with other parties in connection with all Services to be delivered under this Master Agreement, including without limitation any successor service provider to whom a Purchasing Entity's Data is transferred in connection with the termination or expiration of this Master Agreement. The Contractor shall assist a Purchasing Entity in exporting and extracting a Purchasing Entity's Data, in a format usable without the use of the Services and as agreed by a Purchasing Entity, at no additional cost to the Purchasing Entity. Any transition services requested by a Purchasing Entity involving additional knowledge transfer and support may be subject to a separate transition Statement of Work.

b. A Purchasing Entity and the Contractor shall, when reasonable, create a Transition Plan Document identifying the transition services to be provided and including a Statement of Work if applicable.

c. The Contractor must maintain the confidentiality and security of a Purchasing Entity's Data during the transition services and thereafter as required by the Purchasing Entity.

33. Waiver of Breach: Failure of the Lead State, Participating Entity, or Purchasing Entity to declare a default or enforce any rights and remedies shall not operate as a waiver under this Master Agreement or Participating Addendum. Any waiver by the Lead State, Participating Entity, or Purchasing Entity must be in writing. Waiver by the Lead State or Participating Entity of any default, right or remedy under this Master Agreement or Participating Addendum, or by Purchasing Entity with respect to any Purchase Order, or breach of any terms or requirements of this Master Agreement, a Participating Addendum, or Purchase Order shall not be construed or operate as a waiver of any subsequent default or breach of such term or requirement, or of any other term or requirement under this Master Agreement, Participating Addendum, or Purchase Order.

34. Assignment of Antitrust Rights: Contractor irrevocably assigns to a Participating Entity who is a state any claim for relief or cause of action which the Contractor now has or which may accrue to the Contractor in the future by reason of any violation of state or federal antitrust laws (15 U.S.C. § 1-15 or a Participating Entity's state antitrust provisions), as now in effect and as may be amended from time to time, in connection

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

with any goods or services provided to the Contractor for the purpose of carrying out the Contractor's obligations under this Master Agreement or Participating Addendum, including, at a Participating Entity's option, the right to control any such litigation on such claim for relief or cause of action.

35. Debarment : The Contractor certifies, to the best of its knowledge, that neither it nor its principals are presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation in this transaction (contract) by any governmental department or agency. This certification represents a recurring certification made at the time any Order is placed under this Master Agreement. If the Contractor cannot certify this statement, attach a written explanation for review by the Lead State.

36. Performance and Payment Time Frames that Exceed Contract Duration: All maintenance or other agreements for services entered into during the duration of an SLA and whose performance and payment time frames extend beyond the duration of this Master Agreement shall remain in effect for performance and payment purposes (limited to the time frame and services established per each written agreement). No new leases, maintenance or other agreements for services may be executed after the Master Agreement has expired. For the purposes of this section, renewals of maintenance, subscriptions, SaaS subscriptions and agreements, and other service agreements, shall not be considered as "new."

37. Governing Law and Venue

a. The procurement, evaluation, and award of the Master Agreement shall be governed by and construed in accordance with the laws of the Lead State sponsoring and administering the procurement. The construction and effect of the Master Agreement after award shall be governed by the law of the state serving as Lead State (in most cases also the Lead State). The construction and effect of any Participating Addendum or Order against the Master Agreement shall be governed by and construed in accordance with the laws of the Participating Entity's or Purchasing Entity's State.

b. Unless otherwise specified in the RFP, the venue for any protest, claim, dispute or action relating to the procurement, evaluation, and award is in the Lead State. Venue for any claim, dispute or action concerning the terms of the Master Agreement shall be in the state serving as Lead State. Venue for any claim, dispute, or action concerning any Order placed against the Master Agreement or the effect of a Participating Addendum shall be in the Purchasing Entity's State.

c. If a claim is brought in a federal forum, then it must be brought and adjudicated solely and exclusively within the United States District Court for (in decreasing order of priority): the Lead State for claims relating to the procurement, evaluation, award, or contract performance or administration if the Lead State is a party; the Participating State if a named party; the Participating Entity state if a named party; or the Purchasing Entity state if a named party.

d. This section is also not a waiver by the Participating State of any form of immunity,

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

including but not limited to sovereign immunity and immunity based on the Eleventh Amendment to the Constitution of the United States.

38. No Guarantee of Service Volumes: The Contractor acknowledges and agrees that the Lead State and NASPO ValuePoint makes no representation, warranty or condition as to the nature, timing, quality, quantity or volume of business for the Services or any other products and services that the Contractor may realize from this Master Agreement, or the compensation that may be earned by the Contractor by offering the Services. The Contractor acknowledges and agrees that it has conducted its own due diligence prior to entering into this Master Agreement as to all the foregoing matters.

39. NASPO ValuePoint eMarket Center: In July 2011, NASPO ValuePoint entered into a multi-year agreement with JAGGAER, formerly SciQuest, whereby JAGGAER will provide certain electronic catalog hosting and management services to enable eligible NASPO ValuePoint's customers to access a central online website to view and/or shop the goods and services available from existing NASPO ValuePoint Cooperative Contracts. The central online website is referred to as the NASPO ValuePoint eMarket Center.

The Contractor will have visibility in the eMarket Center through Ordering Instructions. These Ordering Instructions are available at no cost to the Contractor and provided customers information regarding the Contractors website and ordering information.

At a minimum, the Contractor agrees to the following timeline: NASPO ValuePoint eMarket Center Site Admin shall provide a written request to the Contractor to begin Ordering Instruction process. The Contractor shall have thirty (30) days from receipt of written request to work with NASPO ValuePoint to provide any unique information and ordering instructions that the Contractor would like the customer to have.

40. Contract Provisions for Orders Utilizing Federal Funds: Pursuant to Appendix II to 2 Code of Federal Regulations (CFR) Part 200, Contract Provisions for Non-Federal Entity Contracts Under Federal Awards, Orders funded with federal funds may have additional contractual requirements or certifications that must be satisfied at the time the Order is placed or upon delivery. These federal requirements may be proposed by Participating Entities in Participating Addenda and Purchasing Entities for incorporation in Orders placed under this master agreement.

41. Government Support: No support, facility space, materials, special access, personnel or other obligations on behalf of the states or other Participating Entities, other than payment, are required under the Master Agreement.

42. NASPO ValuePoint Summary and Detailed Usage Reports: In addition to other reports that may be required by this solicitation, the Contractor shall provide the following NASPO ValuePoint reports.

a. Summary Sales Data. The Contractor shall submit quarterly sales reports directly to

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

NASPO ValuePoint using the NASPO ValuePoint Quarterly Sales/Administrative Fee Reporting Tool found at http://calculator.naspovaluepoint.org. Any/all sales made under the contract shall be reported as cumulative totals by state. Even if Contractor experiences zero sales during a calendar quarter, a report is still required. Reports shall be due no later than 30 day following the end of the calendar quarter (as specified in the reporting tool).

b. Detailed Sales Data. Contractor shall also report detailed sales data by: (1) state; (2) entity/customer type, e.g. local government, higher education, K12, non-profit; (3) Purchasing Entity name; (4) Purchasing Entity bill-to and ship-to locations; (4) Purchasing Entity and Contractor Purchase Order identifier/number(s); (5) Purchase Order Type (e.g. sales order, credit, return, upgrade, determined by industry practices); (6) Purchase Order date; (7) and line item description, including product number if used. The report shall be submitted in any form required by the solicitation. Reports are due on a quarterly basis and must be received by the Lead State and NASPO ValuePoint Cooperative Development Team no later than thirty (30) days after the end of the reporting period. Reports shall be delivered to the Lead State and to the NASPO ValuePoint Cooperative Development Team electronically through a designated portal, email, CD-Rom, flash drive or other method as determined by the Lead State and NASPO ValuePoint. Detailed sales data reports shall include sales information for all sales under Participating Addenda executed under this Master Agreement. The format for the detailed sales data report is in shown in Attachment H.

c. Reportable sales for the summary sales data report and detailed sales data report includes sales to employees for personal use where authorized by the solicitation and the Participating Addendum. Report data for employees should be limited to ONLY the state and entity they are participating under the authority of (state and agency, city, county, school district, etc.) and the amount of sales. No personal identification numbers, e.g. names, addresses, social security numbers or any other numerical identifier, may be submitted with any report.

d. Contractor shall provide the NASPO ValuePoint Cooperative Development Coordinator with an executive summary each quarter that includes, at a minimum, a list of states with an active Participating Addendum, states that Contractor is in negotiations with and any PA roll out or implementation activities and issues. NASPO ValuePoint Cooperative Development Coordinator and Contractor will determine the format and content of the executive summary. The executive summary is due 30 days after the conclusion of each calendar quarter.

e. Timely submission of these reports is a material requirement of the Master Agreement. The recipient of the reports shall have exclusive ownership of the media containing the reports. The Lead State and NASPO ValuePoint shall have a perpetual, irrevocable, non-exclusive, royalty free, transferable right to display, modify, copy, and otherwise use reports, data and information provided under this section.

f. If requested by a Participating Entity, the Contractor must provide detailed sales data

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

within the Participating State.

43. NASPO ValuePoint Cooperative Program Marketing, Training, and Performance Review:

a. Contractor agrees to work cooperatively with NASPO ValuePoint personnel. Contractor agrees to present plans to NASPO ValuePoint for the education of Contractor's contract administrator(s) and sales/marketing workforce regarding the Master Agreement contract, including the competitive nature of NASPO ValuePoint procurements, the Master agreement and participating addendum process, and the manner in which qualifying entities can participate in the Master Agreement.

b. Contractor agrees, as Participating Addendums become executed, if requested by ValuePoint personnel to provide plans to launch the program within the participating state. Plans will include time frames to launch the agreement and confirmation that the Contractor's website has been updated to properly reflect the contract offer as available in the participating state.

c. Contractor agrees, absent anything to the contrary outlined in a Participating Addendum, to consider customer proposed terms and conditions, as deemed important to the customer, for possible inclusion into the customer agreement. Contractor will ensure that their sales force is aware of this contracting option.

d. Contractor agrees to participate in an annual contract performance review at a location selected by the Lead State and NASPO ValuePoint, which may include a discussion of marketing action plans, target strategies, marketing materials, as well as Contractor reporting and timeliness of payment of administration fees.

e. Contractor acknowledges that the NASPO ValuePoint logos may not be used by Contractor in sales and marketing until a logo use agreement is executed with NASPO ValuePoint.

f. The Lead State expects to evaluate the utilization of the Master Agreement at the annual performance review. Lead State may, in its discretion, terminate the Master Agreement pursuant to section 6 when Contractor utilization does not warrant further administration of the Master Agreement. The Lead State may exercise its right to not renew the Master Agreement if vendor fails to record or report revenue for three consecutive quarters, upon 60-calendar day written notice to the Contractor. This subsection does not limit the discretionary right of either the Lead State or Contractor to terminate the Master Agreement pursuant to section 7.

g. Contractor agrees, within 30 days of their effective date, to notify the Lead State and NASPO ValuePoint of any contractual most-favored-customer provisions in third-part contracts or agreements that may affect the promotion of this Master Agreements or whose terms provide for adjustments to future rates or pricing based on rates, pricing in, or Orders from this master agreement. Upon request of the Lead State or NASPO

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

ValuePoint, Contractor shall provide a copy of any such provisions.

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

45. NASPO ValuePoint Cloud Offerings Search Tool: In support of the Cloud Offerings Search Tool here: http://www.naspovaluepoint.org/#/contract-details/71/search Contractor shall ensure its Cloud Offerings are accurately reported and updated to the Lead State in the format/template shown in Attachment I.

46. Contractor Proprietary and Other Rights / Usage Restrictions:

a. Contractor owns all right, title and interest in and to the Product, except for sub-components which it may license from third parties. Contractor and its licensors reserve all rights, title and interest in and to the Product and its components, including all related intellectual property rights. No rights are granted to Participating Entity other than those expressly provided in this Agreement and Exhibit 1 to this Agreement. No implied licenses are granted by Contractor.

b. Participating Entity will not (a) make the Product available to, or use the Product for the benefit of, anyone other than Participating Entity and its users; (b) use the Product to create, store or transmit infringing, libelous, or otherwise unlawful or tortious material, or to create, store or transmit material in violation of third-party privacy, copyright, trademark, patent or other intellectual property rights, (c) use Product to create, store or transmit malicious code, (d) interfere with or disrupt the integrity or performance of the Product; (e) attempt to gain unauthorized access to the Product, or any systems or networks related to the foregoing; (f) permit direct or indirect access to, or use of, the Product in a way that circumvents any Product usage limit; (g) copy any Product, or any part, feature, function or user interface of it; (h) embed or mirror any part of the Product, other than embedding Participating Entity's own intranets or otherwise for its own internal business purposes or as permitted by Contractor documentation for the Product; (i) access the Product in order to develop, create, improve or build a product or service that competes with Contractor's Product, or for any other benchmarking or competitive purpose, or (j) use any third party content with the Product other than as permitted by the applicable third party's terms and conditions therefor and this Agreement.

47. Entire Agreement: This Master Agreement, along with any attachment, including the Laserfiche Terms of Use, Laserfiche Privacy Policy, and Data Protection Addendum attached within Attachment E, contains the entire understanding of the parties hereto with respect to the Master Agreement unless a term is modified in a Participating Addendum with a Participating Entity. No click-through, or other end user terms and conditions or agreements required by the Contractor ("Additional Terms") provided with any Services hereunder shall be binding on Participating Entities or Purchasing Entities, even if use of such Services requires an affirmative "acceptance" of those Additional Terms before access is permitted.

48. LIMITATION OF LIABILITY:

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

a. CONTRACTOR'S AGGREGATE LIABILITY FOR ALL DAMAGES ARISING OUT OF OR RELATED TO THIS MASATER AGREEMENT OR A PURCHASING ENTITY'S ORDER, WHETHER IN CONTRACT OR TORT, OR OTHERWISE, SHALL IN NO EVENT EXCEED THE GREATER OF (i) TWO TIMES THE TOTAL AMOUNTS ACTUALLY PAID TO CONTRACTOR IN THE TWELVE MONTH PERIOD IMMEDIATELY PRECEDING THE EVENT GIVING RISE TO SUCH LIABILITY LESS ANY REFUNDS OR CREDITS RECEIVED BY THE PURCHASIN GENTITYY FROM CONTRACTOR UNDER SUCH OR (II) ONE MILLION DOLLARS.

b. NOTWITHSTANDING THE ABOVE, NEITHER THE CONTRACTOR NOR THE PURCHASING ENTITY SHALL BE LIABLE FOR ANY CONSEQUENTIAL, INDIRECT, INCIDENTAL, PUNITIVE OR SPECIAL DAMAGES OR ANY KIND ARISING DIRECTLY OR INDIRECTLY OUT OF THIS MASTER AGREEMENT OR A PURCHASING ENTITY'S ORDER, INCLUDING, WITHOUT LIMTIATION, DAMAGES, RESULTING FROM LOSS OF USE OR LOSS OF PROFIT OR REVENUCE (EXCLUDING FEES UNDER THIS MASTER AGREEMENT), DATA, OR DATA USE BY THE PURCHASING ENTITY, THE CONTRACTOR, OR BY OTHERS.

c. Contractor's obligation to indemnify for (i) infringement claims or damages under Sections 13(b) Indemnification – Intellectual Property or (ii) claim(s) of bodily injury and death under Section 13(a) shall apply without regard to whether the damages exceed the limits of liability under this Section 48, Limitations of Liability.

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

Exhibit 1 to the Master Agreement: Software-as-a-Service

1. Data Ownership: The Purchasing Entity will own all right, title and interest in its data that is related to the Services provided by this Master Agreement. The Contractor shall not access Purchasing Entity user accounts or Purchasing Entity data, except (1) in the course of data center operations, (2) in response to service or technical issues, (3) as required by the express terms of this Master Agreement, Participating Addendum, SLA, and/or other contract documents, or (4) at the Purchasing Entity's written request.

Contractor shall not collect, access, or use user-specific Purchasing Entity Data except as strictly necessary to provide Service to the Purchasing Entity. No information regarding a Purchasing Entity's use of the Service may be disclosed, provided, rented or sold to any third party for any reason unless required by law or regulation or by an order of a court of competent jurisdiction. This obligation shall survive and extend beyond the term of this Master Agreement.

