Cloud Security Alliance

Cloud Control Matrix

Version 3.01

Last Updated: March 2016

Introduction:

Salesforce (or the "Company") is a leading provider of enterprise cloud computing technologies and is dedicated to helping customers transform themselves into social enterprises. Through social, mobile, and open technologies, Salesforce enables companies to place customers at the heart of their business and engage them in new and powerful ways.

Salesforce provides applications including customer relationship management ("CRM"), collaboration, and social media monitoring to businesses of all sizes and industries worldwide. Also, the Company provides platforms for customers and developers to build and run business applications.

Based on Salesforce's real-time, multi-tenant architecture, the Company's application and platform services allow customers to:

- Create solutions for better productivity through sales force automation, access to better and more organized data about current customers and prospects and relationship management functionality with Sales Cloud accessible on mobile devices.
- Provide a comprehensive solution for customer service interactions across every service channel – from call centers to social networks with Service Cloud.
- Develop, build and run social, mobile, and real-time business applications from the Force.com or Heroku cloud platforms.
- Create enterprise social networks that allow teams to sync up and take action, and powers Communities to connect like never before with Salesforce Chatter. Connect customers, partners, and employees directly with your business to provide an engaging customer experience, connect partners to sell more effectively, agencies to work more efficiently, and employees to promote engagement with Salesforce Communities.
- Allow marketers to create 1:1 campaigns like never before by combining traditional digital channels like email, mobile, social, and the Web with any conceivable product – from toothbrushes to cars – to turn consumers into customers with the Salesforce Marketing Cloud.
- Know your customers and prospects better and connect with them faster to make better data-driven decisions, with access to the right data at the right moment. Data.com brings B2B contact and account information directly to your team to boost your pipeline and sales productivity.
- Get B2B marketing automation that easily integrates with the Sales Cloud with Pardot. Marketing and sales teams use Pardot to generate and qualify leads, and create, deploy, and manage online campaigns from a central platform.
- Drive team performance to a whole new level with Work.com, built on the Salesforce1 Platform. Set metrics-based goals, give coaching notes, and provide continuous feedback directly within the Sales Cloud. Onboard new reps faster, and amplify winning behaviors with real-time recognition and rewards.
- Empower small businesses to become social enterprises with Desk.com.
- Extend a company's social enterprise with applications from the leading enterprise application marketplace, AppExchange.

The information provided in this document applies to services branded as Force.com, Database.com, Sales Cloud, Service Cloud, Communities, and Chatter (referred to hereafter as the "Salesforce Services").

Please note that this document is for informational purposes only. Salesforce has made every effort to provide responses that are accurate as of the date of publication. Because our procedures and policies change from time to time, we cannot guarantee that responses contained herein will be identical to those in our contracts. If you choose Salesforce as your service provider, we will enter into contracts that cover many of the topics below, and those contracts will be definitive agreements.

The Cloud Security Alliance's Cloud Control Matrix

In this document, Salesforce provides detailed information about how the Company helps fulfill the applicable security, privacy, compliance, and risk management requirements defined by the Cloud Security Alliance's (CSA) Cloud Control Matrix (CCM). The CSA is a not-for-profit, member-driven organization of leading industry practitioners with a mission to promote the use of best practices for providing security assurance within Cloud Computing, and to provide education on the uses of Cloud Computing to help secure all other forms of computing. CSA is led by a broad coalition of industry practitioners, corporations, associations and other key stakeholders.

The CSA CCM is specifically designed to provide fundamental security principles to guide cloud vendors and to assist prospective cloud customers in assessing the overall security risk of a cloud provider. The CSA CCM provides a controls framework that gives detailed understanding of security and privacy concepts and principles that are aligned to the Cloud Security Alliance guidance in 16 domains. It also serves to provide a mapping of Salesforce's controls to industry-accepted security standards, regulations, and controls frameworks that we comply with such as ISO 27001/27002, PCI, and NIST.

Salesforce's Service Delivery

Salesforce delivers the Salesforce Services over the Internet through commercially-available Web connections and browser software. Customers log into the Salesforce Services from the Salesforce Web site using a unique username and password. The Salesforce Services allow for additional authentication methods that may be activated by customers.

Salesforce services its customers using what is known in the industry as "multi-tenant" architecture. Multi-tenant applications and platforms permit many users to simultaneously access and use the same services, with logical separation of data allowing each customer to view only its "instance" of Salesforce's services and associated data. Salesforce's multi-tenant architecture is similar to that used to provide online banking and brokerage services to consumers, which can also be accessed and used by thousands of users simultaneously through the logical – rather than physical – separation of data.

Salesforce's Trust Program

Salesforce has a world-class program referred to as "Trust" that carefully considers security, privacy, compliance, and risk-related matters at every level and in every business function of the organization on an ongoing basis. Salesforce's Information Security Management System is based on the internationally-recognized ISO 27002 framework, and the Company has achieved and continues to maintain ISO 27001 certification.

- **Certifications, Audits and Compliance**: Multiple third parties have certified and audited Salesforce's security and privacy controls. Salesforce's geographical recognition includes: approval from 29 European data protection authorities for the Salesforce Processor Binding Corporate Rules, the TRUSTe Privacy Program seal, privacy mark certification by the Japan Information Processing Development Corporation (also known as "JIPDC") for the Company's Japanese affiliate, and privacy mark certification by TÜV for the Company's German affiliate.

