CLOUD SECURITY ALLIANCE (CSA) CLOUD CONTROLS MATRIX (CCM) SUBMISSION FOR LASERFICHE CLOUD

JULY 2018

Copyright 2018 Laserfiche

Tables of Contents

Copyright 2018 Laserfiche

Introduction

Laserfiche Cloud is hosted by AWS in its entirety, including all the virtual machines, storage, and networking systems used during service operation. Laserfiche Cloud components do not directly communicate with systems operated out of the Laserfiche corporate network. As Laserfiche Cloud is a fully managed SaaS application suite, access to AWS resources that support Laserfiche Cloud is restricted to Laserfiche personnel responsible for the management and operation of the service.

The Laserfiche suite of software applications consists of web applications, application servers, client applications that run on Microsoft Windows, and apps that run on mobile devices running Android, iOS, and Microsoft's Universal Windows Platform (UWP) stack. Laserfiche also distributes a SDK for developers to write applications that integrate with the Laserfiche platform. Laserfiche Cloud removes the need for customers to install and maintain their own Laserfiche application servers and associated databases and infrastructure, while retaining compatibility with existing Laserfiche desktop clients and other on-premises Laserfiche applications, Laserfiche apps for mobile devices, and many third-party applications that use the Laserfiche SDK.

The Laserfiche web client (also called "Web Access") provides access to Laserfiche repositories and the content management features of Laserfiche, such as search, document storage and retrieval, document imaging, records management, and library services. Document scanning is supported by the Laserfiche Scanning downloadable program, and gives users the ability to scan document images from their web browser. Laserfiche Public Portal is a streamlined, intuitive interface for accessing document repositories that allows users to view, download, and search documents that have been published by the user entity to a secure area.

Laserfiche Audit Trail enables users to design and view reports of Laserfiche repository audit log data. The repository audit log includes details of user actions, including viewing, modifying, creating, and deleting documents, and similar operations on metadata and other repository objects.

Laserfiche Forms is an electronic forms and business process automation (BPA) application available in Laserfiche Cloud. Laserfiche Forms allows business users to design web forms quickly and without any programming, while offering form designers the ability to customize the appearance and behavior of forms extensively. Laserfiche Forms processes are collections of discrete actions organized in a data-flow graph, and specify how data submitted via electronic forms are transformed, transmitted, and tracked to automate business processes. Users can build approval and routing processes using an intuitive drag-and-drop interface.

The Laserfiche Account Control System (ACS) is the authentication, authorization, and user management interface for Laserfiche Cloud. Laserfiche ACS consists of a web application component that hosts a web-based sign-in page, and provides a web interface for controlling user entity onboarding, account management, user and group management, and billing and payment settings. Additional back-end components implement accounting, authorization, and identity management services.

Copyright 2018 Laserfiche

Compliance

Certified independent auditors assess the effectiveness of Laserfiche's controls modeled on the AICPA's Trust Services Criteria, culminating in a Service Organization Controls 2 (SOC 2) report, annually. The SOC 2 reports are available on request.

Cloud Control Matrix (CCM) Response

The following table provides the Laserfiche responses to the Cloud Security Alliance (CSA) Cloud Control Matrix (CCM).

Application and Interface Security

Control Domain	Control ID	Control Specification	Laserfiche Cloud Response
Application & Interface Security Application Security	AIS-01	Applications and programming interfaces (APIs) shall be designed, developed, deployed, and tested in accordance with leading industry standards (e.g., OWASP for web applications) and adhere to applicable legal, statutory, or regulatory compliance obligations.	Laserfiche follows industry standards for change approval and change testing prior to deployment to production. Laserfiche develops software using an Agile software development methodology while also incorporating secure software development lifecycle (SDLC) standards at defined points in the product development process. Risk assessments are performed on changes before deployment to production environments.
Application & Interface Security Customer Access Requirements	AIS-02	Prior to granting customers access to data, assets, and information systems, identified security, contractual, and regulatory requirements for customer access shall be addressed.	Customers are responsible for establishing internal procedures to help ensure that information sent to Laserfiche is complete, properly authorized, and in accordance with Laserfiche's requirements and applicable laws. These procedures are the responsibility of users of the system. Customers administer access to their instance of Laserfiche Cloud. Laserfiche documents user entity control responsibilities in its service documentation.
Application & Interface Security Data Integrity	AIS-03	Data input and output integrity routines (i.e., reconciliation and edit checks) shall be implemented for application interfaces and databases to prevent manual or systematic processing errors, corruption of data, or misuse.	Data validation logic is implemented in application code in the front-end, back-end, and data storage layers, where appropriate to maintain data integrity. Validation logic may include checks of length, type, and format, as appropriate.

Copyright 2018 Laserfiche

Control Domain	Control ID	Control Specification	Laserfiche Cloud Response
Application & Interface Security Data Security / Integrity	AIS-04	Policies and procedures shall be established and maintained in support of data security to include (confidentiality, integrity, and availability) across multiple system interfaces, jurisdictions, and business functions to prevent improper disclosure, alteration, or destruction.	Laserfiche's information security policies and standards are reviewed regularly and updated as needed. The Information Security Policy defines an information security management system aligned with ISO 27001 and includes policies on areas such as identifying and classifying assets, assessing risks to information and computing assets, managing third party vendor risks, requiring standards for security technologies such as encryption, and responding to security incidents.

Copyright 2018 Laserfiche

Audit Assurance & Compliance

Control Domain	Control ID	Control Specification	Laserfiche Cloud Response
Audit Assurance & Compliance Audit Planning	AAC-01	Audit plans shall be developed and maintained to address business process disruptions. Auditing plans shall focus on reviewing the effectiveness of the implementation of security operations. All audit activities must be agreed upon prior to executing any audits.	Based on a risk assessment, Laserfiche identifies audit areas that are approved by Company management before an audit commences. Audit plans define the scope of audits, and assess and limit the allowed potential impact to operations by audit procedures.
Audit Assurance & Compliance Independent Audits	AAC-02	Independent reviews and assessments shall be performed at least annually to ensure that the organization addresses nonconformities of established policies, standards, procedures, and compliance obligations.	A third-party CPA firm performs an annual SOC 2 attestation annually. The SOC 2 reports are available to customers upon request under NDA. A third party performs external penetration tests for Laserfiche Cloud at least annually. Risk assessments are performed annually. Laserfiche uses a third-party vendor to conduct external penetration testing of the Laserfiche Cloud system.
Audit Assurance & Compliance Information System Regulatory Mapping	AAC-03	Organizations shall create and maintain a control framework which captures standards, regulatory, legal, and statutory requirements relevant for their business needs. The control framework shall be reviewed at least annually to ensure changes that could affect the business processes are reflected.	The Laserfiche internal control framework is designed according to industry best-practices and standards. Controls are designed to address the AICPA Trust Services Criteria and are aligned with ISO 27001. Laserfiche development policies are reviewed at least annually.

Copyright 2018 Laserfiche

Business Continuity Management & Operational Resilience

Control Domain	Control ID	Control Specification	Laserfiche Cloud Response
Business Continuity Management & Operational Resilience Business Continuity Planning	BCR-01	A consistent unified framework for business continuity planning and plan development shall be established, documented, and adopted to ensure all business continuity plans are consistent in addressing priorities for testing, maintenance, and information security requirements. Requirements for business continuity plans include the following: • Defined purpose and scope, aligned with relevant dependencies • Accessible to and understood by those who will use them • Owned by a named person(s) who is responsible for their review, update, and approval • Defined lines of communication, roles, and responsibilities • Detailed recovery procedures, manual work-around, and reference information • Method for plan invocation	Laserfiche policies include backup and recovery to support maintaining the continuity of operations during a disaster event. The Laserfiche Cloud backup and recovery system is designed to backup customer data at regular intervals. Backup operations are initiated automatically without needing manual intervention by the engineering team. Backup data is encrypted and access to encrypted backup sets are limited to restoration components. Backup data is replicated across multiple datacenters for resiliency.
Business Continuity Management & Operational Resilience Business Continuity Testing	BCR-02	Business continuity and security incident response plans shall be subject to testing at planned intervals or upon significant organizational or environmental changes. Incident response plans shall involve impacted customers (tenant) and	Restoration tests of backups are performed at regular intervals to validate the correctness of the backup and restoration logic. Evidence of testing is recorded in a ticketing system. An Incident management policy describes the procedure for recording, classifying, prioritizing, escalating, and concluding incident response. Laserfiche maintains a security incident response plan and performs an annual