Notwithstanding the foregoing, Contractor may (i) compile statistical and other information related to the performance, operation and use of the Service, and (ii) use Data from the Service in aggregated form for security and operations management, to create statistical analyses, and for research and development purposes (clauses i and ii are collectively referred to as "Service Analyses"). Contractor retains all intellectual property rights in Service Analyses.

2. Data Protection: Protection of personal privacy and data shall be an integral part of the business activities of the Contractor to ensure there is no inappropriate or unauthorized use of Purchasing Entity information at any time. To this end, the Contractor shall safeguard the confidentiality, integrity and availability of Purchasing Entity information and comply with the following conditions:

a. The Contractor shall implement and maintain appropriate administrative, technical and organizational security measures to safeguard against unauthorized access, disclosure or theft of Personal Data and Non-Public Data. Such security measures shall be in accordance with recognized industry practice and not less stringent than the measures the Contractor applies to its own Personal Data and Non-Public Data of similar kind.

b. Unless stated otherwise herein, aAll data obtained by the Contractor in the performance of the Master Agreement shall become and remain the property of the Purchasing Entity.

c. All Personal Data shall be encrypted at rest and in transit with controlled access. Unless otherwise stipulated, the Contractor is responsible for encryption of the Personal Data. Any stipulation of responsibilities will identify specific roles and responsibilities and shall be included in the service level agreement (SLA), or otherwise made a part of the Master Agreement.

d. Unless otherwise stipulated, the Contractor shall encrypt all Non-Public Data at rest and in transit. The Purchasing Entity shall identify data it deems as Non-Public Data to the Contractor. The level of protection and encryption for all Non-Public Data shall be identified in the SLA.

e. Unless stated otherwise herein, at no time shall any data or processes — that either belong to or are intended for the use of a Purchasing Entity or its officers, agents or employees — be

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

copied, disclosed or retained by the Contractor or any party related to the Contractor for subsequent use in any transaction that does not include the Purchasing Entity.

f. Unless stated otherwise herein, the Contractor shall not use any information collected in connection with the Services issued from this Master Agreement for any purpose other than fulfilling the Services.

3. Data Location: The Contractor shall provide its services to the Purchasing Entity and its end users solely from data centers in the U.S. Storage of Purchasing Entity data at rest shall be located solely in data centers in the U.S. The Contractor shall not allow its personnel or contractors to store Purchasing Entity data on portable devices, including personal computers, except for devices that are used and kept only at its U.S. data centers. The Contractor shall permit its personnel and contractors to access Purchasing Entity data remotely only as required to provide technical support. The Contractor may provide technical user support on a 24/7 basis using a Follow the Sun model, unless otherwise prohibited in a Participating Addendum.

4. Security Incident or Data Breach Notification:

a. Incident Response: Contractor may need to communicate with outside parties regarding a security incident, which may include contacting law enforcement, fielding media inquiries and seeking external expertise as mutually agreed upon, defined by law or contained in the contract. Discussing security incidents with the Purchasing Entity should be handled on an urgent as-needed basis, as part of Contractor's communication and mitigation processes as mutually agreed upon, defined by law or contained in the Master Agreement.

b. Security Incident Reporting Requirements: The Contractor shall report a security incident to the Purchasing Entity identified contact immediately as soon as possible or promptly without out reasonable delay, or as defined in the SLA.

c. Breach Reporting Requirements: If the Contractor has actual knowledge of a confirmed data breach that affects the security of any purchasing entity's content that is subject to applicable data breach notification law, the Contractor shall (1) as soon as possible or promptly without out reasonable delay notify the Purchasing Entity, unless shorter time is required by applicable law, and (2) take commercially reasonable measures to address the data breach in a timely manner.

5. Personal Data Breach Responsibilities: This section only applies when a Data Breach occurs with respect to Personal Data within the possession or control of the Contractor.

a. The Contractor, unless stipulated otherwise, shall immediately notify the appropriate Purchasing Entity identified contact by telephone in accordance with the agreed upon security plan or security procedures if it reasonably believes there has been a security incident.

b. The Contractor, unless stipulated otherwise, shall promptly notify the appropriate Purchasing Entity identified contact within 24 hours or sooner by telephone, unless shorter time is required

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

by applicable law, if it has confirmed that there is, or reasonably believes that there has been a Data Breach. The Contractor shall (1) cooperate with the Purchasing Entity as reasonably requested by the Purchasing Entity to investigate and resolve the Data Breach, (2) promptly implement necessary remedial measures, if necessary, and (3) document responsive actions taken related to the Data Breach, including any post-incident review of events and actions taken to make changes in business practices in providing the services, if necessary.

c. Unless otherwise stipulated, if a data breach is a direct result of Contractor's breach of its contractual obligation to encrypt personal data or otherwise prevent its release as reasonably determined by the Purchasing Entity, the Contractor shall bear the costs associated with (1) the investigation and resolution of the data breach; (2) notifications to individuals, regulators or others required by federal and state laws or as otherwise agreed to; (3) a credit monitoring service required by state (or federal) law or as otherwise agreed to; (4) a website or a toll-free number and call center for affected individuals required by federal and state laws — all not to exceed the average per record per person cost calculated for data breaches in the United States (currently $217 per record/person) in the most recent Cost of Data Breach Study: Global Analysis published by the Ponemon Institute at the time of the data breach; and (5) complete all corrective actions as reasonably determined by Contractor based on root cause.

6. Notification of Legal Requests: The Contractor shall contact the Purchasing Entity upon receipt of any electronic discovery, litigation holds, discovery searches and expert testimonies related to the Purchasing Entity's data under the Master Agreement, or which in any way might reasonably require access to the data of the Purchasing Entity. The Contractor shall not respond to subpoenas, service of process and other legal requests related to the Purchasing Entity without first notifying and obtaining the approval of the Purchasing Entity, unless prohibited by law from providing such notice.

7. Termination and Suspension of Service:

a. In the event of a termination of the Master Agreement or applicable Participating Addendum, the Contractor shall implement an orderly return of purchasing entity's data in a CSV or another mutually agreeable format at a time agreed to by the parties or allow the Purchasing Entity to extract it's data and the subsequent secure disposal of purchasing entity's data.

b. During any period of service suspension, the Contractor shall not take any action to intentionally erase or otherwise dispose of any of the Purchasing Entity's data.

c. In the event of termination of any services or agreement in entirety, the Contractor shall not take any action to intentionally erase purchasing entity's data for a period of:

- 10 days after the effective date of termination, if the termination is in accordance with the contract period
- 30 days after the effective date of termination, if the termination is for convenience
- 60 days after the effective date of termination, if the termination is for cause

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

After such period, the Contractor shall have no obligation to maintain or provide any purchasing entity's data and shall thereafter, unless legally prohibited, delete all purchasing entity's data in its systems or otherwise in its possession or under its control.

d. The purchasing entity shall be entitled to any post termination assistance generally made available with respect to the services, unless a unique data retrieval arrangement has been established as part of an SLA.

e. Upon termination of the Services or the Agreement in its entirety, Contractor shall securely dispose of all Purchasing Entity's data in all of its forms, such as disk, CD/ DVD, backup tape and paper, unless stipulated otherwise by the Purchasing Entity. Data shall be permanently deleted and shall not be recoverable, according to National Institute of Standards and Technology (NIST)-approved methods. Certificates of destruction shall be provided to the Purchasing Entity.

8. Background Checks: Upon the request of the Purchasing Entity, the Contractor shall conduct criminal background checks and not utilize any staff, including subcontractors, to fulfill the obligations of the Master Agreement who have been convicted of any crime of dishonesty, including but not limited to criminal fraud, or otherwise convicted of any felony or misdemeanor offense for which incarceration for up to 1 year is an authorized penalty. The Contractor shall promote and maintain an awareness of the importance of securing the Purchasing Entity's information among the Contractor's employees and agents. If any of the stated personnel providing services under a Participating Addendum is not acceptable to the Purchasing Entity in its sole opinion as a result of the background or criminal history investigation, the Purchasing Entity, in its' sole option shall have the right to either (1) request immediate replacement of the person, or (2) immediately terminate the Participating Addendum and any related service agreement.

9. Access to Security Logs and Reports: The Contractor shall provide reports on a schedule specified in the SLA to the Purchasing Entity in a format as specified in the SLA agreed to by both the Contractor and the Purchasing Entity. Reports shall include latency statistics, user access, user access IP address, user access history and security logs for all public jurisdiction files related to this Master Agreement and applicable Participating Addendum.

10. Contract Audit: The Contractor shall allow the Purchasing Entity to audit information directly related to conformance to the Master Agreement terms. All audits will be conducted during regular business hours, and no more frequently than once in any 12 month period, and in a manner that does not unreasonably interfere with Contractor's business operations. The Purchasing Entity may perform this audit or contract with a third party bound by written confidentiality and restricted use obligations at least as protective of Confidential Information as the terms set forth in the Master Agreement, at its discretion and at the Purchasing Entity's expense.

11. Data Center Audit: The Contractor will provide a Service Organization Control (SOC) 2 independent audit report from AWS to the Purchasing Entity at least annually. AWS may remove its proprietary

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

information from the unredacted version. A Service Organization Control (SOC) 2 audit report or approved equivalent sets the minimum level of a third-party audit.

12. Change Control and Advance Notice: The Contractor shall give a minimum forty eight (48) hour advance notice (or as determined by a Purchasing Entity and included in the SLA) to the Purchasing Entity of any upgrades (e.g., major upgrades, minor upgrades, system changes) that may impact service availability and performance. A major upgrade is a replacement of hardware, software or firmware with a newer or better version in order to bring the system up to date or to improve its characteristics. It usually includes a new version number.

Contractor will make updates and upgrades available to Purchasing Entity at no additional costs when Contractor makes such updates and upgrades generally available to its users.

No update, upgrade or other charge to the Service may decrease the Service's functionality, adversely affect Purchasing Entity's use of or access to the Service, or increase the cost of the Service to the Purchasing Entity; provided that new functionality and improvements to the Product may incur additional charges.

Contractor will notify the Purchasing Entity at least thirty days in advance prior to any major update or upgrade.

13. Security: As requested by a Purchasing Entity, the Contractor shall disclose its non-proprietary system security plans (SSP) or security processes and technical limitations to the Purchasing Entity such that adequate protection and flexibility can be attained between the Purchasing Entity and the Contractor. For example: virus checking and port sniffing — the Purchasing Entity and the Contractor shall understand each other's roles and responsibilities.

14. Non-disclosure and Separation of Duties: The Contractor shall enforce separation of job duties, require commercially reasonable non-disclosure agreements, and limit staff knowledge of Purchasing Entity data to that which is absolutely necessary to perform job duties.

15. Import and Export of Data: The Purchasing Entity shall have the ability to import or export data in piecemeal or in entirety at its discretion without interference from the Contractor at any time during the term of Contractor's contract with the Purchasing Entity. This includes the ability for the Purchasing Entity to import or export data to/from other Contractors. Contractor shall specify if Purchasing Entity is required to provide its' own tools for this purpose, including the optional purchase of Contractors tools if Contractors applications are not able to provide this functionality directly.

16. Responsibilities and Uptime Guarantee: The Contractor shall be responsible for the acquisition and operation of all hardware, software and network support related to the services being provided. The technical and professional activities required for establishing, managing and maintaining the environments are the responsibilities of the Contractor. The system shall be available 24/7/365 (with agreed-upon maintenance downtime), and provide service to customers as defined in the SLA.

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

17. Subcontractor Disclosure: Contractor shall identify all of its strategic business partners related to services provided under this Master Agreement, including but not limited to all subcontractors or other entities or individuals who may be a party to a joint venture or similar agreement with the Contractor, and who shall be involved in any application development and/or operations.

18. Right to Remove Individuals: The Purchasing Entity shall have the right at any time to require that the Contractor remove from interaction with Purchasing Entity any Contractor representative who the Purchasing Entity believes is detrimental to its working relationship with the Contractor. The Purchasing Entity shall provide the Contractor with notice of its determination, and the reasons it requests the removal. If the Purchasing Entity signifies that a potential security violation exists with respect to the request, the Contractor shall immediately remove such individual. The Contractor shall not assign the person to any aspect of the Master Agreement or future work orders without the Purchasing Entity's consent.

19. Business Continuity and Disaster Recovery: The Contractor shall provide an abbreviated and redacted business continuity and disaster recovery plan upon request and ensure that the Purchasing Entity's recovery time objective (RTO) of XXX hours/days is met. (XXX hour/days shall be provided to Contractor by the Purchasing Entity.) Contractor must work with the Purchasing Entity to perform an annual Disaster Recovery test and take action to correct any issues detected during the test in a time frame mutually agreed between the Contractor and the Purchasing Entity.

20. Compliance with Accessibility Standards: The Contractor shall comply with and adhere to Accessibility Standards of Section 508 Amendment to the Rehabilitation Act of 1973, or any other state laws or administrative regulations identified by the Participating Entity.

21. Web Services: The Contractor shall use Web services exclusively to interface with the Purchasing Entity's data in near real time.

22. Encryption of Data at Rest: The Contractor shall ensure hard drive encryption consistent with validated cryptography standards as referenced in FIPS 140-2, Security Requirements for Cryptographic Modules for all Personal Data, unless the Purchasing Entity approves in writing for the storage of Personal Data on a Contractor portable device in order to accomplish work as defined in the statement of work.

23. Subscription Terms: Contractor grants to a Purchasing Entity a license to: (i) access and use the Service for its business purposes; (ii) for SaaS, use underlying software as embodied or used in the Service; and (iii) view, copy, upload and download (where applicable), and use Contractor's documentation.

No Contractor terms, including standard click through license or website terms or use of privacy policy, shall apply to Purchasing Entities unless such terms are included in this Master Agreement.

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

Attachment B – Scope of Services Awarded to Contractor

1.1 Awarded Service Model(s).

Contractor is awarded the following Service Model:

- Software as a Serivce (SaaS)

1.2 Risk Categorization.

Contractor's offered solutions offer the ability to store and secure data under the following risk categories:

Service Model	Low Risk Data	Moderate Risk Data	High Risk Data	Deployment Models Offered
SaaS	X	X		Public

2.1 Deployment Models.

Contractor may provide cloud based services through the following deployment methods:

- **Private cloud.** The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.
- **Community cloud.** The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.
- **Public cloud.** The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.
- **Hybrid cloud.** The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds)

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

Attachment C - Pricing Discounts and Schedule

Cloud Service Model: Software as a Service (SaaS)

Contractor: **Compulink Management Center, Inc. dba Laserfiche**

Pricing Notes

1. % discounts are based on minimum discounts off Contractor's commercially published pricelists versus fixed pricing. Nonetheless, Orders will be fixed-price or fixed-rate and not cost reimbursable contracts. Contractor has the ability to update and refresh its respective price catalog, as long as the agreed-upon discounts are fixed.

2. Minimum guaranteed contract discounts do not preclude an Offeror and/or its authorized resellers from providing deeper or additional, incremental discounts at their sole discretion.

3. Purchasing entities shall benefit from any promotional pricing offered by Contractor to similar customers. Promotional pricing shall not be cause for a permanent price change.

4. Contractor's price catalog include the price structures of the cloud service models, value added services (i.e., Maintenance Services, Professional Services, Etc.), and deployment models that it intends to provide including the types of data it is able to hold under each model. Pricing shall all-inclusive of infrastructure and software costs and management of infrastructure, network, OS, and software.

5. Contractor provides tiered pricing to accompany its named user licensing model, therefore, as user count reaches tier thresholds, unit price decreases.