  In addition to its ISO 27001 certification, the Company undergoes the following audit and compliance activities:
  - Periodic SSAE 16 / ISAE 3402 audits and AICPA Trust Principles examinations resulting in Type II Service Organization Control (SOC) reports are performed by Salesforce's independent external auditors.
  - Salesforce is PCI Level 1 compliant and has received a signed Attestation of Compliance (AoC) for the Payment Card Industry Data Security Standard (PCI-DSS). Customer administrators must configure features of the Salesforce Services to support their organization's PCI controls and compliance.
  - Salesforce has received a FedRAMP Agency Authority to Operate (ATO) at the moderate impact level issued by Health and Human Services (HHS) for the Salesforce Government Cloud of the Salesforce Services. The Salesforce Government Cloud is a partitioned instance of Salesforce's multi-tenant public cloud infrastructure, specifically for use by U.S federal, state, and local government customers, U.S. government contractors, and Federally Funded Research and Development Centers (FFRDCs). A security assessment of the information system was conducted by a third party assessment organization (3PAO) in accordance with NIST 800-53A Rev. 1 and FedRAMP requirements. To maintain compliance with FedRAMP, Salesforce conducts continuous monitoring. Continuous monitoring includes ongoing technical vulnerability detection and remediation, remediation of open compliance related findings, and an independent assessment at least annually for a selection of security controls.
  - The Company's internal audit functions regularly assess the Company's security and privacy programs.

- **Policies**: Salesforce implements internal policies based on the ISO 27002 standard that also reflect Salesforce's contractual commitments to safeguard Customer Data and meet regulatory requirements. These policies include Salesforce's Code of Conduct (which includes sections on confidentiality, privacy, and information security), information security and privacy policies regarding handling of Customer Data, and confidentiality agreements with all personnel. Additionally, Salesforce has implemented a business continuity and disaster recovery plan.
- **Practices**: Salesforce has a multi-faceted employee awareness program focused on Salesforce's obligations to safeguard confidential information, including Customer Data. This program includes the following elements:

- Requiring employees to certify compliance with Salesforce's Code of Conduct on an annual basis;
- Requiring all employees to complete an annual information security and privacy awareness program and pass an associated test; and
- Communicating with employees via internal company-wide communications.

Additionally, Salesforce communicates with its customers and end users about privacy and security topics through http://trust.salesforce.com.

- **Professionals**: Salesforce's Trust department, led by the Chief Trust Officer, is responsible for security-related technology, policies, and procedures. Salesforce's Privacy department, led by the Vice President, Global Privacy & Associate General Counsel, is responsible for designing, implementing, and ensuring compliance with Salesforce's privacy program. Salesforce's Compliance Center, led by the Chief Compliance Officer, is responsible for Salesforce's comprehensive audit and compliance program, which includes internal assessments of Salesforce's compliance with its privacy and security program.

Resources

For more information about Salesforce's Trust program, including security and privacy, please visit http://trust.salesforce.com

Control Area	Control ID	Control Specification	Control Notes
Application & Interface Security *Application Security*	AIS-01	Applications and interfaces (APIs) shall be designed, developed, and deployed in accordance with industry acceptable standards (e.g., OWASP for web applications) and adhere to applicable legal, statutory, or regulatory compliance obligations.	Salesforce's Software Development Lifecycle (SDLC) processes are consistent with industry standards and follow internal SDLC requirements, which address applicable guidance (such as OWASP) to prevent vulnerabilities. As such, Salesforce has been evaluated against the following external audit standards: PCI-DSS, FedRAMP, and ISO 27001.
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.	Salesforce uses administrative, technical and physical controls in providing and operating the Salesforce Services. Customer data submitted to the Salesforce Services by Salesforce's customers ("Customer Data") is managed by the customer in their use of the Salesforce Services. Such customers are responsible for complying with applicable laws in using the Salesforce Services. All user and application□level security controls are defined and maintained by the organization administrator, and not by Salesforce. The organization administrator is appointed by the customer. An organization's sharing model sets the default access that users have to Customer Data.
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.	Application logic enforces input by Customer Data type. It is the customer's responsibility for monitoring proper entry of Customer Data. Salesforce offers many features to help ensure the capture of effective and relevant Customer Data. The system offers features such as validation rules with red-highlighted error messages, administrator-defined field picklists, field default values, required fields, and bubble help text on data entry screens. Database changes for the Salesforce Services are committed only under appropriate transaction controls.

Control Area	Control ID	Control Specification	Control Notes
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.	Salesforce is ISO 27001 certified and has documented security policies and procedures, per requirements of this certification. Connections to the environment for the Salesforce Services is only available over a secure channel (HTTPS) and data in transit is TLS encrypted via cryptographic controls using global step-up certificates, ensuring that users have a secure connection from their browsers to the Salesforce Services. Customers who enable integration with systems outside their instance of the Salesforce Services can install their own certificates.
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.	Salesforce's mission is to be a trusted service provider on behalf of our customers. To help accomplish this mission, Salesforce provides robust security and privacy protections for information submitted to the Salesforce Services ("Customer Data") based on internationally-recognized standards, such as the ISO 27001 standard. Salesforce regularly undergoes audits by independent third parties to test the security and privacy control framework for Salesforce Services, including: ISO 27001, SOC 1 (SSAE 16/ISAE 3402), SOC 2, SOC 3 (formerly SysTrust), PCI-DSS, and FedRAMP. Additional information about Salesforce's independent reviews and assessments is available at: http://trust.salesforce.com.
Audit Assurance & Compliance *Independent Audits*	AAC-02	Independent reviews and assessments shall be performed at least annually, or at planned intervals, to ensure that the organization addresses any nonconformities of established policies, procedures, and known contractual, statutory, or regulatory compliance obligations.	Please also refer to the response provided to AAC-01 above. Customers with a signed NDA can review Salesforce's SOC 2 report upon request.