Copyright 2018 Laserfiche

Control Domain	Control ID	Control Specification	Laserfiche Cloud Response
		other business relationships that represent critical intra-supply chain business process dependencies.	test to ensure that parties are ready to execute the plan in case of a security incident.
Business Continuity Management & Operational Resilience Power / Telecommunications	BCR-03	Data center utilities services and environmental conditions (e.g., water, power, temperature and humidity controls, telecommunications, and internet connectivity) shall be secured, monitored, maintained, and tested for continual effectiveness at planned intervals to ensure protection from unauthorized interception or damage, and designed with automated fail-over or other redundancies in the event of planned or unplanned disruptions.	Laserfiche Cloud is hosted in its entirety by Amazon Web Services (AWS). AWS provides physical and environmental controls for securing, monitoring, maintaining, and testing of AWS data centers that provide infrastructure services. Laserfiche reviews the latest Service Organization Control (SOC) report for third party companies' services on an annual basis.
Business Continuity Management & Operational Resilience Documentation	BCR-04	Information system documentation (e.g., administrator and user guides, and architecture diagrams) shall be made available to authorized personnel to ensure the following: • Configuring, installing, and operating the information system • Effectively using the system's security features	Product and service documentation for Laserfiche Cloud is available online to customers and includes configuration information on securing their content within Laserfiche Cloud.
Business Continuity Management & Operational Resilience Environmental Risks	BCR-05	Physical protection against damage from natural causes and disasters, as well as deliberate attacks, including fire, flood, atmospheric electrical discharge, solar induced geomagnetic storm, wind, earthquake, tsunami, explosion, nuclear	Laserfiche Cloud services that require high availability are deployed across multiple availability zones within an AWS Region. Services that are not deployed across multiple availability zones are monitored and can trigger an incident management process to restore services in alternate availability zones.

Copyright 2018 Laserfiche

Control Domain	Control ID	Control Specification	Laserfiche Cloud Response
		accident, volcanic activity, biological hazard, civil unrest, mudslide, tectonic activity, and other forms of natural or man-made disaster shall be anticipated, designed, and have countermeasures applied.	
Business Continuity Management & Operational Resilience Equipment Location	BCR-06	To reduce the risks from environmental threats, hazards, and opportunities for unauthorized access, equipment shall be kept away from locations subject to high probability environmental risks and supplemented by redundant equipment located at a reasonable distance.	Laserfiche Cloud services that require high availability are deployed across multiple availability zones within an AWS Region. Services that are not deployed across multiple availability zones are monitored and can trigger an incident management process to restore services in alternate availability zones.
Business Continuity Management & Operational Resilience Equipment Maintenance	BCR-07	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for equipment maintenance ensuring continuity and availability of operations and support personnel.	Capacity reviews are performed regularly to support appropriate planning for CPU, disk space, and other key areas.
Business Continuity Management & Operational Resilience Equipment Power Failures	BCR-08	Protection measures shall be put into place to react to natural and man-made threats based upon a geographically-specific business impact assessment.	Laserfiche Cloud services that require high availability are deployed across multiple availability zones within an AWS Region. Services that are not deployed across multiple availability zones are monitored and can trigger an incident management process to restore services in alternate availability zones.
Business Continuity Management & Operational Resilience Impact Analysis	BCR-09	There shall be a defined and documented method for determining the impact of any disruption to the organization (cloud provider, cloud consumer) that must incorporate the following: • Identify critical	A service health monitoring system monitors system capacity and service status and generates alerts for engineers when conditions deviate from expected normal operating boundaries. An incident response plan determines the process for reviewing high-priority alerts. Senior engineers perform periodic review of incident responses to verify that

Copyright 2018 Laserfiche

Control Domain	Control ID	Control Specification	Laserfiche Cloud Response
		products and services • Identify all dependencies, including processes, applications, business partners, and third party service providers • Understand threats to critical products and services • Determine impacts resulting from planned or unplanned disruptions and how these vary over time • Establish the maximum tolerable period for disruption • Establish priorities for recovery • Establish recovery time objectives for resumption of critical products and services within their maximum tolerable period of disruption • Estimate the resources required for resumption"	response times meet service level objectives. Information about the current availability of Laserfiche Cloud and the individual services that comprise the service offering is published to a status website. Information about upcoming planned system maintenance operations is also published on the status website.
Business Continuity Management & Operational Resilience Policy	BCR-10	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for appropriate IT governance and service management to ensure appropriate planning, delivery, and support of the organization's IT capabilities supporting business functions, workforce, and/or customers based on industry acceptable standards (i.e., ITIL v4 and COBIT 5). Additionally, policies and procedures shall include defined roles and	Laserfiche's information security policies and standards are reviewed regularly and updated as needed. The Information Security Policy defines an information security management system aligned with ISO 27001 and includes policies on areas such as identifying and classifying assets, assessing risks to information and computing assets, managing third party vendor risks, requiring standards for security technologies such as encryption, and responding to security incidents.. Information policies and procedures are accessible to all Company employees via the Company intranet. A formal security awareness program is in place to make all employees aware of the company's security policy, standards, and obligations to users. On an annual basis, training

Control Domain	Control ID	Control Specification	Laserfiche Cloud Response
		responsibilities supported by regular workforce training.	requirements are evaluated for key members of the development staff and provided accordingly. All engineers receive training on secure software development practices.
Business Continuity Management & Operational Resilience Retention Policy	BCR-11	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for defining and adhering to the retention period of any critical asset as per established policies and procedures, as well as applicable legal, statutory, or regulatory compliance obligations. Backup and recovery measures shall be incorporated as part of business continuity planning and tested accordingly for effectiveness.	Data backups are retained for a limited time to support system recovery operations in the event of a disaster or other contingency. Backups sets that exceed the defined retention are removed automatically by batch processes. User entities may request that their data stored in Laserfiche Cloud be permanently deleted. Requests for permanent deletion of data are authenticated before execution.

Copyright 2018 Laserfiche

Change Control & Configuration Management

Control Domain	Control ID	Control Specification	Laserfiche Cloud Response
Change Control & Configuration Management New Development / Acquisition	CCC-01	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to ensure the development and/or acquisition of new data, physical or virtual applications, infrastructure network, and systems components, or any corporate, operations and/or data center facilities have been pre-authorized by the organization's business leadership or other accountable business role or function.	Laserfiche has defined and documented a formalized change management process to promote and maintain system stability when deploying software and updating software and system configurations.
Change Control & Configuration Management Outsourced Development	CCC-02	External business partners shall adhere to the same policies and procedures for change management, release, and testing as internal developers within the organization (e.g., ITIL service management processes).	Laserfiche management monitors the services performed by its subservice organizations to ensure the quality of the delivered service and that the controls it expects to be implemented at subservice organizations are in operation. Management also communicates with the subservice organizations to relay any issues or concerns, if any.
Change Control & Configuration Management Quality Testing	CCC-03	Organizations shall follow a defined quality change control and testing process (e.g., ITIL Service Management) with established baselines, testing, and release standards that focus on system availability, confidentiality, and integrity of systems and services.	The Laserfiche software development standards mandate that specific security development and quality assurance activities occur at key phases of the software development process to minimize the scope, impact, and prevalence of security flaws in the design and implementation of software products. Laserfiche technical product owners and other development staff create requirements for new features to meet the objectives specified by product roadmaps. All change requests and their requirements are tracked in a centralized ticketing system. Request for changes to software that do not have functional requirements, or do not impact user-facing interfaces are also tracked using the ticketing system. All

Copyright 2018 Laserfiche

Control Domain	Control ID	Control Specification	Laserfiche Cloud Response
			changes are approved and prioritized by senior engineering personnel, and high risk and high integrity code undergoes code review before changes are merged into production code branches. Quality assurance (QA) activity is performed by both dedicated QA personnel and software developers on an ongoing basis, and evidence of testing is recorded in the ticketing system. All changes are tested by a qualified individual in Laserfiche Development who is not involved in the development of the change.
Change Control & Configuration Management Unauthorized Software Installations	CCC-04	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to restrict the installation of unauthorized software on organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.	The Laserfiche Information Security Policy documents the acceptable use policy of Company information technology resources, including desktop, laptop and end user controls.
Change Control & Configuration Management Production Changes	CCC-05	Policies and procedures shall be established for managing the risks associated with applying changes to: • Business-critical or customer (tenant)-impacting (physical and virtual) applications and system-system interface (API) designs and configurations. • Infrastructure network and systems components. Technical measures shall be implemented to provide assurance that all changes directly correspond to a registered change request, business-	Laserfiche has defined and documented a formalized change management process to promote and maintain system stability when deploying software and updating software and system configurations. Requests to deploy new or updated software packages are documented, tested, and approved using a production change control process that supplements the software development process. Changes to software products are not automatically or immediately deployed to production environments, and are reviewed for adherence to the change process and appropriateness by senior personnel before deployment. Laserfiche IT maintains a change management process to minimize business impact or disruptions when changes are made in Laserfiche's production IT environment. Change requests must be documented and include assigned personnel for

Control Domain	Control ID	Control Specification	Laserfiche Cloud Response
		critical or customer (tenant), and/or authorization by, the customer (tenant) as per agreement (SLA) prior to deployment.	implementation, testing procedures, and a rollback plan.