SaaS Minimum Discount % Off

Description	Discount
Full User (0-49)	0.00%
Full User (50-99)	8.95%
Full User (100-199)	22.03%
Full User (200-499)	35.34%
Full User (500-999)	48.60%
Full User (1,000+)	59.57%
Average SaaS OEM Discount Off*	**29.08%**

Additional Value Added Services

		Onsite Hourly Rate		Remote Hourly Rate	
Item Description		**NVP Price**	**Catalog Price**	**NVP Price**	**Catalog Price**
Maintenance Services		$188.00	$225.00	$188.00	$225.00
Professional Services					
	Deployment Services	$188.00	$225.00	$188.00	$225.00
	Integration Services)	$250.00	$300.00	$250.00	$300.00
	Consulting/Advisory Services	$188.00	$225.00	$188.00	$225.00
	Architectural Design Services	$188.00	$225.00	$188.00	$225.00
	Statement of Work Services	$188.00 - $250.00	$225.00 - $300.00	$188.00 - $250.00	$225.00 - $300.00
Partner Services		$188.00	$225.00	$188.00	$225.00
Training Deployment Services		$188.00	$225.00	$188.00	$225.00
Migration Services		$250.00	$300.00	$250.00	$300.00
Testing Services		$188.00	$225.00	$188.00	$225.00

	Deliverable Rates	
	NVP Price	**Catalog Price**
None	None	None
[Insert additional value added services as necessary]	N/A	N/A
[Insert additional value added services as necessary]	N/A	N/A
[Insert additional value added services as necessary]	N/A	N/A

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

Laserfiche®

Technical Response

SK18008

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

8. Technical Response

If applicable to an Offeror's Solution, an Offeror must provide a point by point response to each technical requirement demonstrating its technical capabilities. If a technical requirement is not applicable to an Offeror's Solution then the Offeror must explain why the technical requirement is not applicable.

If an Offeror's proposal contains more than one Solution (i.e., SaaS and Paas) then the Offeror must provide a response for each Solution. However, Offerors do not need to submit a proposal for each Solution.

8.1 (M) (E) Technical Requirements

8.1.1 For the purpose of the RFP, meeting NIST essential characteristics is a primary concern. As such, describe how your proposed solution(s) meet the characteristics defined in NIST Special Publication 800-145.

Laserfiche Cloud meets the five essential characteristics in the following ways:

On-demand self-service

Laserfiche Cloud transparently and unilaterally provisions the computing, storage, and networking capacity needed to serve its customers from AWS.

Broad network access

Laserfiche Cloud is a web-based application that is generally accessible to customers over the network from Windows, Mac, iOS, and Android clients. Laserfiche Cloud supports all major browsers, including IE11, Edge, Firefox, and Chrome, and has dedicated Windows, iOS, and Android apps.

Resource pooling

Laserfiche Cloud utilizes multi-tenant infrastructure provided by AWS abstracted from the consumer. All Laserfiche Cloud computing resources and data currently reside within the continental United States.

Rapid elasticity

Laserfiche Cloud elastically provisions the compute and storage resources from AWS necessary to serve its consumers.

Measured service

Laserfiche Cloud meters and reports on relevant metrics for the service (e.g. storage and user accounts) internally and to consumers. Customers can sign up for notifications to alert them automatically when their system usage for measurements such as storage is approaching purchased limits. Customers will be automatically when system use has reached regular intervals such as 75%, 90% and 95% of purchased limits.

Laserfiche Cloud provides the capability for consumers to use the Laserfiche Cloud software, which runs on public cloud infrastructure provisioned from the AWS and managed by Laserfiche. Laserfiche Cloud is a web-based application accessible through web browsers and dedicated Windows, iOS, and Android apps. Consumers of Laserfiche Cloud have no control over the underlying cloud infrastructure, and have limited control over the application capabilities through configuration settings. Thus, Laserfiche Cloud meets the definition for the Software as a Service (SaaS) service model.

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

8.1.2 As applicable to an Offeror's proposal, Offeror must describe its willingness to comply with, the requirements of Attachments C & D.

Laserfiche Cloud adheres to the five essential characteristics and SaaS NIST Service Model described in Attachment C / NIST SP 800-145, as detailed in our response to 8.1.1 above. Laserfiche intends to maintain Laserfiche Cloud as a cloud-based SaaS product in adherence with the NIST SP 800-145 definitions, and will cooperate with Participating Entities to perform Risk Categorizations prior to signing a Participating Addendum, pursuant to the terms of the contract. Please see [Compulink Management Center Inc., dba Laserfiche] Cover Letter for the relevant SaaS sub-categories and Risk Categories.

8.1.3 As applicable to an Offeror's proposal, Offeror must describe how its offerings adhere to the services, definitions, and deployment models identified in the Scope of Services, in Attachment D.

Laserfiche is a Cloud-based Service Provider. The Laserfiche Cloud service adheres to the five essential characteristics and SaaS NIST Service Model described in Attachment D 1.1.3 and NIST SP 800-145, as detailed in our response to 8.1.1 above.

Prior to signing a Participating Addendum, Laserfiche will cooperate with a Participating Entity to determine what type of risk categories of data it would store in Laserfiche Cloud. Please see our response to 8.3.6 for further details.

8.2 (E) Subcontractors

8.2.1 Offerors must explain whether they intend to provide all cloud solutions directly or through the use of Subcontractors. Higher points may be earned by providing all services directly or by providing details of highly qualified Subcontractors; lower scores may be earned for failure to provide detailed plans for providing services or failure to provide detail regarding specific Subcontractors. Any Subcontractor that an Offeror chooses to use in fulfilling the requirements of the RFP must also meet all Administrative, Business and Technical Requirements of the RFP, as applicable to the Solutions provided. Subcontractors do not need to comply with Section 6.3.

While the majority of Laserfiche solutions are sold through authorized resellers throughout the world, Laserfiche Consulting (LFC), a division of Laserfiche, selectively bids on opportunities it considers strategically important. In this instance, we feel the NASPO ValuePoint Master Agreement would greatly benefit from LFC's direct involvement versus purchasing Laserfiche through a reseller. We view this arrangement as a long-term, mutually beneficial partnership where customers benefit from working directly with the software developer, Laserfiche, and contemporaneously, Laserfiche receives real-world feedback as it continues to improve way Laserfiche solutions meet the needs of organizations that purchase off of this Master Agreement.

8.2.2 Offeror must describe the extent to which it intends to use subcontractors to perform contract requirements. Include each position providing service and provide a detailed description of how the subcontractors are anticipated to be involved under the Master Agreement.

N/A.

8.2.3 If the subcontractor is known, provide the qualifications of the subcontractor to provide the services; if not, describe how you will guarantee selection of a subcontractor that meets the experience requirements of the RFP. Include a description of how the Offeror will ensure that all subcontractors and their employees will meet all Statement of Work requirements.

N/A.

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

8.3 (E) Working with Purchasing Entities

8.3.1 Offeror must describe how it will work with Purchasing Entities before, during, and after a Data Breach, as defined in the Attachments and Exhibits. Include information such as:

- **Personnel who will be involved at various stages, include detail on how the Contract Manager in Section 7 will be involved;**
- **Response times;**
- **Processes and timelines;**
- **Methods of communication and assistance; and**
- **Other information vital to understanding the service you provide.**

Laserfiche will work with Purchasing Entities on specific security breach notification requirements, including personnel involved, response timeframes, communication methods and other areas as these requirements are typically specific to each organization. Laserfiche will include the Contract Manager in the notification process upon approval of each Purchasing Entity. Laserfiche has security incident response policies and an incident response plan that guides the organization's collective response to security incidents, including incidents that impact the confidentiality or availability of the Laserfiche Cloud system. The security incident response plan is reviewed, tested, and updated as needed. In the event a data breach has been confirmed, Laserfiche will notify Purchasing Entities in accordance with its Laserfiche Cloud agreements and applicable laws.

8.3.2 Offeror must describe how it will not engage in nor permit its agents to push adware, software, or marketing not explicitly authorized by the Participating Entity or the Master Agreement.

Laserfiche takes privacy seriously and we do not permit agents to push adware, software or marketing that is not explicitly authorized by customers or the Master Agreement. More information regarding our privacy policy can be found at https://www.laserfiche.com/legal/privacy/.

8.3.3 Offeror must describe whether its application-hosting environments support a user test/staging environment that is identical to production.

Additional Laserfiche Cloud accounts can be created to provide test and staging environments that mirror the production account. User content such as metadata templates and processes can be downloaded and imported into other accounts to provide flexible transfer options.

8.3.4 Offeror must describe whether or not its computer applications and Web sites are accessible to people with disabilities, and must comply with Participating Entity accessibility policies and the Americans with Disability Act, as applicable.

End user applications such as the document repository and electronic forms are Section 508 compliant. Some administrative actions require drag-and-drop to configure.

8.3.5 Offeror must describe whether or not its applications and content delivered through Web browsers are be accessible using current released versions of multiple browser platforms (such as Internet Explorer, Firefox, Chrome, and Safari) at a minimum.

Web-based Laserfiche applications are compatible with the following browser platforms:

- Internet Explorer – 11+
- Edge – Supported

- Chrome – 6+
- Firefox – 4+
- Safari – 4+

8.3.6 Offeror must describe how it will, prior to the execution of a Service Level Agreement, meet with the Purchasing Entity and cooperate and hold a meeting to determine whether any sensitive or personal information will be stored or used by the Offeror that is subject to any law, rule or regulation providing for specific compliance obligations.

Prior to executing any agreements, Laserfiche Consulting conducts preliminary requirements gathering on the scope of the solution. For Purchasing Entities under this contract, the requirements gathering will include a discovery session to determine whether any sensitive, personal, or otherwise regulated data would be stored by the solution.

8.3.7 Offeror must describe any project schedule plans or work plans that Offerors use in implementing their Solutions with customers. Offerors should include timelines for developing, testing, and implementing Solutions for customers.

Laserfiche Consulting is versed in both traditional Waterfall/SDLC and Agile project management methodologies. The methodology used for each project is determined in collaboration with the customer to ensure it is aligned with their preferences. In practice, most projects are implemented using elements of both where the Statement of Work includes distinct phases with objective milestones/deliverables while the project teams have daily standups and weekly demos are used to show progress and get feedback early and often. In the process of compiling a Statement of Work, Laserfiche Consulting will gather enough information to provide a preliminary project schedule, which will then be formalized during the requirements gathering phase of the project. Project plans and work breakdown schedules are typically created in Microsoft Project format.

Laserfiche Consulting works with each customer to provide a customized timeline for their specific solution implementation. However, here are some general examples to use as guidelines:

Example Project	Time to Develop, Test, Train, and Implement
Simple content repository with basic capture and automation (e.g. auto-filing)	One to three months
Contracts management solution for one or two departments	Three to four months
Records management solution with automation for six departments	Four months
Large content migration (500GB+) from structured source (e.g. legacy ECM)	Four to five months
Enterprise-wide deployment with many complex workflows and integrations	Nine to eighteen months

8.3.8 The State of Utah expects Offeror to update the services periodically as technology changes. Offer must describe:

- **How Offeror's services during Service Line Additions and Updates pursuant to section 2.12 will continue to meet the requirements outlined therein.**

Laserfiche uses a three-level impact and risk classification system to help assess changes to the Production Cloud. This composite system attempts to capture both user impact and deployment risk in a single semi-objective score. The highest numeric level is assigned that satisfies the impact and risk level, so if a change meets level three criteria for impact but level two for risk, the change should be classified as a level three change. Patches, or emergency fixes, are outside the system of change impact progression, but have a defined limit to user impact.

The levels and their definitions:

Release Type	Scope	User Impact Level	Period of Downtime
Level 3: Major Release	• Major updates to an application or the service • May include bug fixes, new features and functionality	Moderate - High	Moderate
Level 2: Minor Release	• Minor updates to an application or the service • May include bug, new features and functionality	Low – Moderate	Short
Level 1: Infrastructure Update	• Consists of updates to the back-end infrastructure	None – Low	None - Minimal
Patch (Emergency Fix)	• May address a specific software failure, bug, or security-related vulnerability • Released after testing has completed, preferably after 6PM PST on weekdays, but potentially immediately after testing has completed	Limited – Moderate	None - Low

- **How Offeror will maintain discounts at the levels set forth in the contract.**

Laserfiche's named user licensing model is accompanied in this RFP response by a tiered pricing model, so as individual organizations reach the defined tiers, the unit prices per named user will decrease.

- **How Offeror will report to the Purchasing Entities, as needed, regarding changes in technology and make recommendations for service updates.**

Laserfiche maintains strict practices in order to ensure upgrades to the Laserfiche software are handled in a transparent, communicative and methodological manner. We regularly issues releases on a quarterly basis and follow the below procedures to provide all subscribers advance notification and resources for all software upgrades.

In addition to the below, as noted previously, subscribers can follow our status.laserfiche.com page for regular emailed reported of any upcoming incidents for release scheduled downtime, if needed.

Major Release

#	Action Item	Timeframe
1	Downtime notification mail sent to customers with a high-level summary of changes	10 Days Pre-Release
2	Downtime notification banner posted visible to all Laserfiche Cloud accounts	10 Days Pre-Release
3	Release notes link will be posted on the Laserfiche Cloud Answers Group Page	Just Prior to Deployment
4	Email customers link to posted release notes and video	Just Prior to Deployment

Minor Release

#	Action Item	Timeframe
1	Downtime notification mail sent to customers with a high-level summary of changes	5 Days Pre-Release
2	Downtime notification banner posted visible to all Laserfiche Cloud accounts	5 Days Pre-Release
3	Release notes link will be posted on the Laserfiche Cloud Answers Group Page	Just Prior to Deployment
4	Email customers link to posted release notes and video	Just Prior to Deployment

Infrastructure Update

#	Action Item	Timeframe
1	Downtime notification mail sent to customers	5 Days Pre-Release
2	Downtime notification banner posted visible to all Laserfiche Cloud accounts	5 Days Pre-Release

Patch

For Patches (Emergency Fixes), customers may be notified as soon as possible after the patch is deployed, but advance notification before deployment may not be possible.

- **How Offeror will provide transition support to any Purchasing Entity whose operations may be negatively impacted by the service change.**

Laserfiche offers multiple avenues by which support will be provided in the scenario a Purchasing Entities operations are negatively impacted by service changes:

Customer Success Management Team

Dedicated Customer Success Managers support all Laserfiche Cloud customers. These individuals specialize in ensuring customer satisfaction by effectively managing and triaging customer issues / requests, asking clarifying questions to determine the correct source & impact of issues and utilizing known best practices to coach customers to alternate solutions when possible.

The Customer Success Management team act as the voice of the customer, working cross-functionally with Marketing, Sales, Product, and Engineering to ensure customer feedback directly translates to implemented product and process improvements. Customer Success Managers will provide support in the scenario a Purchasing Entity's operations are negatively impacted by any deployed service changes.

Product Support

Laserfiche provides a dedicated team of support representatives to support any immediate product bug or issue uncovered in the software. Under the included SLA, support maintains high quality standards of responsiveness and issue resolution to ensure, in the scenario a deployment negatively affected the Purchasing Entities' operations, we would proactively work to quickly address and resolve all issues experienced.

Support Site

In addition to providing ample notifications, release notes and training videos of any enhancement to the product, Laserfiche also provides access for all end users to our Support Site - a robust online library of help documentation, Q&A forum with Laserfiche developers and supportive customer community, training videos, step-by-step walk through training videos, use case guides, regularly training webinars and more materials to assist all subscribers in the transition of new software releases. We recognize the key to seeing value from a Cloud purchase lays in the adoption of end

users utilizing that tool; with that in mind, we're very diligent and critical in providing ample resources for training and support, not only prior to all releases but following as well.

Beta Test Programs

We maintain a regular practice of rolling out software modifications into a Beta State prior to full production release. Our Beta programs provide our Laserfiche customers and reseller community the opportunity to proactively test and provide feedback on our software enhancements prior to a release / modification to our code base. Beta programs are optional to participate in and are coordinated through our Customer Success network. By maintaining this practice, we reduce the possibility of negative experiences following releases because we encourage and invite customers to voice their concerns and suggestions to ensure our enhancements are ideal for their current software business processes.

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

8.4 (E) Customer Service

8.4.1 Offeror must describe how it will ensure excellent customer service is provided to Purchasing Entities. Include:

- **Quality assurance measures;**

Laserfiche Support utilizes a case tracking system to document customer issues, communications, action steps, and resolutions. From this data in this system, Laserfiche can produce reports for customers upon request. Laserfiche is actively engaged in enhancing its support systems to collect additional actionable data and provide greater visibility to our customers.

- **Escalation plan for addressing problems and/or complaints; and**

The standard escalation path start with the Laserfiche Consulting Support team. If needed, they escalate cases to the Corporate Laserfiche Support team. Further escalations involve Laserfiche Development, the Director of Development and/or the VP of Sales as appropriate for the issue.

All support contacts and their relevant information are provided to customer teams during the project kick-off, and during an active services project Laserfiche's project manager and Director of Consulting Services may serve as alternative escalation points.