Control Area	Control ID	Control Specification	Control Notes
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.	Salesforce has a certified set of control frameworks capturing a broad range of regulatory requirements applicable to the provision of the Salesforce Services. This framework is reviewed on a regular basis, once a year or more. Salesforce has comprehensive privacy and security assessments and certifications performed by multiple third parties.

Control Area	Control ID	Control Specification	Control Notes
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	Salesforce has developed a Business Continuity program applicable to the Salesforce Services, which is managed by the Business Continuity team. Individual teams are responsible for the development and maintenance of their respective plans. This program is overseen by senior management for each of the key functional areas within Salesforce, and is supported by executive leadership at the highest level.

Control Area	Control ID	Control Specification	Control Notes
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 other business relationships that represent critical intra-supply chain business process dependencies.	Business continuity plans applicable to the Salesforce Services are tested annually at a minimum. Salesforce has a security incident response process. During a security incident, the process guides Salesforce personnel in management, communication, and resolution activities. Regular updates are provided to engaged parties (including customers where appropriate) until issue resolution.
Business Continuity Management & Operational Resilience *Datacenter Utilities / Environmental Conditions*	BCR-03	Datacenter 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.	The Salesforce Services are configured to be N+1 redundant at a minimum, where N is the number of components of a given type needed for the service to operate, and +1 is the redundancy. In many cases, the Salesforce Services have more than one piece of redundant equipment for a given function. The data center engineering staff provides 24-hour monitoring in the operations center for all critical components Audits of security controls at the data centers used for the Salesforce Services are performed multiple times throughout the year for SOC 1 (SSAE 16), SOC 2, ISO 27001 and PCI-DSS.

Control Area	Control ID	Control Specification	Control Notes
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	Detailed process narratives and standard operating procedures are documented and available for information systems supporting the Salesforce Services system documentation. Documentation is accessible on internal Company sites and restricted to personnel responsible for managing the system. Salesforce provides a help and training portal that brings together resources to help solve problems quickly and easily. Salesforce also provides context-sensitive help icons throughout application screens to make it easier for users to obtain unique help without searching.
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 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.	When picking a data center location, physical protection against damage from natural causes and disasters, as well as deliberate attacks, are considered in the evaluation criteria. Salesforce's data centers used for the Salesforce Services are located above sea level with no basement, dedicated pump rooms, drainage/evacuation systems and moisture detectors. Buildings are engineered for local seismic, storm, and flood risks. Data centers are in geographically disparate locations, so that a disaster at one data center would mean that the service fails over to a backup data center remote from the disaster area.
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.	Some data centers for the Salesforce Services may be located in locales with environmental risks, such as earthquakes, however additional precautions have been implemented to minimize the impact of such events. Please refer to the response provided to BCR-05 above for additional details.

Control Area	Control ID	Control Specification	Control Notes
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.	Maintenance of physical and environmental systems for the Salesforce Services is performed in accordance to manufacturer specifications. These controls are tested for operating effectiveness during Salesforce's periodic third party compliance and audit activities.
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.	Please refer to the response provided to BCR-03 and BCR-05 above for additional details.

Control Area	Control ID	Control Specification	Control Notes
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 that must incorporate the following: • Identify critical 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	Salesforce performs a Business Impact Assessment for the Salesforce Services that identifies critical processes and services, dependencies, threats, and impacts resulting from disruption of the Salesforce Services, and establishes maximum tolerable period, priorities for recovery, and resources required. In addition to the global BIA, Salesforce's Business Continuity plans and Disaster Recovery processes are updated and tested on an annual basis and include, but are not limited to, review of critical processes, recovery time objectives, and key resources.

Control Area	Control ID	Control Specification	Control Notes
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 responsibilities supported by regular workforce training.	Procedures are maintained by the Operations teams to ensure that consistent processes are followed in the management and support of the Salesforce Services. These documents are available to all appropriate personnel required to perform Operations functions.
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.	Retention: Salesforce's customers determine how long their respective Customer Data is retained in the Salesforce Services. Customers may utilize the Salesforce Services' "Weekly Export" feature to export Customer Data and retain such information in separate systems. Backup: Customer Data is replicated to disk in near-real time at the designated secondary data center, and backed up at the primary and secondary data centers. Backups are performed daily at each data center facility without stopping access to the application. Replication is transmitted over an encrypted network. Disaster Recovery: The disaster recovery facilities for the Salesforce Services are geographically remote from primary data center facilities, with production-level hardware, software, and Internet connectivity. Salesforce has managed disaster recovery plans in place and tests them regularly.

Control Area	Control ID	Control Specification	Control Notes
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 datacenter facilities have been pre-authorized by the organization's business leadership or other accountable business role or function.	Salesforce has established policies and procedures for management authorization for development or acquisition of new applications, systems, databases, infrastructure, services, operations, and facilities for the Salesforce Services.
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).	Salesforce does not outsource software development for the Salesforce Services.