Copyright 2018 Laserfiche

Data Security & Information Lifecycle Management

Control Domain	Control ID	Control Specification	Laserfiche Cloud Response
Data Security & Information Lifecycle Management Classification	DSI-01	Data and objects containing data shall be assigned a classification by the data owner based on data type, value, sensitivity, and criticality to the organization.	The Laserfiche Information Security Policy defines a data sensitivity classification scheme for data stored on Laserfiche systems. Customer data is classified at the highest level of sensitivity, with corresponding controls to safeguard the data.
Data Security & Information Lifecycle Management Data Inventory / Flows	DSI-02	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to inventory, document, and maintain data flows for data that is resident (permanently or temporarily) within the service's geographically distributed (physical and virtual) applications and infrastructure network and systems components and/or shared with other third parties to ascertain any regulatory, statutory, or supply chain agreement (SLA) compliance impact, and to address any other business risks associated with the data. Upon request, provider shall inform customer (tenant) of compliance impact and risk, especially if customer data is used as part of the services.	Access to the Laserfiche Cloud production system is logically and physically segregated from the Laserfiche corporate network. Customer data is logically segregated between accounts by using separately allocated databases and virtual disk volumes.
Data Security & Information Lifecycle Management Ecommerce Transactions	DSI-03	Data related to electronic commerce (ecommerce) that traverses public networks shall be appropriately classified and protected from fraudulent activity, unauthorized disclosure, or modification in such a manner to prevent contract dispute and compromise of data.	All customer interfaces to Laserfiche Cloud, including web, mobile device and desktop application access paths, are encrypted using TLS encryption.

Copyright 2018 Laserfiche

Control Domain	Control ID	Control Specification	Laserfiche Cloud Response
Data Security & Information Lifecycle Management Handling / Labeling / Security Policy	DSI-04	Policies and procedures shall be established for the labeling, handling, and security of data and objects which contain data. Mechanisms for label inheritance shall be implemented for objects that act as aggregate containers for data.	The Laserfiche Information Security Policy defines a data sensitivity classification scheme for data stored on Laserfiche systems. A master list of the production system inventory is maintained within an inventory management system. The inventory management system keeps track of operating systems, all installed software, databases, version information, etc., to support vulnerability identification and mitigation, as well as other risk management activities.
Data Security & Information Lifecycle Management Non-Production Data	DSI-05	Production data shall not be replicated or used in non-production environments. Any use of customer data in non-production environments requires explicit, documented approval from all customers whose data is affected, and must comply with all legal and regulatory requirements for scrubbing of sensitive data elements.	Laserfiche employees are prohibited from accessing customer production data without a customer's request and authorization. All attempts by Laserfiche employees to access customer production data are detected by monitoring tools that automatically transmit alerts to the engineering team supporting Laserfiche Cloud for review and follow-up, as applicable.
Data Security & Information Lifecycle Management Ownership / Stewardship	DSI-06	All data shall be designated with stewardship, with assigned responsibilities defined, documented, and communicated.	The Laserfiche Information Security Policy defines a data sensitivity classification scheme for data stored on Laserfiche systems.
Data Security & Information Lifecycle Management Secure Disposal	DSI-07	Policies and procedures shall be established with supporting business processes and technical measures implemented for the secure disposal and complete removal of data from all storage media, ensuring data is not recoverable by any computer forensic means.	Data for trial customers and subscription customers are removed after the end of the trial period and upon written notice by the customer, respectively.

Copyright 2018 Laserfiche

Datacenter Security

Control Domain	Control ID	Control Specification	Laserfiche Cloud Response
Datacenter Security Asset Management	DCS-01	Assets must be classified in terms of business criticality, service-level expectations, and operational continuity requirements. A complete inventory of business-critical assets located at all sites and/or geographical locations and their usage over time shall be maintained and updated regularly, and assigned ownership by defined roles and responsibilities.	Laserfiche utilizes the AWS platform for its production environment and does not operate its own datacenters. 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.
Datacenter Security Controlled Access Points	DCS-02	Physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks, and security patrols) shall be implemented to safeguard sensitive data and information systems.	See the response for control DCS-01.
Datacenter Security Equipment Identification	DCS-03	Automated equipment identification shall be used as a method of connection authentication. Location-aware technologies may be used to validate connection authentication integrity based on known equipment location.	See the response for control DCS-01.
Datacenter Security Off-Site Authorization	DCS-04	Authorization must be obtained prior to relocation or transfer of hardware, software, or data to an offsite premises.	See the response for control DCS-01.
Datacenter Security Off-Site Equipment	DCS-05	Policies and procedures shall be established for the secure disposal of equipment (by asset type)	See the response for control DCS-01.

Copyright 2018 Laserfiche

Control Domain	Control ID	Control Specification	Laserfiche Cloud Response
		used outside the organization's premises. This shall include a wiping solution or destruction process that renders recovery of information impossible. The erasure shall consist of a full overwrite of the drive to ensure that the erased drive is released to inventory for reuse and deployment, or securely stored until it can be destroyed.	
Datacenter Security Policy	DCS-06	Policies and procedures shall be established, and supporting business processes implemented, for maintaining a safe and secure working environment in offices, rooms, facilities, and secure areas storing sensitive information.	See the response for control DCS-01.
Datacenter Security Secure Area Authorization	DCS-07	Ingress and egress to secure areas shall be constrained and monitored by physical access control mechanisms to ensure that only authorized personnel are allowed access.	See the response for control DCS-01.
Datacenter Security Unauthorized Persons Entry	DCS-08	Ingress and egress points such as service areas and other points where unauthorized personnel may enter the premises shall be monitored, controlled and, if possible, isolated from data storage and processing facilities to prevent unauthorized data corruption, compromise, and loss.	See the response for control DCS-01.
Datacenter Security User Access	DCS-09	Physical access to information assets and functions by users and	See the response for control DCS-01.

Copyright 2018 Laserfiche

Control Domain	Control ID	Control Specification	Laserfiche Cloud Response
		support personnel shall be restricted.	

Copyright 2018 Laserfiche

Encryption & Key Management

Control Domain	Control ID	Control Specification	Laserfiche Cloud Response
Encryption & Key Management Entitlement	EKM-01	Keys must have identifiable owners (binding keys to identities) and there shall be key management policies.	Laserfiche has defined SSH key pair and AWS access key management policies. A key management system prevents users from accessing private keys assigned to other users.
Encryption & Key Management Key Generation	EKM-02	Policies and procedures shall be established for the management of cryptographic keys in the service's cryptosystem (e.g., lifecycle management from key generation to revocation and replacement, public key infrastructure, cryptographic protocol design and algorithms used, access controls in place for secure key generation, and exchange and storage including segregation of keys used for encrypted data or sessions). Upon request, provider shall inform the customer (tenant) of changes within the cryptosystem, especially if the customer (tenant) data is used as part of the service, and/or the customer (tenant) has some shared responsibility over implementation of the control.	All data and authentication encryption keys are rotated annually. Documentation of authentication key rotation is maintained in the ticketing system.
Encryption & Key Management Sensitive Data Protection	EKM-03	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for the use of encryption protocols for protection of sensitive data in storage (e.g., file servers, databases, and end-user workstations), data in use (memory), and data in transmission (e.g., system	All customer interfaces to Laserfiche Cloud, including web, mobile device and desktop application access paths, are encrypted using TLS encryption.

Copyright 2018 Laserfiche

Control Domain	Control ID	Control Specification	Laserfiche Cloud Response
		interfaces, over public networks, and electronic messaging) as per applicable legal, statutory, and regulatory compliance obligations.	
Encryption & Key Management Storage and Access	EKM-04	Platform and data-appropriate encryption (e.g., AES-256) in open/validated formats and standard algorithms shall be required. Keys shall not be stored in the cloud (i.e., at the cloud provider in question), but maintained by the cloud consumer or trusted key management provider. Key management and key usage shall be separated duties.	Laserfiche has defined SSH key pair and AWS access key management policies. The policy prohibits storing private SSH key files on a network file share, FTP site, or other directory where files may be accessed remotely. A manager with responsibility for Service operations maintains a catalog of SSH keys.

Governance and Risk Management

Control Domain	Control ID	Control Specification	Laserfiche Cloud Response
Governance and Risk Management Baseline Requirements	GRM-01	Baseline security requirements shall be established for developed or acquired, organizationally-owned or managed, physical or virtual, applications and infrastructure system and network components that comply with applicable legal, statutory, and regulatory compliance obligations. Deviations from standard baseline configurations must be authorized following change management policies and procedures prior to deployment, provisioning, or use. Compliance with security baseline requirements must be reassessed at least annually unless an alternate frequency has been established and authorized based on business needs.	Policies and procedures are maintained, reviewed, and updated, if applicable, annually by relevant organizations. Policies and procedures are communicated via the Company intranet and made available to employees. Information Security and Risk Management policies and procedures are reviewed and approved annually by Company leadership, or when there are significant changes to the organization or risk environment that warrant a review. Policies are communicated to employees using a combination of training, internal documentation, and regular reviews.
Governance and Risk Management Data Focus Risk Assessments	GRM-02	Risk assessments associated with data governance requirements shall be conducted at planned intervals and shall consider the following: • Awareness of where sensitive data is stored and transmitted across applications, databases, servers, and network infrastructure • Compliance with defined retention periods and end-of-life disposal requirements • • Data classification	IT Management updates the risk assessment of the Company's IT environment (people, processes, and technology) at least annually, and considers performing an additional risk assessment when there is a significant change to the Laserfiche Cloud service environment.