- **Service Level Agreement (SLA).**

Please see attached [Compulink Management Center, Inc. dba Laserfiche] Service Level Agreement (SLA) under Supplier Attachments in SciQuest.

8.4.2 Offeror must describe its ability to comply with the following customer service requirements:

a. You must have one lead representative for each entity that executes a Participating Addendum. Contact information shall be kept current.

Laserfiche Consulting (LFC) has provided one dedicated Solutions Manager, Brigitte Meiselman, that will service as the lead representative. If any changes are made as it relates to the Solutions Manager's contact information, NASPO will be notified.

b. Customer Service Representative(s) must be available by phone or email at a minimum, from 7AM to 6PM on Monday through Sunday for the applicable time zones.

Laserfiche offers two support tiers: Standard and Premium.

- Laserfiche's Standard support hours for phone and email are 6AM to 6PM Pacific time, Monday to Friday, excluding major holidays.
- Laserfiche's Premium support tier offers prioritized responses for high impact issues and adds weekend email support from 6am to 6pm, excluding major holidays.

c. Customer Service Representative will respond to inquiries within one business day.

Laserfiche support monitors all of its inbound communication channels and responds to inquiries within one business day (including weekends for Premium support subscribers). Customers who submit support requests before Laserfiche's support hours begin will receive a same-business day response; requests submitted after support hours end will receive a next-business day response.

d. You must provide design services for the applicable categories.

Laserfiche's professional services group, Laserfiche Consulting, has provided design and implementation services for Laserfiche solutions for over 20 years. Its core competencies are:

- Content Capture
- Records Management
- Business Process Design
- Report Design
- Process Automation
- Content Migration
- Integrations
- Solutions using Laserfiche APIs

e. You must provide Installation Services for the applicable categories.

While Laserfiche Cloud does not have any required installation per se, Laserfiche Consulting provides implementation services. These services can range from initial account setup to complex implementations with multiple business processes and content migrations. Laserfiche's professional services teams are based out of both California and Virginia to best accommodate customers throughout the country.

8.5 (E) Security of Information

8.5.1 Offeror must describe the measures it takes to protect data. Include a description of the method by which you will hold, protect, and dispose of data following completion of any contract services.

All customer data are subject to strict confidentiality and security policies, and security controls have been implemented by Laserfiche to protect data from unauthorized access by either Laserfiche employees or third-party entities. Customer data are stored in separate, dedicated databases and virtual disk volumes. All data at rest are encrypted, including backup copies, and all connections to transfer data over computer networks are encrypted. Only Cloud Infrastructure personnel have privileged access to the production environment; other Laserfiche employees and contractors are not granted privileged access to the production environment. Privileged access refers to direct access to server host operating systems, databases, AWS infrastructure services, and other types and levels of access restricted to Laserfiche employees.

For data disposal, data becomes immediately inaccessible after an account is disabled. Purging of long-term storage of data backups can be requested in writing for immediate permanent deletion. Once confirmed, all customer data will be permanently and irrecoverably deleted for the specified account. All deletion operations are logged.

8.5.2 Offeror must describe how it intends to comply with all applicable laws and related to data privacy and security.

Compliance is very important to Laserfiche. Of course, data privacy and security issues are central to technology business processes and a key part of Laserfiche's compliance initiatives. Laserfiche's legal team proactively works with outside legal specialists and Laserfiche's Chief Information Officer to monitor current and future data privacy legislation and industry goings on with respect to both data privacy and security standards. Laserfiche has historically stayed abreast and ahead of all developments by implementing and evolving its industry standard data privacy and security policies and framework so that it is prepared for and complies with all applicable laws related to data privacy and security. Laserfiche also periodically trains its personnel on such policies and upcoming legislative changes so that all team members have data privacy and security at the forefront of their thoughts.

Laserfiche takes data privacy and security very seriously. Note that Laserfiche Cloud Services have undergone a rigorous SOC 2 evaluation. SOC 2 is an attestation that ensures that companies such as Laserfiche securely manage data to protect the interests and the privacy of their clients.

Laserfiche will continue to undergo SOC 2 scrutiny and will in the future continue to adapt in a timely fashion to changes in data privacy and security laws that effect its operations.

8.5.3 Offeror must describe how it will not access a Purchasing Entity's user accounts or data, except in the course of data center operations, response to service or technical issues, as required by the express terms of the Master Agreement, the applicable Participating Addendum, and/or the applicable Service Level Agreement.

Laserfiche has a stringent data access policy for customer cloud data and systems access. No Laserfiche employees are able to access customer data unless authorized by a customer or specifically required for support reasons. System access is logged and tracked for auditing and security monitoring purposes, and all customer data is encrypted at rest.

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

8.6 (E) Privacy and Security

8.6.1 Offeror must describe its commitment for its Solutions to comply with NIST, as defined in NIST Special Publication 800-145, and any other relevant industry standards, as it relates to the Scope of Services described in Attachment D, including supporting the different types of data that you may receive.

Laserfiche Cloud adheres to the five essential characteristics and SaaS NIST Service Model described in Attachment C / NIST SP 800-145, as detailed in our response to 8.1.1 above. Laserfiche intends to maintain Laserfiche Cloud as a cloud-based SaaS product in adherence with the NIST SP 800-145 definitions, and will cooperate with Participating Entities to perform Risk Categorizations prior to signing a Participating Addendum, pursuant to the terms of the contract.

8.6.2 Offeror must list all government or standards organization security certifications it currently holds that apply specifically to the Offeror's proposal, as well as those in process at time of response. Specifically include HIPAA, FERPA, CJIS Security Policy, PCI Data Security Standards (DSS), IRS Publication 1075, FISMA, NIST 800-53, NIST SP 800-171, and FIPS 200 if they apply.

Laserfiche has a SOC-2 Type I certification available and is presently working to obtain a SOC-2 Type II certification for the Laserfiche Cloud service.

8.6.3 Offeror must describe its security practices in place to secure data and applications, including threats from outside the service center as well as other customers co-located within the same service center.

All customer data are subject to strict confidentiality and security policies, and security controls have been implemented by Laserfiche to protect data from unauthorized access by either Laserfiche employees or third-party entities. Customer data are stored in separate, dedicated databases and virtual disk volumes. All data at rest are encrypted, including backup copies, and all connections to transfer data over computer networks are encrypted. Only Cloud Infrastructure personnel have privileged access to the production environment; other Laserfiche employees and contractors are not granted privileged access to the production environment. Privileged access refers to direct access to server host operating systems, databases, AWS infrastructure services, and other types and levels of access restricted to Laserfiche employees.

Laserfiche utilizes AWS platforms for its production environment. The physical and environmental controls related to the facilities housing the production environments are managed by the subservice organization. Annually, the Company reviews the latest Service Organization Control (SOC) report for all third party companies' services that are used. Any exceptions will be subject to a customer impact assessment and communicated to appropriate parties.

Laserfiche uses third-party vendors to run dynamic vulnerability scans of Laserfiche Cloud web applications and to conduct external penetration testing of the Laserfiche Cloud system.

Changes to address identified vulnerabilities and weaknesses are deployed using the standard change management process for deploying software updates to Laserfiche Cloud.

8.6.4 Offeror must describe its data confidentiality standards and practices that are in place to ensure data confidentiality. This must include not only prevention of exposure to unauthorized personnel, but also managing and reviewing access that administrators have to stored data. Include information on your hardware policies (laptops, mobile etc).

Laserfiche does not permit employees to access customer data and prohibits the transfer of customer data out of the service environment unless specifically requested by the customer for support reasons.

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

For administrators that have access to confidential data, we enforce monitoring controls and auditing to ensure there is no misuse of privileged access. Laserfiche only permits company approved devices that support our approved information security standards to access service environments. In addition, mobile devices such as laptops and phones utilize encryption in transit and at rest.

8.6.5 Offeror must provide a detailed list of the third-party attestations, reports, security credentials (e.g., FedRamp High, FedRamp Moderate, etc.), and certifications relating to data security, integrity, and other controls.

Laserfiche has a SOC-2 Type I certification available and is presently working to obtain a SOC-2 Type II certification for the Laserfiche Cloud service.

8.6.6 Offeror must describe its logging process including the types of services and devices logged; the event types logged; and the information fields. You should include detailed response on how you plan to maintain security certifications.

Laserfiche maintains a central logging server for production systems to capture log information about system and service accesses, and privileged command execution. This includes items such as customer data deletion operations. Access logs and system event logs do not contain regulated data, such as field data or file contents. Laserfiche maintains certifications to provide our customers independent assessments of Laserfiche Cloud security, confidentiality, and availability. Laserfiche maintains a committee invested with the responsibility to schedule and facilitate certification activities. Internally, regular meetings review procedures and configuration to maintain or exceed compliance with certification criteria. Security logging, auditing and monitoring controls are included in the SOC 2 attestation report, which is provided by a third party audit firm.

8.6.7 Offeror must describe whether it can restrict visibility of cloud hosted data and documents to specific users or groups.

Each entity subscribing to Laserfiche Cloud subscriber has one or more accounts that act as logical containers for their data. Within an account, Laserfiche provides customer administrators the ability to set granular access controls on its data at both the group/role and individual user levels.

8.6.8 Offeror must describe its notification process in the event of a security incident, including relating to timing, incident levels. Offeror should take into consideration that Purchasing Entities may have different notification requirements based on applicable laws and the categorization type of the data being processed or stored.

Laserfiche has developed security incident response policies and an incident response plan that guides the organization's collective response to security incidents, including incidents that impact the confidentiality or availability of the Laserfiche Cloud system. The security incident response plan is reviewed, tested, and updated as needed. In the event a data breach has been confirmed, Laserfiche will notify Purchasing Entities in accordance with its Laserfiche Cloud agreements and applicable laws.

8.6.9 Offeror must describe and identify whether or not it has any security controls, both physical and virtual Zones of Control Architectures (ZOCA), used to isolate hosted servers.

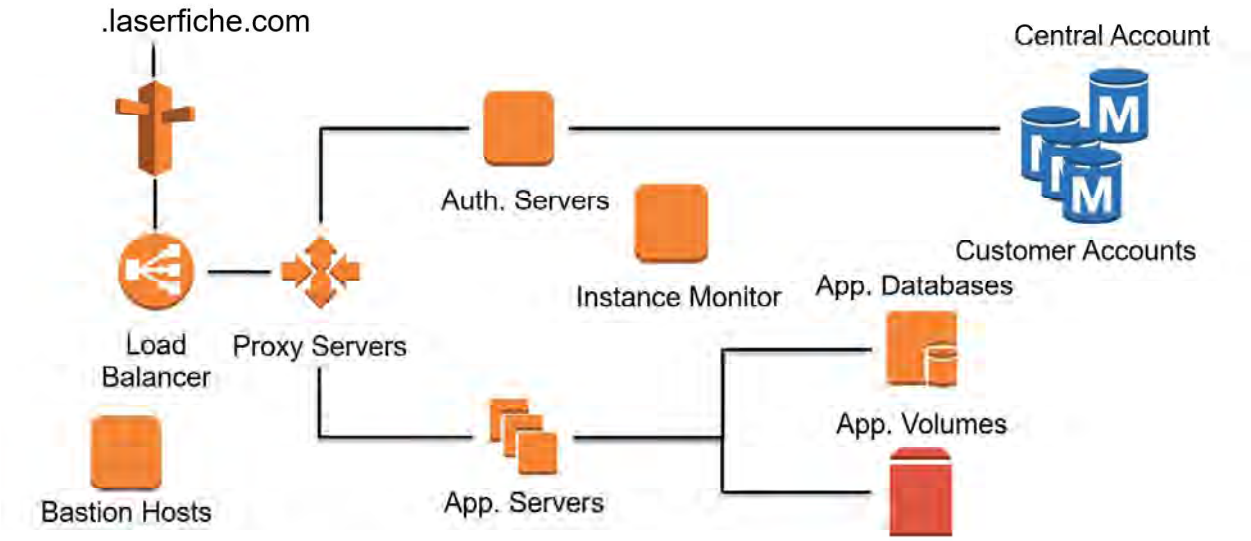
The Laserfiche Cloud service uses multiple virtual and physical layers of security. The Laserfiche Cloud production infrastructure resides within a dedicated virtual private network (AWS VPC) in a dedicated AWS Account, with least-privilege networking and access controls. Cloud-based servers running Laserfiche Cloud services are only permitted to connect to other servers and services necessary for their operation through a combination of administrative controls, firewalls, and network access control lists (NACLs). Laserfiche tightly controls backend administrative access to the Laserfiche Cloud services to a

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

limited number of vetted operations personnel, who can only connect to management interfaces through bastion hosts from whitelisted Laserfiche corporate locations.

8.6.10 Provide Security Technical Reference Architectures that support Infrastructure as a Service (IaaS), Software as a Service (SaaS) & Platform as a Service (PaaS).

The Laserfiche Cloud SaaS system security architecture isolates application servers within a virtual private network (VPC). HTTPS requests from customers are forwarded by a reverse proxy server and through a firewall. Authentication is handled by a server separate from the application servers. Customer data is stored in separate databases and separate content volumes. System administration is only performed through a bastion host, specially configured to resist attacks. Inter-machine connections within the VPC are encrypted.



8.6.11 Describe security procedures (background checks, foot printing logging, etc.) which are in place regarding Offeror's employees who have access to sensitive data.

Laserfiche employees undergo a background check and verification screening during pre-employment. Laserfiche utilizes monitoring controls and auditing of sensitive data access to ensure there is no misuse of privileged access.

8.6.12 Describe the security measures and standards (i.e. NIST) which the Offeror has in place to secure the confidentiality of data at rest and in transit.

NIST 800-52 standards for TLS are used to encrypt data in transit over HTTPS protocol. From NIST800-111 standards for storage encryption technologies, data at rest is protected using AES-256 encryption and is done at the virtual disk / volume level.

8.6.13 Describe policies and procedures regarding notification to both the State and the Cardholders of a data breach, as defined in this RFP, and the mitigation of such a breach.

Laserfiche has developed security incident response policies and an incident response plan that guides the organization's collective response to security incidents, including incidents that impact the confidentiality or availability of the Laserfiche Cloud system. The security incident response plan is reviewed, tested, and updated as needed. In the event a data breach has been confirmed, Laserfiche will notify Purchasing Entities in accordance with its Laserfiche Cloud agreements and applicable laws.

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

8.7 (E) Migration and Redeployment Plan

8.7.1 Offeror must describe how it manages the end of life activities of closing down a service to a Purchasing Entity and safely deprovisioning it before the Offeror is no longer contractually obligated to maintain the service, include planned and unplanned activities. An Offeror's response should include detail on how an Offeror maintains security of the data during this phase of an SLA, if the Offeror provides for redundancy during migration, and how portable the data is during migration.

Laserfiche Cloud customers may export their data at any point prior to contract expiration using any of Laserfiche Cloud's supported export options. These include:

- Standard file downloads from the web client
- Bulk context export in zip files
- Bulk content export with "Laserfiche Briefcases", an XML-based format that bundles content metadata along with the content files themselves
- Custom export scripts using the Laserfiche SDK, if the Purchasing Entity desires a custom export format

Purchasing Entities would export data from Laserfiche Cloud to their on-premises systems in their desired format. Laserfiche does not obfuscate or place proprietary wrappers around customer data, so Purchasing Entities will receive files in either their native formats or one they select (e.g. exporting a TIFF image as PDF).

Data residing in Laserfiche Cloud is encrypted at-rest and data exports are encrypted in-transit. As exporting data for a migration is functionally identical to exporting data for other purposes, the security and redundancy of the underlying data stored in Laserfiche Cloud does not change during a migration.

Laserfiche Cloud retains customer data for 30 days following the termination of a subscription and will provide access to the data during that period upon the customer's written request, provided the request is made prior to the subscription ending.

8.7.2 Offeror must describe how it intends to provide an orderly return of data back to the Purchasing Entity, include any description in your SLA that describes the return of data to a customer.

Laserfiche Cloud provides the means for a Purchasing Entity to export its data at any point while its subscription is active and up to 30 days afterward (see 8.7.1 above). The Purchasing Entity is responsible for exporting its data from Laserfiche Cloud.

Laserfiche can offer a Purchasing Entity general guidance on data migration approaches based on an Entity's goal, or take a more active role in and responsibility for an Entity's data migration through a Professional Services engagement.