Control Area	Control ID	Control Specification	Control Notes
Change Control & Configuration Management *Quality Testing*	CCC-03	Organization 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.	New system components of the Salesforce Services are evaluated by architectural and operational teams, and are introduced following change management requirements. Baseline configurations for servers, network devices, and databases are consistent with industry-accepted system hardening guidelines that address known security vulnerabilities. Operating systems, upgrades, and applications are tested prior to acceptance. Salesforce implements a multipronged approach to help ensure the software released is secure. From initial ideas to release, Salesforce deploys several tools and processes in this regard. Salesforce application development for the Salesforce Services follows software development lifecycle requirements to help ensure security in the development lifecycle, with participation in architecture reviews, secure coding best practices, use of code scanners and manual security testing and independent third party code reviews.
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.	Salesforce deploys security measures and monitoring solutions to help ensure Salesforce employees download only approved applications and tools. Administrative access to the environment for the Salesforce Services is strictly controlled. Critical hosts employ file integrity monitoring (FIM) to detect and alert on changes to their file systems.

Control Area	Control ID	Control Specification	Control Notes
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-critical or customer (tenant), and/or authorization by, the customer (tenant) as per agreement (SLA) prior to deployment.	Network and infrastructure change control procedures are required by Salesforce's Change Management Policy applicable to the Salesforce Services and include steps for testing, review, authorization, communication and fallback procedures. All changes to the infrastructure components are tested in a dedicated environment using production class equipment before being deployed into production. An emergency change process is also in place. Changes are reviewed and approved by Operations management prior to deployment to production for the Salesforce Services. System changes and maintenance are managed using an internal case tracking system. Vendor-supplied OS, application, and networking patches are evaluated by systems administrators, tested on internal systems, and are deployed by the Operations team during announced maintenance periods.

Control Area	Control ID	Control Specification	Control Notes
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.	Salesforce generally does not have visibility into the types of information customers host within the Salesforce Services and does not further classify Customer Data. Salesforce treats all Customer Data as strictly private and confidential and contractually agrees to security and privacy provisions. Salesforce's customers have the ability to implement a wide range of customer-controlled security features in their use of the Salesforce Services to further protect customer-selected categories of Customer Data. Additional information about Salesforce's customer-controlled security features is available to customers via the Salesforce Services' "Help & Training" portal.

Control Area	Control ID	Control Specification	Control Notes
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.	Salesforce maintains current network diagrams for the Salesforce Services, and maintains an inventory of data center sites. Each customer's instance of the service and its associated Customer Data is located in a specific data center and replicated to a specific secondary geographically remote data center. Salesforce maintains internal documentation in order to identify where each customers instance is hosted. As noted in response to DSI-01, Salesforce does not have visibility into the data stored within the Salesforce Services. Salesforce does not use or disclose Customer Data except to provide the services and prevent or address service or technical problems, at the customer's request in connection with customer support matters, or as required by law, while providing appropriate safeguards to protect the confidentiality and integrity of Customer Data. All other processing of Customer Data is generally initiated by the customer's users; thus, compliance with privacy laws rests primarily with the customer and its users by design.
Data Security & Information Lifecycle Management *eCommerce Transactions*	DSI-03	Data related to electronic commerce (e-commerce) 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.	The Salesforce Services is not an eCommerce solution; however eCommerce solutions may be built on the platform by customers and partners. Customer Data transmitted over the wire is secured using TLS 1.0 (defaulting to 1.2 shortly) or higher and encrypted using 256 or 128-bit encryption. The Services use International/Global Step Up SSL certificates with 2048-bit Public Keys. We recommend the use of TLS 1.2 if the customer's client software supports it.

Control Area	Control ID	Control Specification	Control Notes
Data Security & Information Lifecycle Management *Handling / Labeling / Security*	DSI-04	Policies and procedures shall be established for labeling, handling, and the security of data and objects which contain data. Mechanisms for label inheritance shall be implemented for objects that act as aggregate containers for data.	Please refer to the response provided to DSI-01 above.
Data Security & Information Lifecycle Management *Non-Production Data*	DSI-05	Production data shall not be replicated or used in non-production environments.	Salesforce may replicate and use sanitized Customer Data in the segregated, non-production performance testing environment. Physical security controls over the test environment are consistent with the access controls in place for the production environment and tested as a part of external audit/compliance efforts. Logical access controls are in place to restrict access to a small number of performance engineering users and the systems engineering team supporting those systems. Customers may opt out of having Salesforce replicate their Customer Data in non-production environments.
Data Governance *Ownership / Stewardship*	DSI-06	All data shall be designated with stewardship, with assigned responsibilities defined, documented, and communicated.	Salesforce's customers retain all ownership rights to their respective Customer Data and can use the Salesforce Services features to limit accessibility to their data.