Copyright 2018 Laserfiche

Control Domain	Control ID	Control Specification	Laserfiche Cloud Response
		and protection from unauthorized use, access, loss, destruction, and falsification	
Governance and Risk Management Management Oversight	GRM-03	Managers are responsible for maintaining awareness of, and complying with, security policies, procedures, and standards that are relevant to their area of responsibility.	See the response for control GRM-01.
Governance and Risk Management Management Program	GRM-04	An Information Security Management Program (ISMP) shall be developed, documented, approved, and implemented that includes administrative, technical, and physical safeguards to protect assets and data from loss, misuse, unauthorized access, disclosure, alteration, and destruction. The security program shall include, but not be limited to, the following areas insofar as they relate to the characteristics of the business: • Risk management • Security policy • Organization of information security • Asset management • Human resources security • Physical and environmental security • Communications and operations management • Access control • Information systems acquisition, development, and maintenance	The Laserfiche Information Security Management (ISM) program and related information security policies and procedures have been documented and are updated by management continually as business needs and the wider cybersecurity threat environment change.
Governance and Risk	GRM-05	Executive and line	The President and CTO are supported by

Control Domain	Control ID	Control Specification	Laserfiche Cloud Response
Management Management Support/Involvement		management shall take formal action to support information security through clearly-documented direction and commitment, and shall ensure the action has been assigned.	the Chief Information Officer, who is responsible for IT and security governance, and the Information security Officer (ISO), who is responsible for coordinating and overseeing Company-wide compliance with policies and procedures regarding information assets.
Governance and Risk Management Policy	GRM-06	Information security policies and procedures shall be established and made readily available for review by all impacted personnel and external business relationships. Information security policies must be authorized by the organization's business leadership (or other accountable business role or function) and supported by a strategic business plan and an information security management program inclusive of defined information security roles and responsibilities for business leadership.	See the response for control GRM-01.
Governance and Risk Management Policy Enforcement	GRM-07	A formal disciplinary or sanction policy shall be established for employees who have violated security policies and procedures. Employees shall be made aware of what action might be taken in the event of a violation, and disciplinary measures must be stated in the policies and procedures.	The Laserfiche Information Security Policy specifies that disciplinary action may be taken in the event of policy violations and specifies a range of sanctions.
Governance and Risk Management Policy Impact on Risk Assessments	GRM-08	Risk assessment results shall include updates to security policies, procedures, standards, and controls to ensure that they remain relevant and effective.	See the response for control GRM-02.

Copyright 2018 Laserfiche

Control Domain	Control ID	Control Specification	Laserfiche Cloud Response
Governance and Risk Management Policy Reviews	GRM-09	The organization's business leadership (or other accountable business role or function) shall review the information security policy at planned intervals or as a result of changes to the organization to ensure its continuing alignment with the security strategy, effectiveness, accuracy, relevance, and applicability to legal, statutory, or regulatory compliance obligations.	See the response for control GRM-01.
Governance and Risk Management Risk Assessments	GRM-10	Aligned with the enterprise-wide framework, formal risk assessments shall be performed at least annually or at planned intervals, (and in conjunction with any changes to information systems) to determine the likelihood and impact of all identified risks using qualitative and quantitative methods. The likelihood and impact associated with inherent and residual risk shall be determined independently, considering all risk categories (e.g., audit results, threat and vulnerability analysis, and regulatory compliance).	IT Management updates the risk assessment of the Company's IT environment at least annually and considers performing an additional risk assessment when there is significant change to the Laserfiche Cloud service environment.
Governance and Risk Management Risk Management Framework	GRM-11	Risks shall be mitigated to an acceptable level. Acceptance levels based on risk criteria shall be established and documented in accordance with reasonable resolution time frames and stakeholder approval.	Laserfiche's objective in performing risk assessments is effective risk mitigation through control implementation to reduce the likelihood of system compromise via the identified threats to an acceptable level.

Copyright 2018 Laserfiche

Human Resources

Control Domain	Control ID	Control Specification	Laserfiche Cloud Response
Human Resources Asset Returns	HRS-01	Upon termination of workforce personnel and/or expiration of external business relationships, all organizationally-owned assets shall be returned within an established period.	Upon being notified of an employee termination, the Human Resources Department will immediately notify Laserfiche IT to disable the unique user identifier used to assign logical data access and badge physical access. The Human Resources Department is responsible for collecting the badge from the terminated user.
Human Resources Background Screening	HRS-02	Pursuant to local laws, regulations, ethics, and contractual constraints, all employment candidates, contractors, and third parties shall be subject to background verification proportional to the data classification to be accessed, the business requirements, and acceptable risk.	The Company conducts background checks on all prospective employees as part of the recruiting and selection process.
Human Resources Employment Agreements	HRS-03	Employment agreements shall incorporate provisions and/or terms for adherence to established information governance and security policies and must be signed by newly hired or on-boarded workforce personnel (e.g., full or part-time employee or contingent staff) prior to granting workforce personnel user access to corporate facilities, resources, and assets.	New employees are required to read and sign statements agreeing to abide by company policies, confidentiality agreements, and a code of conduct, which is included in the Employee Handbook.
Human Resources Employment Termination	HRS-04	Roles and responsibilities for performing employment termination or change in employment procedures shall be assigned, documented, and communicated.	A process is started that deactivates user accounts upon receiving a notification from HR of a termination of employment event.
Human Resources Mobile Device Management	HRS-05	Policies and procedures shall be established, and supporting business processes and technical	Mobile devices including laptops, smartphones, and tablet computers connecting to the Laserfiche network must be approved devices that support

Copyright 2018 Laserfiche

Control Domain	Control ID	Control Specification	Laserfiche Cloud Response
		measures implemented, to manage business risks associated with permitting mobile device access to corporate resources and may require the implementation of higher assurance compensating controls and acceptable-use policies and procedures (e.g., mandated security training, stronger identity, entitlement and access controls, and device monitoring).	information security standards. Laserfiche IT maintains a list of approved devices and security standards.
Human Resources Non-Disclosure Agreements	HRS-06	Requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details shall be identified, documented, and reviewed at planned intervals.	See the response for control HRS-03.
Human Resources Roles / Responsibilities	HRS-07	Roles and responsibilities of contractors, employees, and third-party users shall be documented as they relate to information assets and security.	The Laserfiche Information Security policy describes the roles and responsibilities of Laserfiche employees as they relate to information assets and security.
Human Resources Technology Acceptable Use	HRS-08	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for defining allowances and conditions for permitting usage of organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.	The Laserfiche Information Security Policy defines an acceptable use policy.

Copyright 2018 Laserfiche

Control Domain	Control ID	Control Specification	Laserfiche Cloud Response
		Additionally, defining allowances and conditions to permit usage of personal mobile devices and associated applications with access to corporate resources (i.e., BYOD) shall be considered and incorporated as appropriate.	
Human Resources Training / Awareness	HRS-09	A security awareness training program shall be established for all contractors, third-party users, and employees of the organization and mandated when appropriate. All individuals with access to organizational data shall receive appropriate awareness training and regular updates in organizational procedures, processes, and policies relating to their professional function relative to the organization.	A formal security awareness program is in place to make all employees aware of the company's security policy, standards, and obligations of users.
Human Resources User Responsibility	HRS-10	All personnel shall be made aware of their roles and responsibilities for: • Maintaining awareness and compliance with established policies and procedures and applicable legal, statutory, or regulatory compliance obligations. • Maintaining a safe and secure working environment	The Employee Handbook, code of conduct, information system and equipment acceptable use policy, and Information Security Policy are published on the Company intranet and is accessible to all employees.
Human Resources Workspace	HRS-11	Policies and procedures shall be established to require that unattended workspaces do not have	The Laserfiche Information Security Policy defines end-user controls for protecting active computer sessions after a specified period of inactivity.

Copyright 2018 Laserfiche

Control Domain	Control ID	Control Specification	Laserfiche Cloud Response
		openly visible (e.g., on a desktop) sensitive documents and user computing sessions are disabled after an established period of inactivity.	