8.8 (E) Service or Data Recovery

8.8.1 Describe how you would respond to the following situations; include any contingency plan or policy.

a. Extended downtime.

In the event an AWS data center hosting services of Laserfiche Cloud become inaccessible for an extended period of time, Laserfiche Cloud infrastructure engineers would redeploy those services in an alternative data center in the AWS region. For some components of the system, there will already be machines running those services in the alternative data center that were handling some of the processing load during normal operations.

b. Suffers an unrecoverable loss of data.

If data corruption occurs and customer data cannot be corrected, then Laserfiche Cloud infrastructure engineers would restore the customer data from the backup saved most recently before the corruption occurred. As noted in point (e), Laserfiche maintains an RTO of 4 working hours.

c. Offeror experiences a system failure.

Laserfiche classifies system failures under multiple categorizations as shown within the included example SLA and included in the below table:

Severity Level	Definition	Goal Initial Response Goals***	Updates
Urgent	Laserfiche Cloud is not operational for all customers.	Within 1 business hour	Customer will be updated 2x daily on progress.
Critical	Software functionality is severely impaired even though it is operational at some level affecting multiple customers.	Within 4 business hours	Customer will be updated daily on progress.
High	A major function in the software is not operational and no acceptable work-around is available, but Subscriber is able to do some production work even though performance and user quality is affected.	Within 8 business hours	Customer will be updated weekly on progress.
Medium	There is a loss of a function or resource in software that does not seriously affect Subscriber's operations or schedules.	Within 10 business days	Customer will be updated weekly on progress.
Low	All other issues with software.	As needed	Customer will be updated as needed.

Severity Level	Definition	Goal Initial Response Goals***	Updates
Enhancement	New features and functionality not currently existing will be reviewed by Laserfiche's development team and included in future releases if approved.	As needed	Customer will be updated as needed.

As noted above, incidents which result in total or partial service unavailability, or with risk of data loss, are categorized as the highest priority. Our goal is to response to such incidents within 1 hour of detection and reach complete recovery/resolution within 4 hours. All customer-impacting issues will be communicated via incident postings on the status page (status.laserfiche.com) as soon usually within the first hour of outage.

d. Ability to recover and restore data within 4 business hours in the event of a severe system outage.

As noted in item (e) below, Laserfiche maintains a standard Recovery Time Objective of 4 working hours.

e. Describe your Recovery Point Objective (RPO) and Recovery Time Objective (RTO).

Laserfiche maintains a Recovery Point Objective of 6 hours and Recovery Time Objective of 4 working hours. As data is backed up on an approximately 6-hour interval (see 8.8.2 below for more details), data will be recoverable to within 6 hours before the initial data loss or corruption.

8.8.2 Describe your methodologies for the following backup and restore services:

a. Method of data backups

Laserfiche has built a tool specializing in performing and maintaining data backups, known as the Backup Manager. This tool performs the following backup-related functions:

- Schedules and initiates backup operations to back up databases, directory trees, and other file-based assets to Amazon S3.
- Tracks where backups are stored in S3.
- Disposes backups that no longer need to be retained.
- Performs and coordinates restoration processes.

Customer databases and file repositories are backed up at regular interval throughout the day (every six hours) by the Backup Manager.

The backups are compressed, encrypted, and moved to an S3 bucket designated for backups. Backups are stored in the same region as the rest of the service. However, per AWS, Amazon S3 runs on the world's largest global cloud infrastructure, and was built from the ground up to deliver a customer promise of 99.999999999% of durability. Data is automatically distributed across a minimum of three physical facilities that are geographically separated by at least 10 kilometers within an AWS Region.

Data checksums are created and verified during the database backup and data transfer process to help ensure that S3 has stored the backup file correctly.

All backup data are stored in an encrypted S3 bucket with AWS Identity and Access Management (IAM) policies that limit access to the bucket to roles that require access.

b. Method of server image backups

Server images are AWS EC2 Amazon Machine Images (AMIs) stored in Amazon S3, where they are replicated amongst three physically separate data centers. Any server that needs to be redeployed is restarted from its AMI VM template.

c. Digital location of backup storage (secondary storage, tape, etc.)

Laserfiche Cloud backs up data to Amazon S3, a distributed, highly available, and durable data store described above.

d. Alternate data center strategies for primary data centers within the continental United States.

AWS has data centers in multiple locations worldwide. Currently, Laserfiche Cloud uses the US West (Oregon) Region to host customer data. Within the US West (Oregon) region, there are three availability zones which consist of at least one data center housed in separate facilities with redundant power, networking and connectivity. Laserfiche Cloud utilizes the other two data centers in the event one of them is subject to a disaster.

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

8.9 (E) Data Protection

8.9.1 Specify standard encryption technologies and options to protect sensitive data, depending on the particular service model that you intend to provide under this Master Agreement, while in transit or at rest.

Communication is protected in transit via HTTPS/TLS encryption. Data is rest is protected using AES-256 encryption.

8.9.2 Describe whether or not it is willing to sign relevant and applicable Business Associate Agreement or any other agreement that may be necessary to protect data with a Purchasing Entity.

Laserfiche is willing to sign relevant and applicable Business Associate Agreement or any other agreement that may be necessary to protect data with a Purchasing Entity.

8.9.3 Offeror must describe how it will only use data for purposes defined in the Master Agreement, participating addendum, or related service level agreement. Offeror shall not use the government data or government related data for any other purpose including but not limited to data mining. Offeror or its subcontractors shall not resell nor otherwise redistribute information gained from its access to the data received as a result of this RFP.

Laserfiche will only use the data for purposes defined in the Master Agreement, participating addendum or related service level agreement. Laserfiche will not use the government data or government related data for any other purpose including but not limited to data mining. Neither Laserfiche nor its subcontractors will resell or otherwise redistribute information gained from its access to the data received as a result of this RFP.

8.10 (E) Service Level Agreements

8.10.1 Offeror must describe whether your sample Service Level Agreement is negotiable. If not describe how it benefits purchasing entity's not to negotiate your Service Level Agreement.

Laserfiche's sample Service Level Agreement is negotiable.

8.10.2 Offeror, as part of its proposal, must provide a sample of its Service Level Agreement, which should define the performance and other operating parameters within which the infrastructure must operate to meet IT System and Purchasing Entity's requirements.

Please see attached [Compulink Management Center, Inc. dba Laserfiche] Service Level Agreement (SLA) under Supplier Attachments in SciQuest.

8.11 (E) Data Proposal

Specify your data disposal procedures and policies and destruction confirmation process.

Backup copies of active customer data will be retained for at least seven days, but no more than 30 days. In the event that a customer account holder chooses to cancel their Laserfiche Cloud subscription, the client will have access to their information 60 days post contract termination.

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

8.12 (E) Performance Measures and Reporting

8.12.1 Describe your ability to guarantee reliability and uptime greater than 99.5%. Additional points will be awarded for 99.9% or greater availability.

Commencing with Subscriber's use of Laserfiche Cloud during the Term of the Agreement, Laserfiche will use commercially reasonable efforts, to make Laserfiche Cloud available 24 hours a day, 7 days a week, subject to the limitations set forth in the included SLA. Laserfiche guarantees Laserfiche Cloud will be available 99.9% of the time each calendar month.

8.12.2 Provide your standard uptime service and related Service Level Agreement (SLA) criteria.

Laserfiche measures uptime by providing available, real-time reporting on all unique components of the Laserfiche Cloud system. Subscribers may view, save and print reports on uptime at any time by visiting status.laserfiche.com. Per the definition in the included SLA, uptime guarantees for Laserfiche Cloud are 99.9% availability.

8.12.3 Specify and provide the process to be used for the participating entity to call/contact you for support, who will be providing the support, and describe the basis of availability.

Laserfiche provides a dedicated team of support representatives to support any immediate product bug or issue uncovered in the software. Under the included SLA, support maintains high quality standards of responsiveness and issue resolution to ensure, in the scenario a deployment negatively affected the Purchasing Entities' operations, we would proactively work to quickly address and resolve all issues experienced.

8.12.4 Describe the consequences/SLA remedies if the Respondent fails to meet incident response time and incident fix time.

If Laserfiche Cloud does not achieve the performance, the Purchasing Entity may be eligible for a service credit equivalent to the percent of a Subscriber's corresponding monthly Subscription Fees (1/12 of a Subscriber's annual fee) for Laserfiche Cloud correlating to Uptime Percentage in the following chart:

Uptime Percentage	Service Credit Percentage
Less than 99.99% but more than or equal to 99.5%	10%
Less than 99.5% but more than or equal to 99.0%	20%
Less than 99.0%	30%

Once awarded, a service credit will appear on a Purchasing Entity's next month's invoice.

8.12.5 Describe the firm's procedures and schedules for any planned downtime.

Laserfiche maintains standard procedures and schedules for all planned downtime. We make these communication expectations available to customers so they're aware of our approaches to communication. In advance of all planned downtime, we follow the below procedures to provide all subscribers advance notification and resources.

In addition to the below, as noted previously, subscribers can follow our status.laserfiche.com page for regular emailed reported of any upcoming incidents for release scheduled downtime, if needed.

Major Release

#	Action Item	Timeframe
1	Downtime notification mail sent to customers with a high-level summary of changes	10 Days Pre-Release
2	Downtime notification banner posted visible to all Laserfiche Cloud accounts	10 Days Pre-Release
3	Release notes link will be posted on the Laserfiche Cloud Answers Group Page	Just Prior to Deployment
4	Email customers link to posted release notes and video	Just Prior to Deployment

Minor Release

#	Action Item	Timeframe
1	Downtime notification mail sent to customers with a high-level summary of changes	5 Days Pre-Release
2	Downtime notification banner posted visible to all Laserfiche Cloud accounts	5 Days Pre-Release
3	Release notes link will be posted on the Laserfiche Cloud Answers Group Page	Just Prior to Deployment
4	Email customers link to posted release notes and video	Just Prior to Deployment

Infrastructure Update

#	Action Item	Timeframe
1	Downtime notification mail sent to customers	5 Days Pre-Release
2	Downtime notification banner posted visible to all Laserfiche Cloud accounts	5 Days Pre-Release

Patch

For Patches (Emergency Fixes), customers may be notified as soon as possible after the patch is deployed, but advance notification before deployment may not be possible.

8.12.6 Describe the consequences/SLA remedies if disaster recovery metrics are not met.

The subscriber will have the right to terminate the subscription agreement if Laserfiche Cloud's uptime in two or more months within a calendar year is lower than 85% in each of such months.

8.12.7 Provide a sample of performance reports and specify if they are available over the Web and if they are real-time statistics or batch statistics.

Real-time statistics of the performance of the Laserfiche system and included applications are available over the web at: status.laserfiche.com

In addition to providing real-time statistics, the status page site also includes a summary of both past incidents and scheduled enhancement periods that have affected the performance of the Laserfiche Cloud system.

8.12.8 Ability to print historical, statistical, and usage reports locally.

A Purchasing Entity can subscribe to emails from the status page to be alerted when changes in status are made to any of the applications or system as a whole. The Purchasing Entity can print those reports if so desired.

Laserfiche Cloud includes a comprehensive Audit Trail application enabling a Purchasing Entity to track activities performed in a Laserfiche repository. The tracked information is efficiently stored in log files processed for use in reports. Combined with other aspects of the Laserfiche system, auditing not only helps to show compliance with legal regulations, but also contributes to the security of the Laserfiche repository.

8.12.9 Offeror must describe whether or not its on-demand deployment is supported 24x365.

Laserfiche will use commercially reasonable efforts to make Laserfiche Cloud available 24 hours a day, 7 days a week and will, per the terms in the included SLA, maintain an uptime of 99.9%.

8.12.10 Offeror must describe its scale-up and scale-down, and whether it is available 24x365.

Laserfiche Cloud leverages the AWS Auto Scaling feature. AWS Auto Scaling monitors your applications and automatically adjusts capacity to maintain steady, predictable performance at the lowest possible cost. Using AWS Auto Scaling, it's easy to setup application scaling for multiple resources across multiple services in minutes. The service provides a simple, powerful user interface that lets you build scaling plans for resources including Amazon EC2 instances and Spot Fleets, Amazon ECS tasks, Amazon DynamoDB tables and indexes, and Amazon Aurora Replicas. AWS Auto Scaling makes scaling simple with recommendations that allow you to optimize performance.

In addition to our focus on auto-scaling and as described in above answers, Laserfiche will use commercially reasonable efforts to make Laserfiche Cloud available 24 hours a day, 7 days a week and will, per the terms in the included SLA, maintain an uptime of 99.9%.

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

8.13 (E) Cloud Security Alliance

Describe and provide your level of disclosure with CSA Star Registry for each Solution offered.

a. Completion of a CSA STAR Self-Assessment. (3 points)

b. Completion of Exhibits 1 and 2 to Attachment B. (3 points)

c. Completion of a CSA STAR Attestation, Certification, or Assessment. (4 points)

d. Completion CSA STAR Continuous Monitoring. (5 points)

Please see [Compulink Management Center, Inc. dba Laserfiche] Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) within the Suppliers Attachments within SciQuest.

8.14 (E) Service Provisioning

8.14.1 Describe in detail how your firm processes emergency or rush services implementation requests by a Purchasing Entity.

Laserfiche provides a dedicated team of support representatives to support any immediate product bug or issue uncovered in the software. Under the included SLA, support maintains high quality standards of responsiveness and issue resolution to ensure, in the scenario a deployment negatively affected the Purchasing Entities' operations, we would proactively work to quickly address and resolve all issues experienced.

For Patches (Emergency Fixes), customers may be notified as soon as possible after the patch is deployed, but advance notification before deployment may not be possible.

8.14.2 Describe in detail the standard lead-time for provisioning your Solutions.

Laserfiche Cloud provisions the infrastructure and application environments for new accounts within approximately 30 minutes. After the account is ready, there are additional basic configuration steps, such as adding or syncing user accounts and setting security roles, before general end users can access the solution. The time those basic configuration tasks take can range from a day in simple cases, to significantly longer if, for example, an organization needs to internally reevaluate its role-based security structure to better utilize the new Laserfiche solution before allowing general end users access.

Similarly, an organization may choose to start having end users use the solution right away and add in process automation as they go, or configure and test a cohesive set of workflow processes before "going live" with the solution. Please see 8.3.7 for several sample project timelines.

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

8.15 (E) Back Up and Disaster Plan

8.15.1 Ability to apply legal retention periods and disposition by agency per purchasing entity policy and/or legal requirements.

Customer data stored within the Laserfiche document repository can be made subject to retention periods and disposition rules as configured by administrative users. Laserfiche software provides the ability to define when a record should enter a read-only state, and how long it should be held before being destroyed or accessioned. These rules can be applied by users with delegated security access, and can be modified to suit purchasing entity policy or legal requirements.

In terms of customer data managed by Laserfiche as a whole, it is subject to a data retention and disposal policy that also applies to backup data. Any content subject to deletion is sent through the Laserfiche Cloud Data Deletion Procedure to validate and approve the request to perform a total deletion of the account upon cancellation.

8.15.2 Describe any known inherent disaster recovery risks and provide potential mitigation strategies.

Laserfiche leverages redundant availability zones to mitigate the risks of a disaster event with AWS US-West-2. However, risks from major events that disrupt entire geographic regions have not been completely mitigated. Currently, backups are stored in encrypted S3 buckets within the same region, however the backups could be stored in another region to mitigate this risk. Laserfiche is planning to expand Laserfiche Cloud to other AWS regions in the near future.

8.15.3 Describe the infrastructure that supports multiple data centers within the United States, each of which supports redundancy, failover capability, and the ability to run large scale applications independently in case one data center is lost.

AWS has data centers in multiple locations worldwide. Currently, Laserfiche Cloud uses the US West (Oregon) Region to host customer data. Within the US West (Oregon) region, there are three availability zones which consist of at least one data center housed in separate facilities with redundant power, networking and connectivity. Laserfiche Cloud utilizes the other two data centers in the event one of them is subject to a disaster.

Laserfiche Cloud is backed up four times a day, starting at 9 a.m. UTC and every 6 hours there after (3 p.m., 9 p.m., and 3 a.m.). Laserfiche Cloud automatically generates database and file backups and turns them into encrypted files stored through AWS' Simple Storage Services (S3).