Control Area	Control ID	Control Specification	Control Notes
Data Security & Information Lifecycle Management *Secure Disposal*	DSI-07	Policies and procedures shall be established, and 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.	Customer Data submitted to the Salesforce Services remains on disk until the customer deletes or updates it. Customer Data deleted by a customer is temporarily available within a "recycle bin" before being deleted from the system. Media containing Customer Data are stored only within Salesforce's secure data centers. When production tapes reach end of life, they are degaussed, and securely destroyed. Hard drives are securely wiped before returning to the vendor. If hard drives cannot be overwritten, they are securely destroyed. Salesforce sanitizes media that contain Customer Data prior to disposal following the NIST SP 800-88 Guidelines for Media Sanitization.
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.	Salesforce maintains an inventory of critical assets, which includes ownership of the asset. Salesforce maintains an inventory of critical supplier relationships. Salesforce has achieved ISO 27001 certification and asset management is defined through the company's Information Systems Asset Management Policy. This covers items such as acquisition, tracking, ownership, responsibilities and disposal.
Datacenter Security *Controlled Access*	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.	Data centers for the Salesforce Services are physically secured using a defense in depth approach. Access to Salesforce data centers is authorized based on position or role and limited to those few individuals with a business need. Access is controlled via badges/pin pads, biometrics, and security guards. Subsequent entry to the production rooms and cage areas requires two-factor access, including biometrics.

Control Area	Control ID	Control Specification	Control Notes
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.	Salesforce controls access to the Salesforce Services' infrastructure, and these infrastructure components are physically and logically controlled by Salesforce staff. Please also refer to the response in DCS-02.
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.	Authorization is required prior to relocation or transfer of hardware, software, or Customer Data of the Salesforce Services to an offsite premise. Customer Data is kept in Salesforce's secure, dedicated data center space until the systems containing Customer Data are to be retired and destroyed.
Datacenter Security *Off-Site Equipment*	DCS-05	Policies and procedures shall be established for the secure disposal of equipment (by asset type) 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.	Customer Data (and the hardware and software in which it resides) submitted to the Salesforce Services is never physically removed from data centers. Customer Data is stored in Salesforce's secure data center facilities. Salesforce sanitizes media that contain Customer Data prior to disposal following the NIST SP 800-88 Guidelines for Media Sanitization.

Control Area	Control ID	Control Specification	Control Notes
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.	Salesforce has established policies and procedures that govern the Company's offices and data centers for the Salesforce Services. Salesforce implements physical security measures to protect the Company's data centers for the Salesforce Services from unauthorized access and intrusion. Access to these data centers is limited to those personnel who require such access to perform their current duties. Hardware and infrastructure supporting the Salesforce Services are managed by full-time Salesforce employees only. Access is controlled via badges, biometrics, and security guards. Data center physical security is covered in Salesforce's SOC 1 and SOC 2 Type II reports, which are performed twice annually. The reports are available upon request under NDA.
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.	Data centers for the Salesforce Services are physically secured using a defense in depth approach. Access to these data centers is authorized based on position or role and strictly limited to individuals with a business need. Access is controlled via badges/pin pads, biometrics, and security guards. Subsequent entry to the dedicated Salesforce production data center cages/computer rooms requires two-factor authentication (a pin pad or badge and biometric access).

Control Area	Control ID	Control Specification	Control Notes
Datacenter Security *Unauthorized Persons*	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.	Physical access to the data centers and server rooms for the Salesforce Services is monitored 24/7 by data center security personnel through guarded lobbies and CCTV cameras set up inside and outside the data centers in critical areas. The critical areas monitored include; doors to colocation areas, access to cage or Salesforce computer room doors, server floor areas, external building perimeter, data center entries and exits, and shipping/ receiving areas. Salesforce controls visitor access (individuals without pre-authorized access) to the data center facilities by authenticating visitors before authorizing access to the facilities. All visitors must be accompanied by an individual on the Salesforce authorized data center access list. Unaccompanied visitors are not allowed access to the data center. Upon arrival visitors must sign in at the front desk, submit a valid government-issued photo ID, and be approved by an individual on the Salesforce authorized list.
Datacenter Security *User Access*	DCS-09	Physical access to information assets and functions by users and support personnel shall be restricted.	Please refer to the responses provided to DCS-07 and DCS-08 above.
Encryption & Key Management *Entitlement*	EKM-01	Keys must have identifiable owners (binding keys to identities) and there shall be key management policies.	When a customer chooses to implement the Classic Encryption feature for Salesforce Services, the application automatically creates a unique Customer encryption key for the exclusive use of that customer org. Key management is automated; no Salesforce personnel participate in the creation of Customer Keys. The Customer Key is stored in the org record for each customer in the database and is encrypted using the Salesforce Master Application Key. Customer Keys stay encrypted except while in memory in the application tier for use of encrypting or decrypting of customer data.

Control Area	Control ID	Control Specification	Control Notes
Encryption & Key Management *Key Generation*	EKM-02	Policies and procedures shall be established, and supporting business processes and technical measures implemented, 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.	The Salesforce Services manages encryption keys on behalf of customers. Key management and rotation procedures are in place to maintain keys for transmission and storage of Customer Data. Salesforce features enable customers to control their own keys and certificates for integrations with external systems. For the Platform Encryption[1] feature within Salesforce Services, Salesforce uses a HSM based Key Management infrastructure and the DEK (Digital Encryption Keys) are derived in real-time and never persisted either in database or file system.

[1] Additional fee applies for the Platform Encryption feature.