Identity & Access Management

Control Domain	Control ID	Control Specification	Laserfiche Cloud Response
Identity & Access Management Audit Tools Access	IAM-01	Access to, and use of, audit tools that interact with the organization's information systems shall be appropriately segregated and access restricted to prevent inappropriate disclosure and tampering of log data.	Laserfiche uses role-based access control methods whenever feasible to assign authorization levels according to business functions. This method supports the principle of least privilege approach by standardizing access. Access to modify monitoring tools and related configuration are restricted to employees with a business need for privileged access.
Identity & Access Management Credential Lifecycle / Provision Management	IAM-02	User access policies and procedures shall be established, and supporting business processes and technical measures implemented, for ensuring appropriate identity, entitlement, and access management for all internal corporate and customer (tenant) users with access to data and organizationally-owned or managed (physical and virtual) application interfaces and infrastructure network and systems components. These policies, procedures, processes, and measures must incorporate the following: • Procedures, supporting roles, and responsibilities for provisioning and de-provisioning user account entitlements following the rule of least privilege based on job function (e.g., internal employee and contingent staff personnel changes, customer-controlled access, suppliers' business relationships, or other third-party	The Laserfiche Information Security Policy defines policies and processes for identity management, including granting, changing, and revoking physical access and identity access. Laserfiche employees must use an internal ticketing system to request access rights to any applications or systems that are connected to the Laserfiche network. Application access requests must state the roles or privileges requested, and the business need if the requested roles or privileges exceed the pre-authorized set assigned to the job role or position of the requester. Changes to access levels for existing user accounts must also requested and authorized. Laserfiche employees with privileged access to the Laserfiche Cloud hosting environment and computing resources, use one of several connection and authentication paths, depending on the type of resource being accessed. Passwords must conform to password standards that meet the requirements stated in the Information Security Policy. Employees accessing the Laserfiche Cloud production environment use multi-factor authentication to provide an additional layer of security beyond username and password authentication. Security tokens issued to employees are tracked and recovered from employees upon termination of employment. Review of privileged access to in-scope Laserfiche Cloud computing resources is conducted on a periodic basis.

Control Domain	Control ID	Control Specification	Laserfiche Cloud Response
		business relationships) • Business case considerations for higher levels of assurance and multi-factor authentication secrets (e.g., management interfaces, key generation, remote access, segregation of duties, emergency access, large-scale provisioning or geographically-distributed deployments, and personnel redundancy for critical systems) • Access segmentation to sessions and data in multi-tenant architectures by any third party (e.g., provider and/or other customer (tenant)) • Identity trust verification and service-to-service application (API) and information processing interoperability (e.g., SSO and federation) • Account credential lifecycle management from instantiation through revocation • Account credential and/or identity store minimization or re-use when feasible • Authentication, authorization, and accounting (AAA) rules for access to data and sessions	

Control Domain	Control ID	Control Specification	Laserfiche Cloud Response
		(e.g., encryption and strong/multi-factor, expireable, non-shared authentication secrets) • Permissions and supporting capabilities for customer (tenant) controls over authentication, authorization, and accounting (AAA) rules for access to data and sessions • Adherence to applicable legal, statutory, or regulatory compliance requirements	
Identity & Access Management Diagnostic / Configuration Ports Access	IAM-03	User access to diagnostic and configuration ports shall be restricted to authorized individuals and applications.	Access to modify monitoring tools and related configuration are restricted to employees with a business need for privileged access.
Identity & Access Management Policies and Procedures	IAM-04	Policies and procedures shall be established to store and manage identity information about every person who accesses IT infrastructure and to determine their level of access. Policies shall also be developed to control access to network resources based on user identity.	Laserfiche uses role-based access control methods whenever feasible to assign authorization levels according to business functions. This method supports the principle of least privilege approach by standardizing access.
Identity & Access Management Segregation of Duties	IAM-05	User access policies and procedures shall be established, and supporting business processes and technical measures implemented, for restricting user access as per defined segregation of duties to address business risks associated with a user-	The Laserfiche Information Security Policy maintains segregation of duties between development and operations. Developers may be granted limited access to production environments where personnel and expertise availability is limited and only for specific troubleshooting or support purposes. Software development must take place in authorized environments.

Copyright 2018 Laserfiche

Control Domain	Control ID	Control Specification	Laserfiche Cloud Response
		role conflict of interest.	
Identity & Access Management Source Code Access Restriction	IAM-06	Access to the organization's own developed applications, program, or object source code, or any other form of intellectual property (IP), and use of proprietary software shall be appropriately restricted following the rule of least privilege based on job function as per established user access policies and procedures.	The Laserfiche Information Security Policy includes a data sensitivity classification scheme for data stored on Laserfiche systems. Laserfiche uses role-based access control methods whenever feasible to assign authorization levels according to business functions, rather than uniquely for each individual. This method supports the principle of least privilege approach by standardizing access. Access to internal Laserfiche source code management (SCM) systems and build servers related to software development and incident management systems are restricted to Laserfiche employees with a business need to use the functions of these systems.
Identity & Access Management Third Party Access	IAM-07	The identification, assessment, and prioritization of risks posed by business processes requiring third-party access to the organization's information systems and data shall be followed by coordinated application of resources to minimize, monitor, and measure likelihood and impact of unauthorized or inappropriate access. Compensating controls derived from the risk analysis shall be implemented prior to provisioning access.	Laserfiche maintains a risk assessment program to identify information security risks across its IT environment. 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.
Identity & Access Management Trusted Sources	IAM-08	Policies and procedures are established for permissible storage and access of identities used for authentication to ensure identities are only accessible based on rules of least privilege and replication limitation only to users explicitly defined as business necessary.	Laserfiche uses role-based access control methods whenever feasible to assign authorization levels according to business functions. This method supports the principle of least privilege approach by standardizing access.

Control Domain	Control ID	Control Specification	Laserfiche Cloud Response
Identity & Access Management User Access Authorization	IAM-09	Provisioning user access (e.g., employees, contractors, customers (tenants), business partners, and/or supplier relationships) to data and organizationally-owned or managed (physical and virtual) applications, infrastructure systems, and network components shall be authorized by the organization's management prior to access being granted and appropriately restricted as per established policies and procedures. Upon request, provider shall inform customer (tenant) of this user access, especially if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control.	Laserfiche employees must use an internal ticketing system to request access rights to any applications or systems that are connected to the Laserfiche network. Application access requests must state the roles or privileges requested, and the business need if the requested roles or privileges exceed the pre-authorized set assigned to the job role or position of the requester. Changes to access levels for existing user accounts must also be made via the ticketing system, and access level changes must be authorized by management and the application administrator before being applied.
Identity & Access Management User Access Reviews	IAM-10	User access shall be authorized and revalidated for entitlement appropriateness, at planned intervals, by the organization's business leadership or other accountable business role or function supported by evidence to demonstrate the organization is adhering to the rule of least privilege based on job function. For identified access violations, remediation must follow established user access policies and procedures.	Laserfiche uses role-based access control methods whenever feasible to assign authorization levels according to business functions. This method supports the principle of least privilege approach by standardizing access. Review of privileged access to in-scope Laserfiche Cloud computing resources is conducted on a periodic basis. The review is documented and includes a system-generated list of accounts, review of the accounts for appropriateness, and any changes required to the accounts. Once the review is completed, actions are taken to enact any changes required to the accounts. Confirmation of changes is documented as evidence of review.
Identity & Access Management User Access	IAM-11	Timely de-provisioning (revocation or modification) of user	When employees terminate employment, the IT organization and application owners de-provision network and

Control Domain	Control ID	Control Specification	Laserfiche Cloud Response
Revocation		access to data and organizationally-owned or managed (physical and virtual) applications, infrastructure systems, and network components, shall be implemented as per established policies and procedures and based on user's change in status (e.g., termination of employment or other business relationship, job change, or transfer). Upon request, provider shall inform customer (tenant) of these changes, especially if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control.	application access rights granted to the employee. Direction regarding removal of an employee's access follows the same workflow as requesting access, except the request for removal can originate from either Human Resources or the employee's manager. Evidence of timely access removal in case of termination is retained.
Identity & Access Management User ID Credentials	IAM-12	Internal corporate or customer (tenant) user account credentials shall be restricted as per the following, ensuring appropriate identity, entitlement, and access management and in accordance with established policies and procedures: • Identity trust verification and service-to-service application (API) and information processing interoperability (e.g., SSO and Federation) • Account credential lifecycle management from instantiation through revocation • Account credential and/or identity store	Laserfiche uses identity and access management systems to provide user accounts and physical access with appropriate privileges to employees and other system users. The Company assigns each individual a unique user identifier (UID). Customers administer access to their instance of Laserfiche Cloud.

Control Domain	Control ID	Control Specification	Laserfiche Cloud Response
		minimization or re-use when feasible • Adherence to industry acceptable and/or regulatory compliant authentication, authorization, and accounting (AAA) rules (e.g., strong/multi-factor, expireable, non-shared authentication secrets)	
Identity & Access Management Utility Programs Access	IAM-13	Utility programs capable of potentially overriding system, object, network, virtual machine, and application controls shall be restricted.	Access to modify monitoring tools and related configuration are restricted to employees with a business need for privileged access. Security-related event logs are monitored for unauthorized access attempts and privileged access changes.