Laserfiche Cloud utilizes Amazon's Elastic Block Store (EBS) to backup data by taking point-in-time snapshots of volumes. With Amazon EBS, Laserfiche is able to create backups of any EBS volume and write a copy of the data in the volume to Amazon S3, where it is stored redundantly in multiple availability zones within the US West (Oregon) region.

Amazon's infrastructure has a high level of availability and provides the features necessary to deploy a resilient IT architecture. AWS has designed its systems to tolerate system or hardware failures with minimal customer impact. For complete information on Amazon Web Services security processes, please consult http://aws.amazon.com/security/ for the latest security information on Amazon Web Services (AWS).

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

8.16 (E) Hosting and Provisioning

8.16.1 Documented cloud hosting provisioning processes, and your defined/standard cloud provisioning stack.

Laserfiche Cloud uses AWS Elastic Compute Cloud (EC2) for the underlying virtual host machines. When new hardware needs to be provisioned, Laserfiche Cloud leverages native EC2 functionality to provision new instances with template specifications according to predefined auto-scaling rules. Note that in general, new resources are not necessarily provisioned on a per-customer basis due to the multi-tenant design of the Laserfiche Cloud infrastructure.

8.16.2 Provide tool sets at minimum for:

1. **Deploying new servers (determining configuration for both stand alone or part of an existing server farm, etc.)**

   When new hardware needs to be provisioned, Laserfiche Cloud leverages native EC2 functionality to provision new instances with template specifications according to predefined auto-scaling rules. Note that in general, new resources are not necessarily provisioned on a per-customer basis due to the multi-tenant design of the Laserfiche Cloud infrastructure.

2. **Creating and storing server images for future multiple deployments**

   To transfer content from an existing Laserfiche Cloud account to a new one, users can download repository content as a Laserfiche briefcase with folder structure intact, as well as download processes for use in another system.

3. **Securing additional storage space**

   Users may purchase additional storage space as necessary, or will be charged fees for overages. There are no additional tools necessary to secure additional storage space.

4. **Monitoring tools for use by each jurisdiction's authorized personnel – and this should ideally cover components of a public (respondent hosted) or hybrid cloud (including Participating entity resources).**

   Data usage can be monitored by users granted administrative access to the account. In addition, audit reporting capabilities are built into the system, and administrative users can run reports on both attempted and successful actions carried out within the document repository. Access to audit features can be granted to individual users or to groups.

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

8.17 (E) Trial and Testing Periods (Pre- and Post-Purchase)

8.17.1 Describe your testing and training periods that your offer for your service offerings.

Laserfiche Consulting tailors testing and training phases to the requirements each specific services implementation project, based on overall scope and complexity. However, the overall structure is usually similar even though durations may vary.

For the testing phase, Laserfiche will provide Sample Test Scripts to the customer and assist them in developing complete UAT Test Scripts. In Laserfiche's experience, UAT coverage is most thorough when the customer takes the lead in developing test cases, as the customer's Business Analysts and power users have intimate familiarity with their business requirements. Laserfiche will then work with the customer to conduct user acceptance testing and remediate any issues identified until acceptance criteria are met. The testing phase usually includes time for one additional two-week development cycle to address minor and "quality of life" feature requests made by users during testing. Testing phases most commonly last three to five weeks.

For training, the Laserfiche project team will take a "train the trainer" approach with customer trainers, administrators, and super users on the solution developed and how to use and manage it. Both on-site and remote training options are available. Laserfiche may also provide or assist the customer in creating customized training materials for the customer's solution, and will provide finalized solution documentation prior to project closeout. Finally, the Laserfiche project team will conduct knowledge transfer sessions with Laserfiche Support on the customer's new Laserfiche solution for post-project support. "Training, Knowledge Transfer, and Documentation" phases most commonly last three to four weeks.

8.17.2 Describe how you intend to provide a test and/or proof of concept environment for evaluation that verifies your ability to meet mandatory requirements.

In our current environment capabilities, the Purchasing Entity will be provided multiple accounts in order to provide for active test, proof of concept and production environments. Each account will have the full capabilities of the subscription agreement. The Purchasing Entity can use the quick provide easy import/export tools Laserfiche provides in order to replicate the active production environment.

We will be deploying a feature in early 2019 enabling subscribers to take advantage of multiple repositories under a single account. This feature would enable the purchasing entity to have a test, proof of concept and production environment stored simultaneously with no need to replicate login credentials. In addition, this will allow for streamlined testing of both document and automation roll-outs.

Looking beyond 2019, we plan to deploy a true sandbox environment where replication of account content is possible across multiple instances. In this environment, we plan on providing capabilities for streamlined deployments of changes from one environment, such as test, into another environment, such as production.

8.17.3 Offeror must describe what training and support it provides at no additional cost.

For training, the Laserfiche project team will take a "train the trainer" approach with customer trainers, administrators, and super users on the solution developed and how to use and manage it. Both on-site and remote training options are available. Laserfiche may also provide or assist the customer in creating customized training materials for the customer's solution, and will provide finalized solution documentation prior to project closeout. Finally, the Laserfiche project team will conduct knowledge transfer sessions with Laserfiche Support on the customer's new Laserfiche solution for post-project

support. “Training, Knowledge Transfer, and Documentation” phases most commonly last three to four weeks.

Laserfiche provides access for all end users to our Support Site - a robust online library of help documentation, Q&A forum with Laserfiche developers and supportive customer community, training videos, step-by-step walk through training videos, use case guides, regularly training webinars and more materials to assist all subscribers in the transition of new software releases. We recognize the key to seeing value from a Cloud purchase lays in the adoption of end users utilizing that tool; with that in mind, we’re very diligent and critical in providing ample resources for training and support, not only prior to all releases but following as well.

8.18 (E) Integration and Customization

8.18.1 Describe how the Solutions you provide can be integrated to other complementary applications, and if you offer standard-based interface to enable additional integrations.

Laserfiche offers several integration options with other line of business applications. Out-of-the-box integrations include LaserApp and DocuSign capabilities, and a Laserfiche Software Development Kit is available to make additional customizations.

In addition to these options, Laserfiche Connector is an image enablement tool that facilitates integrations with third party applications. Laserfiche Connector can be configured using a wizard-driven profile creator to extract information from Laserfiche, and use it to populate other application screens or vice versa. Laserfiche Connector can also use extracted data to import content with prepopulated metadata index fields.

8.18.2 Describe the ways to customize and personalize the Solutions you provide to meet the needs of specific Purchasing Entities.

Laserfiche is a content services platform meant to be configured and personalized for the organization using it. To that end, in addition to the integration options discussed above, user interfaces are highly dynamic, allowing users to hide and show content panes as needed. In addition, indexing templates and folder structures can be designed any way the organization would like to best meet customer needs.

In addition, the process designer within Laserfiche allows organizations to create business processes that mirror their own existing procedures. Forms are created through drag and drop designers, allowing process owners to make electronic forms and personalize their appearance to match any branding guidelines or organizational needs. Process routing is also determined by the process creator; Laserfiche provides a process modeler that allows users to configure the steps that they would like, with configurable notifications, assigned users, and more.

In general, the Laserfiche software is a toolset that allows organizations to automate, capture, and store content, meaning that the ability to customize these processes and document capture methods are built in to the platform.

8.19 (E) Marketing Plan

Describe your how you intend to market your Solutions to NASPO ValuePoint and Participating Entities.

Please see below for some of the ways we plan on marketing the solution to NASPO ValuePoint and Participating Entities:

- We have a dedicated vertical marketing team focusing on the government sector and regularly presenting on insightful topics that are top of mind
- Attend government trade shows focusing on different departmental/enterprise-wide needs
- Provide thought leadership articles in government publications (i.e. American City and County; Government Technology; Center for Digital Government; Digital Communities; StateScoop; etc.)
- Organize educational events for government end users through in-person user groups and workshops
- Partner with national associations like NASCIO (strong NASPO partner) and participating on committees such as:
    - Corporate Leadership Council
    - Awards Committee;
    - Cybersecurity Committee;
    - Data Management Working Group; and
    - Privacy & Data Protection Working Group
    - Produce thought leadership webinars containing valuable use cases for participating entities
- Provide nurturing campaigns containing relevant user stories via email
- Write blog posts providing an opinion on the latest trends taking place in the space
- Promote thought leadership events and customer engagements through social media

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

8.20 (E) Related Value-Added Services to Cloud Solutions

Describe the valued-added services that you can provide as part of an awarded contract, e.g. consulting services pre- and post- implementation. Offerors may detail professional services in the RFP limited to assisting offering activities with initial setup, training and access to the services.

Laserfiche Consulting provides the full range of services that are required to implement Laserfiche in the Cloud environment. This includes (but is not limited to) the following services:

- Requirements gathering to work with the customer and make a determination on the business use case for Laserfiche and detailing functional and technical requirements for the solution.
- Development services to build Laserfiche file plans and business processes using Laserfiche Workflow and Forms. Custom programming services are also available to build integrations with 3rd-party applications, extend the core functionality of the software and migrate legacy, imaging systems to Laserfiche.
- Testing at the system and end-user level. This includes creating custom test scripts and performing the actual testing.
- Training for system administrators, business analysts that will be developing their own business processes and end-users who are interacting within the developed solution.
- Go-live support, which involves pushing the developed solution from the test environment to the production environment and providing post-implementation support services.
- General support services to assist the customer in maintaining a smooth running system. For existing systems, this may also include modifying existing business processes based on changing customer requirements.

8.22 (E) Supporting Infrastructure

8.22.1 Describe what infrastructure is required by the Purchasing Entity to support your Solutions or deployment models.

In general, Laserfiche can be accessed through any computer with modern web browsers as listed in section 8.3.5.

Bulk document scanning, batch import from network folders, and integrations built using the Laserfiche Connector tool do require desktop components. These applications can be installed on workstations that run Windows 7/Windows Server 2008R2 or higher. System requirements for these workstations are minimal, with recommended specifications of 2.93GHz CPU or faster, and 4 GB RAM or more.

8.22.2 If required, who will be responsible for installation of new infrastructure and who will incur those costs?

Laserfiche Cloud will handle the provisioning and related hosting fees for new infrastructure to support maintenance and expansion of the Laserfiche Cloud environment. Customers are responsible for the installation and costs of any optional on-premises infrastructure that may interface with Laserfiche Cloud, such as local scanning workstations.

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

Terms of Use

Effective date: February 2018

Welcome to the Laserfiche website (the "Site"). Laserfiche is pleased to offer you a wide-range of resources, products and content ("Services").

PLEASE READ THESE TERMS CAREFULLY BEFORE UTILIZING THIS SITE. YOU AGREE THAT DISPUTES BETWEEN YOU AND LASERFICHE WILL BE RESOLVED BY BINDING, INDIVIDUAL ARBITRATION, AND YOU WAIVE YOUR RIGHT AS A PLAINTIFF IN ANY CLASS ACTION DISPUTE UNLESS YOU OPT OUT IN ACCORDANCE WITH THE ARBITRATION PROVISION SET FORTH IN SECTION 12 BELOW.

1. Agreement to Terms of Use

By accessing or using the Site or Services, you agree to follow and be bound by these terms and conditions concerning your access to and use of the Site and the Services ("Terms"), as well as our Privacy Policy ("Privacy Policy"). If there is a conflict or inconsistency between these Terms and the rules, guidelines, license agreement, user agreement or other terms and conditions for a specific area of the Site or for specific Services, the latter will have precedence with respect to your access and use of that area of the Site or Services.

Laserfiche may revise the Terms and Privacy Policy at any time without notice to you. The revised Terms and Privacy Policy will be effective when posted.

2. Applicable Use Policy; Site, Services and Software

Any information and data available though the Site is provided solely to enable you to learn about Laserfiche and the Services. You agree to use the Site and Services in accordance with its purpose. To the extent that Laserfiche provides downloadable software, open source software, software as a service offerings, or any other such software product or service, from any Laserfiche operated website or reseller ("Software"), such Software is subject to all agreement(s) that are included with or accompanies the Software, and other terms and conditions that may apply. All Software is provided as-is for evaluation, licensed use, and internal use only. Software may be time-disabled and may cease to operate after a period of time. Software may not be modified or altered in any way. Software may not be redistributed unless specifically authorized in writing by a representative of Laserfiche.

You agree not to use the Site or Services in any unauthorized way, including but not limited to, unlawfully gain access to another person's or entity's information, make

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

any copies, adaptations, modifications, alterations, or reconfiguration of Software, unless otherwise agreed to in a formal written agreement. You further agree not to use the Site or Services in any way that is otherwise in violation of these Terms or applicable law.

3. Privacy

By using the Site or Services, you agree to Laserfiche's collection, use and disclosure of your data and information as described in the Privacy Policy here.

4. Third Party Web Sites, Content, Products and Services

The Site and/or Services may integrate, be integrated into, or be provided in connection with third-party web sites, content, products and services. We do not control nor are we responsible for such third-party websites, content, products and services. You should read the terms of use agreements and privacy policies that apply to such third-party websites, services and content.

5. User Material and Feedback

While we are pleased to receive user material, feedback, suggestions, or information regarding Laserfiche or our Services ("Submissions"), we want you to understand that any Submission sent by you to Laserfiche will be considered non-confidential, non-personal, and non-proprietary (other than personal information, as described in the Privacy Policy). Please note that you are not obligated to disclose or share Submissions with Laserfiche by agreeing to these Terms. All Submissions are voluntary by you.

If you provide Laserfiche with any Submissions, you agree and acknowledge that you assign all rights in the Submissions to Laserfiche and that we have the right to use any Submissions in any way we see fit. You agree that you will not provide to Laserfiche any Submissions that you consider to be confidential or proprietary.

Each time you provide Submissions to Laserfiche, you represent and warrant to Laserfiche that you have the right to submit the Submissions, and by submitting it you will not be infringing any rights of any third party, including intellectual property rights (e.g., copyright, trademark or patent), privacy or publicity rights, rights of confidentiality, or any other contractual obligations.

6. Unsolicited Ideas

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

Laserfiche does not accept or consider unsolicited ideas, which includes, but is not limited to, new or improved products or technologies, product improvements, ideas advertising or promotion campaigns, processes, materials, marketing plans or new product names.

Please do not submit any unsolicited ideas, original creative artwork, suggestions or other works in any form to Laserfiche or any of its employees. The purpose of this policy is to avoid potential misunderstandings or disputes when Laserfiche's products, services, features, or marketing strategies might seem similar to ideas submitted to Laserfiche. If, despite our request that you not send us your ideas, you still submit your ideas to Laserfiche, then regardless of what your communication to Laserfiche says, these Terms will apply to your submission(s).

7. Copyright, Trademarks & Other Intellectual Property

The Site, Services, and Software, and other Laserfiche features, are protected by intellectual property rights of either Laserfiche or a third party licensor. Laserfiche reserves all rights to its trademarks, trade names, service marks, and logos (collectively, "Laserfiche Marks"). For information on trademark use and the Laserfiche brand, please visit out Trademark and Brand Usage Guidelines here.

8. Indemnification

You agree to defend, indemnify and hold harmless Laserfiche, its affiliates, licensors and service providers, and their respective officers, directors, employees, contractors, agents, licensors, suppliers, successors and assigns from and against any claims, liabilities, damages, judgments, awards, losses, costs, expenses or fees (including reasonable attorneys' fees) arising out of or relating to your violation of these Terms or your use of the Site, including, but not limited to any use of Laserfiche's content, services and products.

9. Disclaimer, No Warranties, Limitations

The Site and Services are provided as-is and as available. Compulink Management Center, Inc. dba Laserfiche and its shareholders, affiliates, officers, directors, employees, contractors, agents, representatives, business partners, vendors, clients, licensors, and advisors, whether jointly or severally ("Laserfiche Entities"), expressly disclaim any warranties and conditions of any kind, whether express or implied, statutory or otherwise, including but not limited to any warranties of merchantability, non-infringement and fitness for particular purpose.

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

Neither Laserfiche nor any person associated with Laserfiche makes any representation or warranty with respect to the completeness, security, reliability, quality, accuracy, or availability of the Site or Services. Without limiting the foregoing, neither Laserfiche nor any person associated with Laserfiche represents or warrants that the Site or Services or items obtained through the Site or Services will be accurate, reliable, error-free or uninterrupted, that our Site or the server that makes the Site available are free of harmful components, such as viruses, or that the Site or any Services or items obtained through the Site will otherwise meet your needs or expectations.