Control Area	Control ID	Control Specification	Control Notes
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) and data in transmission (e.g., system interfaces, over public networks, and electronic messaging) as per applicable legal, statutory, and regulatory compliance obligations.	Database backups for the Salesforce Services are encrypted. Customers can optionally encrypt custom fields of specific types containing Customer Data which they deem sensitive. Using the Platform Encryption[2] feature, customers can also encrypt a specific set of standard fields, files and attachments in their use of the Salesforce Services. Customer Data transmitted over the wire is secured using TLS 1.0 or higher and encrypted using 256 or 128-bit encryption. Browsers may request a stronger cipher on initial negotiation. The Salesforce Services use International/Global Step Up SSL certificates with 2048-bit Public Keys. Salesforce recommends the use of TLS 1.2 if the customer's client software supports it.
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.	Please refer to the responses provided to EKM-02 and EKM-03 above. Third-party gateway solutions may be utilized in connection with the Salesforce Services for encryption or tokenization of data with strict data residency requirements.

[2] Additional fee applies for the Platform Encryption feature.

Control Area	Control ID	Control Specification	Control Notes
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 established and authorized based on business need.	Salesforce has a formal process for placing a system into the production environment for the Salesforce Services (including the hardware, software and appropriate configuration). This procedure includes a build checklist, server hardening checklist and pre-production testing. Baseline security standards are established by Salesforce's Trust function, which are applied during this process. Prior to go-live with new infrastructure for the Salesforce Services, management approval is required and the decision is based upon the results of the pre-production testing. Salesforce regularly reviews and works to improve its security baseline requirements as changes to the underlying infrastructure supporting the Salesforce Services or external factors dictate.

Control Area	Control ID	Control Specification	Control Notes
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 and protection from unauthorized use, access, loss, destruction, and falsification	Regular enterprise-wide risk assessments are conducted on an annual basis to evaluate risks to the Company's business, including potential loss, unauthorized access to, or misuse of Customer Data submitted to the Salesforce Services. In addition to this corporate view of Salesforce's risk profile, individual functions perform risk assessments within their area as part of the Company's compliance activities, including Sarbanes-Oxley, Salesforce Services' FedRAMP moderate level Authority to Operate, PCI-DSS compliance, and ISO 27001 certification. Salesforce's customers determine how long their respective Customer Data is retained in the Salesforce Services. Customer Data remains on disk until the customer deletes or updates it. Customer Data deleted by a customer is temporarily available within a "recycle bin" before being deleted from the system. Salesforce has defined retention periods and end-of-life disposal requirements. When production tapes for the Salesforce Services reach end-of-life, they are degaussed and destroyed. Hard drives are securely wiped before they are returned to the vendor. If hard drives cannot be overwritten, they are purchased and securely destroyed. Salesforce generally does not have visibility into the types of information customers submit to the Salesforce Services and does not further classify Customer Data.

Control Area	Control ID	Control Specification	Control Notes
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.	Salesforce's Information Security Management System (ISMS) and information security policies applicable to the Salesforce Services are based on the ISO 27002 framework of best practices and are ISO 27001 certified. As required by this certification, the ISMS is endorsed by Senior Management. All employees are required to acknowledge responsibility for complying with Company policies, including specifically Information Security policies.

Control Area	Control ID	Control Specification	Control Notes
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	Please refer to the response provided to GRM-03 above.

Control Area	Control ID	Control Specification	Control Notes
Governance and Risk Management *Management Support/Involvement*	GRM-05	Executive and line management shall take formal action to support information security through clearly-documented direction and commitment, and shall ensure the action has been assigned.	Please refer to the responses provided to GRM-02 and GRM-03 above.
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.	Information security policies are published on the Intranet and communicated to personnel through internal training and awareness campaigns. Required training on Information Security policies is conducted upon hire and annually thereafter. Please refer to the response provided to GRM-03 above.
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.	Salesforce's information security policies contain enforcement sections providing that violations may result in disciplinary action up to and including termination.

Control Area	Control ID	Control Specification	Control Notes
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.	An information security risk assessment applicable to the Salesforce Services is performed annually, as required by the Company's ISO 27001 certification. Security policies and procedures are reviewed a minimum of annually and updated if necessary. Security policies and procedures may also change in the event of a significant change in practice.
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.	Salesforce regularly reviews and improves its Information Security Management System manual and related policies applicable to the Salesforce Services. Individual policy documents are reviewed when revised or annually at a minimum if there are no revisions.
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, 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).	Enterprise-wide risk assessments are performed annually to determine the likelihood and impact of identified risks. Results are contributed to the annual Internal Audit plan.

Control Area	Control ID	Control Specification	Control Notes
Governance and Risk Management *Risk Mitigation / Acceptance*	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 executive approval.	Risk treatment plans for the Salesforce Services state risk mitigation requirements, timelines, and organizational responsibilities. Risk acceptance is based upon recommendation by technical and compliance teams and requires executive signoff.
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.	Salesforce has a defined and documented process for the return of company-owned assets upon employment, contract or agreement termination.
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.	Salesforce utilizes a third-party provider to perform background investigations on all incoming employees in the U.S. Salesforce also uses a third-party provider to perform background investigations on incoming employees in certain foreign countries. The scope of these checks is subject to local laws in the jurisdictions in which the employee is hired. Such investigations may include criminal background checks, education verification, and employment history verification.
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.	Salesforce requires all employees to certify compliance with the Company's Code of Conduct, which includes sections on confidentiality, security, and privacy on an annual basis. Additionally, all employees are required to complete an annual information security and privacy awareness training program. Salesforce communicates on an ongoing basis with all employees regarding information security and privacy issues.