Infrastructure & Virtualization Security

Control Domain	Control ID	Control Specification	Laserfiche Cloud Response
Infrastructure & Virtualization Security Audit Logging / Intrusion Detection	IVS-01	Higher levels of assurance are required for protection, retention, and lifecycle management of audit logs, adhering to applicable legal, statutory or regulatory compliance obligations and providing unique user access accountability to detect potentially suspicious network behaviors and/or file integrity anomalies, and to support forensic investigative capabilities in the event of a security breach.	An intrusion detection system (IDS) is employed to monitor system events for evidence of potential security incidents that are reviewed, escalated, and tracked. Laserfiche uses role-based access control methods whenever feasible to assign authorization levels according to business functions. This method supports the principle of least privilege approach by standardizing access. Access to modify monitoring tools and related configuration are restricted to employees with a business need for privileged access.
Infrastructure & Virtualization Security Change Detection	IVS-02	The provider shall ensure the integrity of all virtual machine images at all times. Any changes made to virtual machine images must be logged and an alert raised regardless of their running state (e.g., dormant, off, or running). The results of a change or move of an image and the subsequent validation of the image's integrity must be immediately available to customers through electronic methods (e.g., portals or alerts).	A change management process provides a formalized approach to maintaining system stability when deploying software and updating software and system configurations. Changes to system configuration are documented, tracked, tested and approved using Laserfiche's change control process. Laserfiche maintains a central logging server for production systems to capture log information about system and service accesses, and privileged command execution. High-priority security events generate real-time alerts that reviewed and investigated.
Infrastructure & Virtualization Security Clock Synchronization	IVS-03	A reliable and mutually agreed upon external time source shall be used to synchronize the system clocks of all relevant information processing systems to facilitate tracing and reconstitution of activity timelines.	Laserfiche Cloud utilizes AWS Network Time Protocol (NTP) on all hosts to synchronize clocks.
Infrastructure & Virtualization Security Information System Documentation	IVS-04	The availability, quality, and adequate capacity and resources shall be planned, prepared, and measured to deliver the required system	A service health monitoring system continuously monitors system capacity utilization and event logs for overcapacity and service failure conditions, and sends alerts to operations staff when conditions deviate

Copyright 2018 Laserfiche

Control Domain	Control ID	Control Specification	Laserfiche Cloud Response
		performance in accordance with legal, statutory, and regulatory compliance obligations. Projections of future capacity requirements shall be made to mitigate the risk of system overload.	from expected normal operating boundaries. Laserfiche Cloud engineers perform monthly capacity reviews to support appropriate planning for CPU, disk space, and other key areas.
Infrastructure & Virtualization Security Vulnerability Management	IVS-05	Implementers shall ensure that the security vulnerability assessment tools or services accommodate the virtualization technologies used (e.g., virtualization aware).	Laserfiche performs periodic vulnerability assessments of hosts that run in the Laserfiche Cloud hosting environment. Risks are assessment with any identified vulnerabilities and remediated in accordance with Laserfiche security policies. Laserfiche uses a third-party vendor to continually run dynamic vulnerability scans of Laserfiche Cloud web applications in both production and test environments with a proprietary tool.
Infrastructure & Virtualization Security Network Security	IVS-06	Network environments and virtual instances shall be designed and configured to restrict and monitor traffic between trusted and untrusted connections. These configurations shall be reviewed at least annually, and supported by a documented justification for use for all allowed services, protocols, ports, and by compensating controls.	Layered network defenses are deployed in the Laserfiche Cloud network environment to defend against both external and internal threats that use the Internet or AWS networks as an attack vector. Laserfiche Cloud employs a combination of network firewalls, host-based firewalls, application proxies, and intrusion detection systems to protect the production network. The firewalls that are managed by AWS analyze the data and packets routed through the network to Laserfiche Cloud applications. On a quarterly basis, Laserfiche performs an external vulnerability scan and configuration assessment of the firewalls managed by AWS. Laserfiche utilizes various host-based intrusion detection systems (HIDS) to monitor for any potential intrusions. Incidents are documented and tracked with corrective actions and resolutions. Incidents are escalated as necessary to support timely resolution.
Infrastructure & Virtualization Security	IVS-07	Each operating system shall be hardened to provide only necessary ports, protocols, and	Standards for end-user devices include protective controls and specific configurations, such as anti-virus software, patching levels, and required

Copyright 2018 Laserfiche

Control Domain	Control ID	Control Specification	Laserfiche Cloud Response
OS Hardening and Base Controls		services to meet business needs and have in place supporting technical controls such as: antivirus, file integrity monitoring, and logging as part of their baseline operating build standard or template.	operating system or software versions. Company-owned machines may be configured to automatically receive upgrades.
Infrastructure & Virtualization Security Production / Non-Production Environments	IVS-08	Production and non-production environments shall be separated to prevent unauthorized access or changes to information assets. Separation of the environments may include: stateful inspection firewalls, domain/realm authentication sources, and clear segregation of duties for personnel accessing these environments as part of their job duties.	Laserfiche maintains separate AWS accounts that host the development, test, and production environments. Changes to Laserfiche Cloud are tested in an isolated test environment before being deployed to live production systems. The security, compatibility, user-interface, and operational impacts of each change are assessed and documented before each deployment.
Infrastructure & Virtualization Security Segmentation	IVS-09	Multi-tenant organizationally-owned or managed (physical and virtual) applications, and infrastructure system and network components, shall be designed, developed, deployed, and configured such that provider and customer (tenant) user access is appropriately segmented from other tenant users, based on the following considerations: • Established policies and procedures • Isolation of business critical assets and/or sensitive user data, and sessions that mandate stronger internal controls and high levels of assurance	Customer data is logically segregated between accounts by using separately allocated databases and virtual disk volumes.

Copyright 2018 Laserfiche

Control Domain	Control ID	Control Specification	Laserfiche Cloud Response
		• Compliance with legal, statutory, and regulatory compliance obligations	
Infrastructure & Virtualization Security VM Security - Data Protection	IVS-10	Secured and encrypted communication channels shall be used when migrating physical servers, applications, or data to virtualized servers and, where possible, shall use a network segregated from production-level networks for such migrations.	All connections to transfer data over computer networks are encrypted. All administrative-level operating system remote access to the Laserfiche Cloud service environment is protected by firewalls that block connections originating from outside the Laserfiche corporate network. Privileged remote access connections are protected by strong encryption to prevent eavesdropping, tampering, or spoofing of sessions. All requests from client applications over the Internet to Laserfiche Cloud use HTTP or HTTP over TLS (HTTPS).
Infrastructure & Virtualization Security Hypervisor Hardening	IVS-11	Access to all hypervisor management functions or administrative consoles for systems hosting virtualized systems shall be restricted to personnel based upon the principle of least privilege and supported through technical controls (e.g., two-factor authentication, audit trails, IP address filtering, firewalls, and TLS encapsulated communications to the administrative consoles).	Only employees with a business need are granted AWS permissions to access AWS management tools for the production environment.
Infrastructure & Virtualization Security Wireless Security	IVS-12	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to protect wireless network environments, including the following: • Perimeter firewalls implemented and configured to restrict unauthorized traffic • Security settings	Laserfiche has implemented network security controls to secure wireless networks. Wireless networks at Company facilities for non-public use are protected through secure data encryption.

Copyright 2018 Laserfiche

Control Domain	Control ID	Control Specification	Laserfiche Cloud Response
		enabled with strong encryption for authentication and transmission, replacing vendor default settings (e.g., encryption keys, passwords, and SNMP community strings) • User access to wireless network devices restricted to authorized personnel • The capability to detect the presence of unauthorized (rogue) wireless network devices for a timely disconnect from the network	
Infrastructure & Virtualization Security Network Architecture	IVS-13	Network architecture diagrams shall clearly identify high-risk environments and data flows that may have legal compliance impacts. Technical measures shall be implemented and shall apply defense-in-depth techniques (e.g., deep packet analysis, traffic throttling, and black-holing) for detection and timely response to network-based attacks associated with anomalous ingress or egress traffic patterns (e.g., MAC spoofing and ARP poisoning attacks) and/or distributed denial-of-service (DDoS) attacks.	Layered network defenses are deployed in the Laserfiche Cloud network environment to defend against both external and internal threats that use the Internet or AWS networks as an attack vector. Laserfiche Cloud employs a combination of network firewalls, host-based firewalls, application proxies, and intrusion detection systems to protect the production network. All administrative-level operating system remote access to the Laserfiche Cloud service environment is protected by firewalls that block connections originating from outside the Laserfiche corporate network. Privileged remote access connections are protected by strong encryption to prevent eavesdropping, tampering, or spoofing of sessions.