You are responsible for implementing sufficient procedures and checkpoints to satisfy your particular requirements for anti-virus protection and accuracy of data input and output, and for maintaining a means external to our site for any reconstruction of any lost data.

Some jurisdictions do not allow the disclaimer or exclusion of certain warranties or the limitation or exclusion of liability for certain damages, or the disclaimer or waiver. To the extent that they are held to be legally invalid, or if Laserfiche may not, as a matter of law, disclaim any implied warranty or limit its liabilities, the scope and duration of such warranty and the extent of Laserfiche's liability will be the minimum permitted under such applicable law. All other terms will remain in full force and effect.

10. Limitation of Liability

In no event will Laserfiche Entities be liable for damages of any kind, under any legal theory, arising out of or in connection with your use, or inability to use, the Site, Services, any websites linked to the Site, any content or information received through the Site, whether it be direct, indirect, special, incidental, consequential, exemplary, or punitive damages, including but not limited to loss of use, data, business or profits, loss of goodwill, loss of data, whether caused by tort (including negligence), breach of contract (foreseeable or otherwise), and on any theory of liability, arising out of or in connection with the Site, Services, or any other such provision by Laserfiche. Access to, and use of, the Site and Services are at your own discretion and risk, and you will be solely responsible for any damage to your computer system or loss of data resulting therefrom.

In the event that you have any basis to recover damages in any circumstance related to Services or breach of these Terms, you agree that our maximum liability to you, arising out of or in connection with the Site or Services will not exceed in aggregate the total amount paid by you to us in respect of the amounts paid in the month preceding any such claim. The existence of more than one claim will not increase such limitation of liability.

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

The foregoing does not affect any liability which cannot be excluded or limited under applicable law.

11. Severability

If any provision of these terms will be unlawful, void or for any reason unenforceable, then that provision will be deemed severed from these Terms and will not affect the validity and enforceability of any remaining provisions. If a court or arbitrator holds that we cannot enforce a part of these Terms as written, we may replace those terms with similar terms to the extent enforceable under relevant law.

12. Arbitration & Class Action Waiver

Laserfiche hopes that we don't have a dispute and we are open to resolving any issues informally. At Laserfiche's sole discretion, it may require you to submit any disputes arising from these Terms or Services, including disputes arising from or concerning their interpretation, violation, invalidity, non-performance, or termination, to **final and binding arbitration under the Commercial Arbitration Rules of the American Arbitration Association ("AAA"). You agree to submit to arbitration in Los Angeles, California.**

Neither you or Laserfiche will enter class arbitration or bring any claims as a plaintiff or class member in any class or representative arbitration proceeding. In the event the prohibition on class arbitration is deemed invalid or unenforceable, then the remaining portions of the arbitration agreement or this Agreement will remain in force. You will have the right to opt out of this agreement to arbitrate by providing written notice of your intention to opt out within 30 days after the Effective Date of the latest Terms.

13. Governing Law & Venue

All matters relating to these Terms and any dispute or claim arising therefrom or related thereto (in each case, including non-contractual disputes or claims), will be governed by and construed in accordance with the laws of the state of California without giving effect to conflicts of law principles.

Any legal suit, action or proceeding arising out of, or related to, these Terms will be instituted exclusively in the federal courts of the United States or the courts of the County of Los Angeles and state of California. You waive any and all objections to the exercise of jurisdiction and venue over you by such courts.

14. Miscellaneous

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

We may assign these Terms, in whole or in part, at any time without notice to you. You may not assign your rights or obligations under these Terms or transfer any rights to use the Services or Site. These Terms are solely for your and our benefit; they aren't for the benefit of any other person, except for Laserfiche's successors and assigns. Persons who are 18 years or younger, or not of the age of majority, may not use the Site or Services thereunder, and we ask that no information in relation to such persons be submitted to Laserfiche. The English language version of these Terms and any notice or other document relating to these Terms shall prevail if there is a conflict except where the document is a constitutional, statutory or other official document.

15. Contact Us

If you have any comments or questions regarding our Terms of Use, please send a message to:

Compulink Management Center, Inc. d/b/a Laserfiche
ATTN: Legal Department
3545 Long Beach Blvd.
Long Beach, CA 90807
USA
notices@laserfiche.com

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

NASPO VALUEPOINT
PUBLIC CLOUD SERVICE LEVEL AGREEMENT

Your use of Laserfiche Cloud is subject to and governed by the NASPO ValuePoint Master Agreement Terms and Conditions and the applicable Participating Entity's Participating Addendum (collectively, the "Agreement") and the following Laserfiche® Public Cloud Service Level Agreement ("SLA"). This SLA forms a binding agreement between Compulink Management Center, Inc. dba Laserfiche® ("Laserfiche") and Subscriber. All capitalized terms not otherwise defined within this SLA shall have their respective meanings as set forth in the Agreement.

1. **LASERFICHE CLOUD SERVICE COMMITMENT**

Commencing with Subscriber's use of Laserfiche Cloud during the Term of the Agreement, Laserfiche will use commercially reasonable efforts based on industry standards, to make Laserfiche Cloud available 24 hours a day, 7 days a week, subject to the limitations set forth in this SLA. Laserfiche guarantees that Laserfiche Cloud will be available 99.9% of the time each calendar month ("Uptime"). Laserfiche measures Uptime by tracking the availability of certain Laserfiche Cloud systems components. Customer may view the status of these components at any time by visiting status.laserfiche.com. Uptime means Laserfiche Cloud functionality of 99.9% or more notwithstanding limitations listed in Section 6 of this SLA.

2. **REMEDIES FOR CLOUD SERVICE FAILURE**

If Laserfiche Cloud does not achieve the performance levels described in paragraph 1 ("Failure"), Subscriber may be eligible for a Service Credit. A "Service Credit" is a credit equivalent to the percent of a Subscriber's corresponding monthly Subscription Fees (1/12 of a Subscriber's annual fee) for Laserfiche Cloud correlating to Uptime Percentage in the following chart:

Uptime Percentage	**Service Credit Percentage**
Less than 99.9% but more than or equal to 99.5%	10%
Less than 99.5% but more than or equal to 99.0%	20%
Less than 99.0%	30%

Once awarded, a Service Credit will appear on a Subscriber's next month's invoice. Subscriber will have the right to terminate the Agreement if Laserfiche Cloud's Uptime in two or more months within a calendar year is lower than 85% in each of such months.

3. **SERVICE CREDIT REQUEST PROCEDURE**

To qualify for a Service Credit:

1. The request must be received by Laserfiche within 15 days of the end of the month for which a credit is sought.
2. Subscriber's account must be in good standing with all invoices paid and up to date.

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

To receive a Service Credit, Subscriber must submit a claim by emailing orders.cloud@laserfiche.com with the following information:

1. "SLA Credit Request" in the subject line;
2. Subscriber's name, account ID, administrator's email address and phone number;
3. The date(s) and time(s) of each qualifying incident you are claiming; and
4. Evidence that documents the errors and corroborates your claimed outage (confidential or sensitive information in these logs should be removed and replaced with asterisks).

Failure to provide all the requested information as required will disqualify the Service Credit claim.

4. **ERROR CORRECTION AND RESPONSE TIME FOR LASERFICHE SOFTWARE COMPONENTS UTILIZED WITH LASERFICHE CLOUD**

This SLA also covers Error correction support for Laserfiche Software features utilized with Laserfiche Cloud. "Error" means failure of Software to materially conform to its documentation, but excluding any nonconformity resulting from Subscriber's misuse, improper use, or unauthorized change of any Software; or the combining of Software with software not supplied or identified as compatible by Laserfiche. Errors are classified in Table A. Upon identification of an Error, Subscriber will notify their Solution Provider or Laserfiche and provide sufficient information to locate and reproduce the Error. Laserfiche will work with Subscriber's Solution Provider and/or Subscriber to determine the classification of such Error. No Service Credits are awarded in connection with Error correction. Laserfiche will use all reasonable commercial efforts to attempt to resolve any problems according to support level within the target times specified in Table A, but failure to meet target times will not constitute a failure to perform a material provision of this SLA. With respect to Subscribers who have Solution Providers, response times below begin upon the Solution Provider's notification with sufficient information to Laserfiche of Error and are dependent on Solution Provider's continuing collaboration with Laserfiche to resolve the problem.

Table A. Error Classification and Response/Communication Targets

Severity Level	***Definition***	***Goal Initial Response Goals*****	***Updates***
Urgent	Laserfiche Cloud is not operational for all customers.	Within 1 business hour	Customer will be updated 2x daily on progress
Critical	Software functionality is severely impaired even though it is operational at some level affecting multiple customers.	Within 4 business hours	Customer will be updated daily on progress
High	A major function in the software is not operational and no acceptable work-around is available, but Subscriber is able to do some production work even though performance and user quality is affected.	Within 8 business hours	Customer will be updated weekly on progress
Medium	There is a loss of a function or resource in software that does not seriously affect Subscriber's operations or schedules.	Within 10 business days	Customer will be updated weekly on progress
Low	All other issues with software.	As needed	Customer will be updated as needed

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

Enhancement	New features and functionality not currently existing will be reviewed by Laserfiche's development team and included in future releases if approved.	As needed	Customer will be updated as needed

**** Business hours as set forth in the following section.**

5. **ENGINEERING SUPPORT**

Laserfiche will maintain support engineers actively on duty monitoring Laserfiche's network operations and assisting customers. These engineers will provide support by e-mail or telephone 6 am – 6 pm PT, weekdays (except holidays).

6. **LIMITATIONS**

A. The minimum period of Failure eligible for a Service Credit is 10 minutes, and shorter periods will not be aggregated. In the event that multiple periods of Failure overlap in time, Service Credits will not be aggregated, and Subscriber will receive Service Credits only for the longest period of Failure. Laserfiche is not required to issue multiple Service Credits for a single incident.

B. Credits available pursuant to this SLA apply only to future Laserfiche Cloud delivery. Service Credits will not entitle Subscriber to any refunds and are not transferable or assignable. If Subscriber retains a credit balance on termination of the account in question, such credit is forfeited. Notwithstanding the foregoing, credits will not be applied against fees for professional services, bundled support, or setup fees.

C. Notwithstanding any provision to the contrary in this SLA, the following do not constitute Failures: (1) downtime during scheduled maintenance or Emergency Maintenance (as defined below) periods; (2) outages caused by acts or omissions of Subscriber, including its applications, operating system(s), equipment, or facilities, or by any use or user of Laserfiche Cloud authorized by Subscriber, or by Subscriber's use of any other software in its operating system(s); (3) outages caused by hackers, sabotage, viruses, worms, or other third-party wrongful actions; (4) DNS issues outside Laserfiche's control; (5) outages resulting from Internet anomalies; (6) outages resulting from Force Majeure events; and (7) failures during a "beta" period.

"Emergency Maintenance" refers to any corrective action intended to remedy conditions likely to cause severe Laserfiche Cloud degradation, as designated by Laserfiche in its sole discretion. Laserfiche will exercise reasonable efforts to inform Subscriber in advance before interrupting Laserfiche Cloud for Emergency Maintenance, but such notice is not guaranteed and failure thereof does not constitute Failure.

D. This SLA does not cover (without limitation): (a) network performance to Subscriber's physical location or Internet access point (such as a local DSL/cable modem) or (b) failures due to denial of service attacks. This SLA does not apply to any feature Laserfiche identifies as "beta" or to any software components made available with Laserfiche Cloud that run outside of the Laserfiche Cloud online service (such as client components installed on-premises).

E. Limitations & Warranty Disclaimer. The remedies set forth in this SLA are Subscriber's sole and exclusive remedies for any Failure or other loss of functionality of Laserfiche Cloud, or any Error with the Software, including without limitation for any breach of warranty, except as specifically set forth in the Agreement. The determination of any Failure or categorization of any Error is ultimately in the sole discretion of Laserfiche.

7. **TERMS OF SERVICE/THE AGREEMENT**

Terms defined in the Agreement will have the same meaning when used in this SLA. In the event of any conflict between this SLA and the Agreement, the Agreement will govern.

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

Laserfiche Data Processing Addendum

This Data Protection Addendum ("**DPA**") applies to the Processing of Personal Data by Laserfiche as part of Laserfiche's provision of Laserfiche cloud services subscribed by you ("**Cloud Services**") in accordance with the Laserfiche's NASPO ValuePoint Master Agreement by and between you and Laserfiche (the "**Agreement**"). The term "Laserfiche" and any other capitialized terms utilized in this DPA, but not defined herein, have their respective means as set forth in the Agreement.

This DPA is subject to the terms of the Agreement, incorporates by reference the Laserfiche Privacy Policy located at https://www.laserfiche.com/legal/privacy/, and will remain in force for the duration of the Subscription Term of the Cloud Services. In the event of any conflict or inconsistency between any of the terms of the Agreement or the Privacy Policy, on the one hand, and the terms of this DPA, on the other hand, the relevant terms of this DPA will take precedence with respect to the subject matter of this DPA.

1. Definitions

1.1 "Applicable Data Protection Law" means (a) as of May 25, 2018, Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation or GDPR); and (ii) any other data privacy or data protection law or regulation that applies to the Processing of Personal Data under this DPA.

1.2 "Binding Corporate Rules," "Controller," "Processor," "Data Subject," "Processing," "Personal Data," "Data Subject Request," and "Supervisory Authority" (or any of the equivalent terms) have the meaning set forth under Applicable Data Protection Law.

1.3 "EU Model Clauses" means the standard contractual clauses annexed to the EU Commission Decision 2010/87/EU of February 5, 2010 for the Transfer of Personal Data to Data Processors established in Third Countries under the Directive 95/46/EC, or any successor standard contractual clauses that may be adopted pursuant to an EU Commission decision.

1.4 "Laserfiche" means Compulink Management Center, Inc. doing business as Laserfiche.

1.5 "Laserfiche Affiliate" means the subsidiaries of Compulink Management Center, Inc. that may assist in the performance of the Cloud Services in accordance with this DPA.

1.6 "Laserfiche Reseller" or "Cloud Solution Provider" means an entity that has entered into an agreement with Laserfiche that, among other things, authorizes the entity to resell Laserfiche Cloud Services and, if applicable, provide certain services.

1.7 "Third Party Subprocessor" means direct and indirect third party subcontractors of Laserfiche, Laserfiche Affiliates, or any of Laserfiche or its Affiliate's subcontractors, which may Process Personal Data in accordance with this DPA, including, without limitation, Laserfiche Resellers. For the avoidance of doubt, a Laserfiche Affiliate is not a Third Party Subprocessor.

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

2. Obligations

2.1 You acknowledge and agree that with regard to the Processing of Personal Data under this DPA, Laserfiche is the Processor and you are the sole Controller of the Personal Data or you have obtained the authorization of relevant Controller(s) to agree to the Processing of Personal Data by Laserfiche as set forth in this DPA. You are responsible for the lawfulness of the Processing of Personal Data and compliance with your obligations as a Controller under Applicable Data Protection Law and in accordance with the features and functionality of the Cloud Service and the Documentation. You will not use the Cloud Services in conjunction with Personal Data to the extent that doing so would violate Applicable Data Protection Law.

2.2 You warrant that as the Controller to this DPA, you have all the necessary rights to provide the Personal Data to Laserfiche for the Processing to be performed in relation to the Cloud Services. To the extent required by Applicable Data Protection Law, you are responsible for ensuring that any necessary Data Subject consents to this Processing are obtained, and for ensuring that a record of such consents is maintained. Controller is responsible for promptly communicating to Processor when a Data Subject exercises a Data Subject Request. You have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which you acquired Personal Data.

2.3 During the Subscription Term, you appoint Laserfiche as a Processor with respect to the Personal Data you provide to Laserfiche under the Agreement and consent to the use of Third Party Subprocessors by Laserfiche in order to allow Laserfiche to fulfill its contractual obligations under the Agreement. Laserfiche is responsible for compliance with its obligations under this DPA and for compliance with its obligations as a Processor under Applicable Data Protection Law. Laserfiche is not responsible for determining the requirements of laws applicable to your business or that Laserfiche's provision of Cloud Services meet the requirements of such laws.