Control Area	Control ID	Control Specification	Control Notes
Human Resources *Employment Termination*	HRS-04	Roles and responsibilities for performing employment termination or change in employment procedures shall be assigned, documented, and communicated.	Roles and responsibilities for performing employment termination or change in employment procedures are managed and documented by the Company's Employee Success (Human Resources) organization. Salesforce's Employee Success and Legal departments determine employee termination processes. Violations of the Company's Code of Conduct, which includes sections on confidentiality, security, and privacy, may result in disciplinary action up to and including termination.
Human Resources *Mobile Device Management*	HRS-05	Policies and procedures shall be established, and supporting business processes and technical 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).	Customer Data submitted to the Salesforce Services is not stored on portable or mobile devices and technical controls are in place to prevent the transfer of Customer Data to portable media by users with logical access to manage the production systems. Salesforce has a comprehensive information security program that includes policies and procedures regarding portable and mobile devices, including the use of Mobile Device Management (MDM) technology. Information security policies are included within the scope of annual testing by the Company's external third-party auditor as part of the Company's ISO 27001 certification.
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.	Salesforce has a dedicated Privacy team to address legal and regulatory requirements for privacy including non-disclosure agreements. Requirements for confidentiality agreements reflecting the organization's needs for the protection of data and operational details are identified, documented and reviewed at planned intervals. Please also refer to the response provided to HRS-03.

Control Area	Control ID	Control Specification	Control Notes
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.	Contracts are in place with all third parties that support the production environment of the Salesforce Services, e.g. colocation data center providers, which define the roles and responsibilities of their personnel as they relate to the relationship and information security. These third party vendors are audited by Salesforce against SLAs and terms within their contract, including adherence to the Company's policies and procedures on a periodic basis.
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. 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.	The confidentiality of Customer Data is of paramount concern to the Company. Salesforce provides contractual assurance to its customers that the data customers host in the Salesforce Services will be kept confidential and not accessed except under narrow circumstances as set forth by contract (such as a support issue). Salesforce claims no ownership rights to Customer Data and Customer Data is only utilized as the customer instructs, or to fulfill contractual or legal obligations. Additional information can be found on the Company's public facing trust website at https://trust.salesforce.com/. Please also refer to the response provided to HRS-06 above.

Control Area	Control ID	Control Specification	Control Notes
Human Resources *Training / Awareness*	HRS-9	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.	Salesforce requires every new hire to complete an information security awareness training course and complete the updated information security training annually thereafter. The Information security policies are published on the Intranet and communicated to personnel through internal training and awareness campaigns on an ongoing basis.
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	Salesforce requires every new hire to complete an information security awareness training course and complete the updated information security training annually thereafter. Training and awareness topics include the responsibility to follow Information Security policies including preventing unauthorized access to information.
Human Resources *Workspace*	HRS-11	Policies and procedures shall be established to require that unattended workspaces do not have openly visible (e.g., on a desktop) sensitive documents and user computing sessions had been disabled after an established period of inactivity.	Salesforce has a Clean Workspace Policy that specifies protection of data in work environment. Centralized management of endpoints forces automated screen lockout due to inactivity and other controls.

Control Area	Control ID	Control Specification	Control Notes
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 segmented and restricted to prevent compromise and misuse of log data.	Salesforce restricts, logs, and monitors access to its information security management systems for the Salesforce Services. Access to log data is restricted to a limited number of authorized personnel. Segregation of duties are in place to ensure that individuals with access to logs are separate from operations teams.
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 and 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 business relationships)	Salesforce's information security policies for the Salesforce Services contain access control sections based on the least-privilege principle. A formal process is in place to request access to applications, databases, and server and network infrastructure supporting the Salesforce Services. All access requests must be approved by management, documented and periodically reviewed for appropriateness. Revocation of user access is performed in a timely manner upon termination or transfer into a role that no longer requires existing access. Customer access to their Customer Data stored within the Salesforce Services is managed by the customer's application administrator(s). Salesforce offers a Security Implementation Guide that describes the controls and features available to application administrators within the service: http://resources.docs.salesforce.com/198/0/en-us/sfdc/pdf/salesforce_security_impl_guide.pdf Refer to Salesforce's Multi-tenant Architecture whitepaper for information regarding access and logical data segmentation within the infrastructure: https://developer.salesforce.com/page/Multi_Tenant_Architecture

Control Area	Control ID	Control Specification	Control Notes
		• 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 (e.g., encryption and strong/multi-factor, expireable, non-shared authentication secrets) • Permissions and supporting capabilities for customer (tenant)	

Control Area	Control ID	Control Specification	Control Notes
		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.	Salesforce has internally-developed guidelines for hardening systems related to the Salesforce Services. All unused services, ports, and packages are disabled. Devices are configured to not expose management interfaces externally to the internet. A minimal set of user accounts is maintained and no shared password files are allowed. User access to systems supporting the Salesforce Services is restricted based on the least privilege principle.
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.	Please refer to the response for Server Administrative Access in the IAM-02 Credential Lifecycle and Provision Management response above.