Copyright 2018 Laserfiche

Interoperability & Portability

Control Domain	Control ID	Control Specification	Laserfiche Cloud Response
Interoperability & Portability APIs	IPY-01	The provider shall use open and published APIs to ensure support for interoperability between components and to facilitate migrating applications.	Laserfiche supports a set of APIs that allow customers to access their Laserfiche repository content data. API documentation is published and made available to customers.
Interoperability & Portability Data Request	IPY-02	All structured and unstructured data shall be available to the customer and provided to them upon request in an industry-standard format (e.g., .doc, .xls, .pdf, logs, and flat files).	Customers can choose to export their data at any time. Export instructions are available in the product documentation.
Interoperability & Portability Policy & Legal	IPY-03	Policies, procedures, and mutually-agreed upon provisions and/or terms shall be established to satisfy customer (tenant) requirements for service-to-service application (API) and information processing interoperability, and portability for application development and information exchange, usage, and integrity persistence.	See the response for control IPY-01.
Interoperability & Portability Standardized Network Protocols	IPY-04	The provider shall use secure (e.g., non-clear text and authenticated) standardized network protocols for the import and export of data and to manage the service, and shall make available a document to consumers (tenants) detailing the relevant interoperability and portability standards that are involved.	All requests from client applications over the Internet to Laserfiche Cloud use HTTP or HTTP over TLS (HTTPS).
Interoperability & Portability Virtualization	IPY-05	The provider shall use an industry-recognized virtualization platform and standard virtualization formats	Laserfiche uses Amazon Web Services (AWS), a subservice organization, to provide cloud Infrastructure-as-as-Service (IaaS), including virtual machines.

Copyright 2018 Laserfiche

Control Domain	Control ID	Control Specification	Laserfiche Cloud Response
		(e.g., OVF) to help ensure interoperability, and shall have documented custom changes made to any hypervisor in use and all solution-specific virtualization hooks available for customer review.	

Copyright 2018 Laserfiche

Mobile Security

Control Domain	Control ID	Control Specification	Laserfiche Cloud Response
Mobile Security Anti-Malware	MOS-01	Anti-malware awareness training, specific to mobile devices, shall be included in the provider's information security awareness training.	
Mobile Security Application Stores	MOS-02	A documented list of approved application stores has been defined as acceptable for mobile devices accessing or storing provider managed data.	Mobile devices including laptops, smartphones, and tablet computers connecting to the Laserfiche network must be approved devices that support Laserfiche information security standards. Laserfiche IT maintains a list of approved devices and required security standards.
Mobile Security Approved Applications	MOS-03	The company shall have a documented policy prohibiting the installation of non-approved applications or approved applications not obtained through a pre-identified application store.	
Mobile Security Approved Software for BYOD	MOS-04	The BYOD policy and supporting awareness training clearly states the approved applications, application stores, and application extensions and plugins that may be used for BYOD usage.	
Mobile Security Awareness and Training	MOS-05	The provider shall have a documented mobile device policy that includes a documented definition for mobile devices and the acceptable usage and requirements for all mobile devices. The provider shall post and communicate the policy and requirements through the company's security awareness and training program.	Laserfiche's Information Security Policy defines acceptable usage requirements and limits for mobile devices that connect to or access Company information assets and systems.
Mobile Security	MOS-06	All cloud-based services	

Copyright 2018 Laserfiche

Control Domain	Control ID	Control Specification	Laserfiche Cloud Response
Cloud Based Services		used by the company's mobile devices or BYOD shall be pre-approved for usage and the storage of company business data.	
Mobile Security Compatibility	MOS-07	The company shall have a documented application validation process to test for mobile device, operating system, and application compatibility issues.	
Mobile Security Device Eligibility	MOS-08	The BYOD policy shall define the device and eligibility requirements to allow for BYOD usage.	See the response for control MOS-05.
Mobile Security Device Inventory	MOS-09	An inventory of all mobile devices used to store and access company data shall be kept and maintained. All changes to the status of these devices (i.e., operating system and patch levels, lost or decommissioned status, and to whom the device is assigned or approved for usage (BYOD)) will be included for each device in the inventory.	Laserfiche may permit employees and others to use their own equipment to connect to its network and systems. Use of mobile devices must be based on job function and authorization from business unit managers is required for BYOD network access. Manager authorization must be documented on the BYOD request. For approved BYOD devices, Laserfiche IT may install specific security controls on the device; such as mobile device management software, access controls, encryption, remote wiping software, or other security controls.
Mobile Security Device Management	MOS-10	A centralized, mobile device management solution shall be deployed to all mobile devices permitted to store, transmit, or process customer data.	Laserfiche does not permit the storage, transmission, or processing of customer data on mobile devices.
Mobile Security Encryption	MOS-11	The mobile device policy shall require the use of encryption either for the entire device or for data identified as sensitive on all mobile devices, and shall be enforced through technology controls.	Encryption at rest is required for any mobile device storing Company data. Encryption in transit is also required for any mobile device transmitting Company data.
Mobile Security Jailbreaking and	MOS-12	The mobile device policy shall prohibit the circumvention of built-in	

Control Domain	Control ID	Control Specification	Laserfiche Cloud Response
Rooting		security controls on mobile devices (e.g., jailbreaking or rooting) and shall enforce the prohibition through detective and preventative controls on the device or through a centralized device management system (e.g., mobile device management).	
Mobile Security Legal	MOS-13	The BYOD policy includes clarifying language for the expectation of privacy, requirements for litigation, e-discovery, and legal holds. The BYOD policy shall clearly state the expectations regarding the loss of non-company data in the case that a wipe of the device is required.	
Mobile Security Lockout Screen	MOS-14	BYOD and/or company-owned devices are configured to require an automatic lockout screen, and the requirement shall be enforced through technical controls.	
Mobile Security Operating Systems	MOS-15	Changes to mobile device operating systems, patch levels, and/or applications shall be managed through the company's change management processes.	
Mobile Security Passwords	MOS-16	Password policies, applicable to mobile devices, shall be documented and enforced through technical controls on all company devices or devices approved for BYOD usage, and shall prohibit the changing of password/PIN lengths and authentication requirements.	

Copyright 2018 Laserfiche

Control Domain	Control ID	Control Specification	Laserfiche Cloud Response
Mobile Security Policy	MOS-17	The mobile device policy shall require the BYOD user to perform backups of data, prohibit the usage of unapproved application stores, and require the use of anti-malware software (where supported).	
Mobile Security Remote Wipe	MOS-18	All mobile devices permitted for use through the company BYOD program or a company-assigned mobile device shall allow for remote wipe by the company's corporate IT or shall have all company-provided data wiped by the company's corporate IT.	For approved BYOD devices, Laserfiche IT may install specific security controls on the device; such as mobile device management software, access controls, encryption, remote wiping software, or other security controls.
Mobile Security Security Patches	MOS-19	Mobile devices connecting to corporate networks, or storing and accessing company information, shall allow for remote software version/patch validation. All mobile devices shall have the latest available security-related patches installed upon general release by the device manufacturer or carrier and authorized IT personnel shall be able to perform these updates remotely.	
Mobile Security Users	MOS-20	The BYOD policy shall clarify the systems and servers allowed for use or access on a BYOD-enabled device.	

Copyright 2018 Laserfiche

Security Incident Management, E-Discovery, & Cloud Forensics

Control Domain	Control ID	Control Specification	Laserfiche Cloud Response
Security Incident Management, E-Discovery, & Cloud Forensics Contact / Authority Maintenance	SEF-01	Points of contact for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities shall be maintained and regularly updated (e.g., change in impacted-scope and/or a change in any compliance obligation) to ensure direct compliance liaisons have been established and to be prepared for a forensic investigation requiring rapid engagement with law enforcement.	The Information Security Officer's Incident Response Plan includes contact information for external notifications.
Security Incident Management, E-Discovery, & Cloud Forensics Incident Management	SEF-02	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to triage security-related events and ensure timely and thorough incident management, as per established IT service management policies and procedures.	Laserfiche has developed a security 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 at least annually and updated as needed.
Security Incident Management, E-Discovery, & Cloud Forensics Incident Reporting	SEF-03	Workforce personnel and external business relationships shall be informed of their responsibilities and, if required, shall consent and/or contractually agree to report all information security events in a timely manner. Information security events shall be reported through predefined communications channels in a timely manner adhering to applicable legal, statutory, or regulatory compliance	Laserfiche has developed a security 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. Laserfiche utilizes various host-based intrusion detection systems to monitor for any potential intrusions. Incidents are documented and tracked with corrective actions and resolutions. Incidents are escalated as necessary to support timely resolution. The Laserfiche Information Security Policy defines an incident reporting responsibility for employees. The process for customers and external

Copyright 2018 Laserfiche

Control Domain	Control ID	Control Specification	Laserfiche Cloud Response
		obligations.	users to inform the Company of possible vulnerabilities is posted on the Company's website.
Security Incident Management, E-Discovery, & Cloud Forensics Incident Response Legal Preparation	SEF-04	Proper forensic procedures, including chain of custody, are required for the presentation of evidence to support potential legal action subject to the relevant jurisdiction after an information security incident. Upon notification, customers and/or other external business partners impacted by a security breach shall be given the opportunity to participate as is legally permissible in the forensic investigation.	The Information Security Officer maintains a security incident reporting and response process to ensure that proper actions and notifications are made based on the severity of the incident. Laserfiche Legal participates in security incident response so that all phases of incident response, including incident notification, comply with applicable laws and regulations.
Security Incident Management, E-Discovery, & Cloud Forensics Incident Response Metrics	SEF-05	Mechanisms shall be put in place to monitor and quantify the types, volumes, and costs of information security incidents.	Laserfiche has developed a security 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. A root cause analysis is performed for critical priority incidents.