2.4 Laserfiche, Laserfiche Affiliates, and any Third Party Subprocessors, will Process Personal Data solely for the purpose of (i) providing Cloud Services in accordance with the Agreement and this DPA; (ii) complying with your documented written instructions, or (iii) complying with Laserfiche's regulatory obligations, all in accordance with the terms of this DPA. If Laserfiche feels that your documented written instructions violate Applicable Data Protection Law, Laserfiche may suspend the performance until you have modified or confirmed the lawfulness of such documented written instructions. If Laserfiche notifies you that either the documented written instructions or the expense for such written instructions are not feasible you may terminate the Cloud Services by providing Laserfiche with a written notice within one month after notification. Laserfiche will refund a prorated portion of any prepaid charges for the period after such termination date. Any Third Party used for purposes of Processing under the Agreement must be authorized by Laserfiche in writing.

3. Subject Matter, Data Subjects, Duration, and Types of Personal Data

3.1 The subject matter of the Processing is the performance of the Cloud Services for you pursuant to this Agreement.

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

3.2 Data Subjects whose Personal Data may be Processed in performing the Cloud Services include, without limitation, your representatives, end users, and persons of interest to your organization. For example, your employees, job applicants, contractors, partners, suppliers, customers and clients.

3.3 The duration of the Processing is for the duration of the Agreement except where otherwise required by applicable law, for Laserfiche to protect its rights or those of a third party, or due to a legitimate interest.

3.4 The types of Personal Data are determined and controlled by you, in your discretion, and may include, but are not limited to any information you provide for Processing that relates to (i) an identified or identifiable natural person; (ii) an identified or identifiable legal entity; or (iii) where such information is protected under Applicable Data Protection Law. Unless expressly specified in your order (including in the Documentation), your content may not include sensitive or special Personal Data that imposes specific data security or data protection obligations on Laserfiche in addition to or different from those specified in the Documentation.

4. The Rights of Data Subjects

4.1 To the extent permitted by law, Laserfiche will inform you of requests from Data Subjects exercising their rights under Applicable Data Protection Law addressed to Laserfiche regarding Personal Data. You will be responsible for responding to such Data Subject requests. Laserfiche will reasonably assist you in responding to such Data Subject requests. This includes requests to access, restrict, receive and transmit, delete or erase, rectify, block access to or object to Processing of specific Personal Data or sets of Personal Data. If a Data Subject or a regulator brings a claim directly against Laserfiche for a violation of Data Subject rights, you will indemnify Laserfiche for any cost, charge, damages, expenses or loss arising from such a claim.

4.2 In the event that electronic access is not available, you may submit a "service request" by emailing privacy@laserfiche.com, and provide detailed written instructions to Laserfiche (including the Personal Data necessary to identify the Data Subject) on how to reasonably assist with such Data Subject requests in relation to Personal Data held in your Services Environment. To the extent legally permitted, you will be responsible for any costs arising from Laserfiche's provision of such assistance.

5. Laserfiche Affiliates and Third Party Subprocessors

5.1 Subject to terms and restrictions set forth in this DPA, you agree and authorize that: (1) Laserfiche may engage Laserfiche Affiliates and Third Party Subprocessors to assist in the performance of the Cloud Services; and (2) Laserfiche, Laserfiche Affiliates, and Third Party Subprocessors may engage each of their respective direct and indirect subcontractors to assist in the performance of the Cloud Services. Laserfiche shall make available to you a current list of Third Party Subprocessors for the Cloud Services upon your written request.

5.2 Within 14 calendar days of Laserfiche providing such notice to you, you may object to the intended involvement of a Third Party Subprocessor or Laserfiche Affiliate in the performance of the Cloud Services, providing, in writing, objective justifiable grounds related to the ability of such Third Party Subprocessor or Laserfiche Affiliate to adequately protect Personal Data in accordance

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

with this DPA or Applicable Data Protection Law. You should submit this writing to privacy@laserfiche.com. In the event your objection is justified, you and Laserfiche will work together in good faith to find a mutually acceptable resolution to address your objections, including without limitation reviewing additional documentation supporting the Third Party Subprocessors' or Laserfiche Affiliate's compliance with this DPA or Applicable Data Protection Law, or delivering the Cloud Services without the involvement of such Third Party Subprocessor. To the extent you and Laserfiche do not reach a mutually acceptable resolution within a reasonable timeframe, you shall have the right to terminate the relevant Cloud Services (i) upon serving prior notice in accordance with the terms of the Agreement; (ii) without liability to you and Laserfiche and (iii) without relieving you from your payment obligations under the Agreement up to the date of termination. If the termination in accordance with this Section only pertains to a portion of Cloud Services under an order, you will enter into an amendment or replacement order to reflect such partial termination.

5.3 Laserfiche Affiliates and Third Party Subprocessors are required to abide by the same level of data protection and security as Laserfiche under this DPA as applicable to their Processing of your Personal Data. Laserfiche remains responsible at all times for requiring Laserfiche Affiliates and Third Party Subprocessors to perform obligations in compliance with the terms of this DPA and Applicable Data Protection Law.

6. Security Measures; Confidentiality

6.1 Each party agrees that it has implemented and will maintain appropriate technical and organizational measures to ensure a level of security of the Processing of Personal Data appropriate to the risk. These measures will take into account the nature, scope and purposes of Processing as specified in this DPA, as appropriate, and are intended to protect Personal Data against the risks inherent to the Processing of Personal Data in the performance of the Cloud Services, in particular risks from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored or otherwise Processed.

6.2 Laserfiche has specifically implemented system access, data access, transmission and encryption, input, data backup, and security oversight, enforcement and other security controls and measures specified in the Documentation. You are advised to carefully review the applicable Documentation to understand which specific security measures and practices apply to the particular Cloud Services ordered by you, and to ensure that these measures and practices are appropriate for the Processing of Personal Data pursuant to this DPA. You hereby instruct Laserfiche to Process Personal Data in accordance with the Documentation.

6.3 All parties hereto will ensure all such persons or parties, within their respective controls, that may have access to Personal Data subject to this DPA have signed an appropriate confidentiality agreement, are otherwise bound to a duty of confidentiality, or are subject to an appropriate statutory obligation of confidentiality.

7. Audits

7.1 Upon written request, Laserfiche may demonstrate the measures it has taken pursuant to Section 6 in relation to the Personal Data applicable to this DPA. Laserfiche will reasonably contribute to such audits by providing you or your Supervisory Authority with the information and assistance

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

reasonably necessary to conduct the audit, including any relevant records of Processing activities applicable to the Cloud Services ordered by you.

7.2 If a third party is to conduct the audit, the third party must be mutually agreed to by you and Laserfiche (except if such Third Party is a competent Supervisory Authority). Laserfiche will not unreasonably withhold its consent to a third party auditor requested by you. The third party must execute a written confidentiality agreement with Laserfiche in order to conduct the audit.

7.3 To request an audit, you must submit a detailed proposed audit plan to Laserfiche at least two weeks in advance of the proposed audit date. The proposed audit plan must describe the proposed scope, duration, and start date of the audit. Laserfiche will review the proposed audit plan and provide you with any concerns or questions. Laserfiche will reasonably assist you to formulate a final audit plan.

7.4 If the requested audit scope is addressed in a SSAE 18 or similar audit report issued by a qualified third party auditor within the prior twelve months and Laserfiche provides such report to you, you agree to accept the findings presented in the third party audit report in lieu of requesting an audit of the same controls covered by the report.

7.5 The audit must be conducted during regular business hours at the applicable facility, subject to the agreed final audit plan and Laserfiche's health and safety or other relevant policies, and may not unreasonably interfere with Laserfiche business activities.

7.6 You will provide Laserfiche any audit reports generated in connection with any audit, unless prohibited by Applicable Data Protection Law or otherwise instructed by a Supervisory Authority. You may use the audit reports only for the purposes of meeting your regulatory audit requirements and/or confirming compliance with the requirements of this DPA. The audit reports are Confidential Information of the parties under the terms of the Agreement.

7.7 Before the commencement of any audit or request under this Section, the parties will mutually agree upon the scope, timing, and duration of the audit in addition to the reimbursement rate for which you will be responsible. You agree to promptly notify Laserfiche with any information in regard to non-compliance during the course of an audit.

8. Incident Notification

8.1 To the extent Laserfiche becomes aware and determines that a security incident qualifies as a breach of security leading to the misappropriation or accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed on Laserfiche systems or the Services Environment that compromises the security, confidentiality or integrity of such Personal Data ("**Incident**"), Laserfiche will inform you of such Incident, as required by Applicable Data Protection Legislation. However, Laserfiche may not have the ability to evaluate or respond to security incidents where your Users are the source of unauthorized access or disclosure of Personal Data.

8.2 In order to address an Incident, Laserfiche defines escalation paths and response teams involving internal functions such as Information Security and the legal department. The goal of Laserfiche's Incident response will be to restore the confidentiality, integrity, and availability of the Services

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

Environment and the Personal Data that may be contained therein, and to establish root causes and remediation steps. Depending on the nature and scope of the Incident, Laserfiche may also involve and work with you and outside law enforcement to respond to the Incident.

9. **Return and Deletion of Personal Data upon Termination of Cloud Services.** Upon termination of the Cloud Services or upon expiry of the retrieval period following termination of the Cloud Services (if available), Laserfiche will delete all copies of Personal Data from the Services Environment by rendering such Personal Data unrecoverable, except as may be required by law and the Agreement.

10. **Cross-Border Data Transfers.** You acknowledge and agree that Personal Data will be stored and processed in the United States and other countries in which Laserfiche or its affiliates maintain facilities. To the extent your use of the Cloud Services involves Personal Data originating outside of the United States, you (a) acknowledge and consent to the transfer of Personal Data outside of its country of origin; (b) shall ensure that you have provided any required notice to, and obtained any required consent(s) from, individuals for the processing of their Personal Data by Laserfiche and for the transfer of their Personal Data outside of its country of origin; and (c) shall comply with all privacy and data protection laws applicable to such Personal Data. To the extent Personal Data is obtained from a country within the European Union ("EU"), you and Laserfiche hereby enter into the EU Model Clauses attached hereto as Exhibit A. Without limiting the foregoing, if you collect or transfer to Laserfiche Personal Data pertaining to data subjects in the EEA or Switzerland, you hereby represent and warrant that any transmission of data from you to Laserfiche is fully compliant with the GDPR; and that all such transmissions at any time are compliant with the Swiss Federal Act on Data Protection. You represent and warrant that, as part of your compliance with these laws, you have provided any legally required notices and obtained any legally required consents for their sharing, transmission, and processing of Personal Data with, to, and by Laserfiche. Without limiting the foregoing, you represent and warrant that you have notified all such data subjects of and obtained all such data subjects' explicit consent to all of the intended uses of such Personal Data with respect to the Cloud Services, as set forth in Laserfiche's then current Privacy Policy.

11. **Limitation of Liability**. Each party's liability (and each of its Affiliate's) liability taken together in the aggregate, arising out of or related to this DPA whether in contract, tort, or under any other theory of lability, is subject to the limitation of liability provisions of the Agreement. Any reference in such limitation of liability provisions to the liability of a party means the aggregate liability of that party and all of its affiliates (including Controller Affiliates) under the Agreement and all DPAs taken together.

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

Exhibit A

Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

The entity identified as "you" in the Addendum

(the "data exporter")

and

Laserfiche

(the "data importer")

each a "party"; together "the parties",

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) '*the data exporter'* means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

(e) '*the applicable data protection law*' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

(and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer[1]

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees

[1] Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, *inter alia,* internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

   The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.
2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.
4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

Data exporter
The data exporter is the entity identified as "you" in the Addendum.

Data importer
The data importer is Laserfiche.

Data subjects
Data subjects include the data exporter's users and employees.

Categories of data
The personal data relating to individuals which is processed by the data importer through the data exporter's use of its services. The data exporter determines the types of data per each product or service used.

Processing operations
The personal data transferred will be subject to the following basic processing activities (as applicable):

- Providing Cloud Services.

Laserfiche may use subprocessors in connection with its processing activities for Customer.

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties. By signing the signature page on page 1 of this Addendum, the parties will be deemed to have signed this Appendix 2.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c):

A. Data importer shall implement appropriate technical and organizational measures to protect personal data against accidental loss, destruction or alteration, unauthorized disclosure or access, or unlawful destruction, including the policies, and procedures and internal controls set forth in this Appendix 2.

B. More specifically, data importer's technical and organizational measures shall include:

Access Control of Processing Areas

Data importer shall implement appropriate measures to prevent unauthorized persons from gaining access to the data processing equipment (namely telephones, database and application servers and related hardware) where the personal data are processed or used, including:

- establishing security areas and physical controls;
- protection and restriction of access paths;
- establishing access authorizations for employees and third parties;
- access to the data center where personal data are hosted is logged, monitored, and tracked; and
- the data center where personal data are hosted is secured by a security alarm system, and other appropriate security measures.

Access Control to Data Processing Systems

Data importer shall implement appropriate measures to prevent data processing systems where personal data are processed and used from being used by unauthorized persons, including:

- use of industry standard encryption technologies;
- automatic temporary lock-out of user terminal if left idle, identification and password required to reopen;
- automatic temporary lock-out of the user ID when several erroneous passwords are entered, log file of events, monitoring of break-in-attempts (alerts); and
- access to data content is logged, monitored, and tracked.

Access Control to Use Specific Areas of Data Processing Systems

Data importer shall implement appropriate measures to help ensure that the persons entitled to use data processing system where personal data are processed and used are only able to access the data within the scope and to the extent covered by their respective access permission (authorization) and that personal data cannot be read, copied or modified or removed without authorization. This shall be accomplished by various measures including:

- employee policies and training in respect of each employee's access rights to the personal data;
- allocation of individual terminals and /or terminal user, and identification characteristics exclusive to specific functions;
- monitoring capability in respect of individuals who delete, add or modify the personal data;

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

- release of data only to authorized persons, including allocation of differentiated access rights and roles;
- use of industry standard encryption technologies; and
- control of files, controlled and documented destruction of data.

Availability Control

Data importer shall implement appropriate measures to help ensure that personal data are protected from accidental destruction or loss, including:

- infrastructure redundancy; and
- backup is stored at an alternative site and available for restore in case of failure of the primary system

Transmission Control

Data importer shall implement appropriate measures to prevent the personal data from being read, copied, altered or deleted by unauthorized parties during the transmission thereof or during the transport of the data media. This is accomplished by various measures including:

- use of industry standard firewall, VPN and encryption technologies to protect the gateways and pipelines through which the data travels;
- providing user alert upon incomplete transfer of data (end to end check); and
- data transmissions are logged, monitored and tracked.

Input Control

Data importer shall implement appropriate input control measures, including:

- an authorization policy for the input, reading, alteration and deletion of data;
- authentication of the authorized personnel;
- protective measures for the data input into memory, as well as for the reading, alteration and deletion of stored data;
- utilization of unique authentication credentials or codes (passwords) and 2 factor authentication;
- providing that entries to data processing facilities (the rooms housing the computer hardware and related equipment) are kept locked;
- automatic log-off of user ID's that have not been used for a substantial period of time;
- proof established within data importer’s organization of the input authorization; and
- electronic recording of entries.

Separation of Processing for different Purposes

Data importer shall implement appropriate measures to help ensure that data collected for different purposes can be processed separately, including:

- access to data is separated through application security for the appropriate users;
- modules within the data importer’s data base separate which data is used for which purpose, i.e. by functionality and function;
- at the database level, data is stored in different normalized tables, separated per module, per controller or function they support; and

Docusign Envelope ID: 229AC2E7-AA21-4844-93B9-053D326123FA

- interfaces, batch processes and reports are designed for only specific purposes and functions, so data collected for specific purposes is processed separately.

Documentation

Data importer will keep documentation of technical and organizational measures in case of audits and for the conservation of evidence. Data importer shall implement appropriate measures to help ensure that its employees, agents, and subprocessors are aware of and comply with the technical and organizational measures set forth in this Appendix 2.

Monitoring

Data importer shall implement appropriate measures to monitor access restrictions to data importer's system administrators and to help ensure that they act in accordance with instructions received. This is accomplished by various measures including:

- individual appointment of system administrators;
- adoption of measures to register system administrators' access logs to the infrastructure and keep them secure;
- audits of system administrators' activity to assess compliance with assigned tasks and applicable laws; and keeping an updated list with system administrators' identification details (e.g. name, surname, function or organizational area) and tasks assigned.