Copyright 2018 Laserfiche

Supply Chain Management, Transparency, and Accountability

Control Domain	Control ID	Control Specification	Laserfiche Cloud Response
Supply Chain Management, Transparency, and Accountability Data Quality and Integrity	STA-01	Providers shall inspect, account for, and work with their cloud supply-chain partners to correct data quality errors and associated risks. Providers shall design and implement controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least-privilege access for all personnel within their supply chain.	Laserfiche management, through its daily operational activities, monitors the services performed by its subservice organizations to ensure the effectiveness of operations and controls expected to be implemented at the subservice organizations. Management also communicates with the subservice organizations to relay any issues or concerns, if any.
Supply Chain Management, Transparency, and Accountability Incident Reporting	STA-02	The provider shall make security incident information available to all affected customers and providers periodically through electronic methods (e.g., portals).	Information about the current availability of Laserfiche Cloud and the individual applications that compromise the service offering is published to a website. Information about upcoming planned system maintenance operations is also published on this website. Non-sensitive information about service outages, including the extent, root causes, and a timeline of events, including corrective actions, is posted on the status website as part of the service history record.
Supply Chain Management, Transparency, and Accountability Network / Infrastructure Services	STA-03	Business-critical or customer (tenant) impacting (physical and virtual) application and system-system interface (API) designs and configurations, and infrastructure network and systems components, shall be designed, developed, and deployed in accordance with mutually agreed-upon service and capacity-level expectations, as well as IT governance and service management policies and procedures.	A service health monitoring system continuously monitors system capacity utilization and event logs for overcapacity and service failure conditions, and sends alerts to operations staff when conditions deviate from expected normal operating boundaries. A monitoring agent process running on hosts in the Laserfiche Cloud system continuously transmits data about system health metrics to a health monitoring service that collects and analyzes health metric data.
Supply Chain Management, Transparency, and	STA-04	The provider shall perform annual internal assessments of	On an annual basis, a risk assessment is performed, where threats to security, availability, and confidentiality of

Copyright 2018 Laserfiche

Control Domain	Control ID	Control Specification	Laserfiche Cloud Response
Accountability Provider Internal Assessments		conformance to, and effectiveness of, its policies, procedures, and supporting measures and metrics.	critical user entity assets are identified and evaluated. 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.
Supply Chain Management, Transparency, and Accountability Supply Chain Agreements	STA-05	Supply chain agreements (e.g., SLAs) between providers and customers (tenants) shall incorporate at least the following mutually-agreed upon provisions and/or terms: • Scope of business relationship and services offered (e.g., customer (tenant) data acquisition, exchange and usage, feature sets and functionality, personnel and infrastructure network and systems components for service delivery and support, roles and responsibilities of provider and customer (tenant) and any subcontracted or outsourced business relationships, physical geographical location of hosted services, and any known regulatory compliance considerations) • Information security requirements, provider and customer (tenant) primary points of contact for the	The Company's third-party contracts are approved by Legal and include provisions for confidentiality, non-disclosure, and/or acceptable use prior to the start of third-party service(s).

Control Domain	Control ID	Control Specification	Laserfiche Cloud Response
		duration of the business relationship, and references to detailed supporting and relevant business processes and technical measures implemented to enable effectively governance, risk management, assurance and legal, statutory and regulatory compliance obligations by all impacted business relationships • Notification and/or pre-authorization of any changes controlled by the provider with customer (tenant) impacts • Timely notification of a security incident (or confirmed breach) to all customers (tenants) and other business relationships impacted (i.e., up- and down-stream impacted supply chain) • Assessment and independent verification of compliance with agreement provisions and/or terms (e.g., industry-acceptable certification, attestation audit report, or equivalent forms of assurance) without posing an unacceptable business risk of exposure to the organization being	

Control Domain	Control ID	Control Specification	Laserfiche Cloud Response
		assessed • Expiration of the business relationship and treatment of customer (tenant) data impacted • Customer (tenant) service-to-service application (API) and data interoperability and portability requirements for application development and information exchange, usage, and integrity persistence	
Supply Chain Management, Transparency, and Accountability Supply Chain Governance Reviews	STA-06	Providers shall review the risk management and governance processes of their partners so that practices are consistent and aligned to account for risks inherited from other members of that partner's cloud supply chain.	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. The Laserfiche Information Security Officer maintains a risk assessment program to oversee service providers that interact with Laserfiche's systems and information. The risk assessment program includes processes to track vendors and service providers, evaluate their capabilities, periodically assess risks, and compliance with this Policy.
Supply Chain Management, Transparency, and Accountability Supply Chain Metrics	STA-07	Policies and procedures shall be implemented to ensure the consistent review of service agreements (e.g., SLAs) between providers and customers (tenants) across the relevant supply chain (upstream/downstream). Reviews shall be performed at least annually and identify any non-conformance to established agreements. The reviews should result in actions to address service-level conflicts or	The Laserfiche Information Security Officer maintains a risk assessment program to oversee service providers that interact with Laserfiche's systems and information. The risk assessment program includes processes to track vendors and service providers, evaluate their capabilities, periodically assess risks, and compliance with this Policy.

Copyright 2018 Laserfiche

Control Domain	Control ID	Control Specification	Laserfiche Cloud Response
		inconsistencies resulting from disparate supplier relationships.	
Supply Chain Management, Transparency, and Accountability Third Party Assessment	STA-08	Providers shall assure reasonable information security across their information supply chain by performing an annual review. The review shall include all partners/third party-providers upon which their information supply chain depends on.	See the response for control STA-07.
Supply Chain Management, Transparency, and Accountability Third Party Audits	STA-09	Third-party service providers shall demonstrate compliance with information security and confidentiality, access control, service definitions, and delivery level agreements included in third-party contracts. Third-party reports, records, and services shall undergo audit and review at least annually to govern and maintain compliance with the service delivery agreements.	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.

Copyright 2018 Laserfiche

Threat and Vulnerability Management

Control Domain	Control ID	Control Specification	Laserfiche Cloud Response
Threat and Vulnerability Management Anti-Virus / Malicious Software	TVM-01	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of malware on organizationally-owned or managed user end-point devices (i.e., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.	The Laserfiche Information Security Policy defines an anti-virus policy whereby all Microsoft Windows and macOS-based systems, file servers and email servers on Company networks must be configured with Laserfiche IT approved anti-virus or anti-malware software.
Threat and Vulnerability Management Vulnerability / Patch Management	TVM-02	Policies and procedures shall be established, and supporting processes and technical measures implemented, for timely detection of vulnerabilities within organizationally-owned or managed applications, infrastructure network and system components (e.g., network vulnerability assessment, penetration testing) to ensure the efficiency of implemented security controls. A risk-based model for prioritizing remediation of identified vulnerabilities shall be used. Changes shall be managed through a change management process for all vendor-supplied patches, configuration changes, or changes to the organization's internally developed software. Upon request, the provider informs customer (tenant) of policies and procedures and identified weaknesses especially if customer (tenant) data is used as part the service and/or	Laserfiche security policies provide requirements for vulnerability management and annual risk assessments. On a quarterly basis, Laserfiche performs a vulnerability scan of all hosts that run in the Laserfiche Cloud hosting environment. 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. All changes are deployed following the standard change management process and are tested in an isolated test environment before being deployed to the production environment. Changes to address identified vulnerabilities and weaknesses are deployed using the standard change management process for deploying software updates to Laserfiche Cloud.

Copyright 2018 Laserfiche

Control Domain	Control ID	Control Specification	Laserfiche Cloud Response
		customer (tenant) has some shared responsibility over implementation of control.	
Threat and Vulnerability Management Mobile Code	TVM-03	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of unauthorized mobile code, defined as software transferred between systems over a trusted or untrusted network and executed on a local system without explicit installation or execution by the recipient, on organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.	Laserfiche Cloud does not use mobile code, and technical measures, including firewalls, have been implemented to isolate the production environment from external systems to prevent the introduction or execution of mobile code. Detective controls utilizing an IDS are used to detect when untrusted code may have been introduced into the production environment.

Copyright 2018 Laserfiche

Notices

Copyright 2018 Laserfiche. Laserfiche makes every effort to ensure the accuracy of these contents at the time of publication. They are for information purposes only and Laserfiche makes no warranties, express or implied, as to the information herein.