Control Area	Control ID	Control Specification	Control Notes
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-role conflict of interest.	Segregation of duties for the Salesforce Services is defined in the Company's Segregation of Duties Standard which covers items such as ensuring administrators to one domain do not normally have access to other domains and the controls in place to grant, supervise and monitor such access. Developers do not have access to make changes to the infrastructure supporting the Salesforce Services. This is tested twice annually as part of Salesforce's SOC 1 and SOC 2 Type II audits.
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.	Controls are in place to prevent unauthorized access to the application, program and object source code for the Salesforce Services. Access is restricted to authorized personnel only. This is tested twice annually as part of Salesforce's SOC 1 and SOC 2 Type II audits. Salesforce allows customers to configure access to their instances of the Salesforce Services. This enables customers to restrict access to their Customer Data as they deem necessary.
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.	Identification and prioritization of risks due to access by third parties is part of Salesforce's overall risk assessment process for the Salesforce Services. Salesforce qualifies such vendors prior to access following the Company's internal standards, including network and host controls, external scanning, and onsite audits and reviews of controls and documentation.

Control Area	Control ID	Control Specification	Control Notes
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.	Please refer to the response for Server Administrative Access in the IAM-02 Credential Lifecycle and Provision Management response above.
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.	Salesforce's information security policies for the Salesforce Services contain access control sections based on the least-privilege principle. Access to production operating systems and databases and code repository for the Salesforce Services is restricted to authorized personnel based on job function and requires documented management approval. All users and application-level security are defined and maintained by a customer's organization administrator, and not by Salesforce. The organization administrator is appointed by the customer. An organization's sharing model sets the default access that users have to each other's data. Please also refer to the response provided to HRS-08 above.

Control Area	Control ID	Control Specification	Control Notes
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.	Salesforce conducts regular access reviews for Salesforce personnel with access to the Salesforce Services. Salesforce performs quarterly reviews for access to systems containing sensitive information. Such reviews are tested twice-annually as part of Salesforce's independent SOC 1 and SOC 2 Type II audits.
Identity & Access Management *User Access Revocation*	IAM-11	Timely de-provisioning (revocation or modification) of user 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.	Salesforce's information security policies for the Salesforce Services contain access de-provisioning sections. Access to production operating systems and databases and code repository for the Salesforce Services is revoked upon notification of an employee's termination by the Employee Success department and such access ends on the date of termination. All users and application-level security are defined and maintained by a customer's organization administrator, and not by Salesforce. The organization administrator is appointed by the customer. An organization's sharing model sets the default access that users have to each other's data. Salesforce provides tools for automated user de-provisioning and access revocation. Administrators appointed by customers can define and configure this process.

Control Area	Control ID	Control Specification	Control Notes
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 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)	User management and application-level security settings for the Salesforce Services are configured and maintained by the customer's administrator. These security controls include password strength (minimum length, complexity, aging, history), lockout after invalid attempts, identity verification prior to password reset, and session inactivity and duration limits. Customers can choose to implement stronger controls, such as SSO, IP address restrictions, and two-factor authentication using third-party packages, or via federated or delegated methods supported by the Salesforce Services, as needed. Customer administrators manage API accounts and their permissions in accessing the Salesforce Services. Equal or stronger controls are in place for Salesforce personnel provisioning the Salesforce Services. Refer to the prior responses for the Identity & Access Management control objective above for details on credential lifecycle management.

Control Area	Control ID	Control Specification	Control Notes
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.	Salesforce has system hardening guidelines applied to servers, databases and network devices for the Salesforce Services. This includes the use of common configuration files to help ensure that the same services are disabled on all machines. In addition, Salesforce has File Integrity Monitoring installed on critical hosts supporting the Salesforce Services and monitor to detect and alert in the event that changes are made to critical system files and configurations. Salesforce does not utilize virtualization in the provision of the Salesforce Services.
Infrastructure & Virtualization Security *Audit Logging / Intrusion Detection*	IVS-01	Higher levels of assurance are required for protection, retention, and lifecyle 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.	Privileged user access/failed attempts to Salesforce infrastructure, file integrity monitoring on hosts, and network intrusion detection events are logged and correlated in a security event monitoring system. Correlated events are configured to generate alerts and logs which are monitored by Salesforce's Computer Security Incident Response Team (CSIRT). As a component of Salesforce Shield[3], Salesforce provides the complete application event logs to customers on demand. Customers can mine these logs and generate reports and visualizations as required by their policies.

[3] Additional fee applies for the Salesforce Shield feature.

Control Area	Control ID	Control Specification	Control Notes
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).	Not applicable. Salesforce does not utilize virtualization in the provision of the Salesforce Services.
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.	Clocks for routers, firewalls, and servers for the Salesforce Services are synchronized using NTP, with the GPS clock as source.

Control Area	Control ID	Control Specification	Control Notes
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 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.	The Salesforce Services are designed to achieve in excess of 99.9% availability. Salesforce uses commercially reasonable efforts to make its on-demand services available to its customers 24/7, except for planned downtime, for which Salesforce gives customers prior notice, and force majeure events. Live and historical statistics on the Salesforce system performance is publicly published at http://trust.salesforce.com/trust/status. Salesforce has defined thresholds for key system components for the Salesforce Services, such as network, storage, memory, I/O, etc., which are monitored by Salesforce personnel. Capacity demands (system and application) are monitored daily. Capacity planning engineers monitor network, data center, infrastructure, and application utilization to ensure capacity demands are met, and future requirements are anticipated.
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).	Not applicable. Salesforce does not utilize virtualization in the provision of the Salesforce Services.
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, and ports, and by compensating controls.	Salesforce's network configuration standards for the Salesforce Services require network device rulesets to control connections to untrusted networks, and include allowed ports, protocols, and services, as well as a review of those rulesets at regular intervals. Network and data flow diagrams are regularly updated and reviewed as part of Salesforce Services' compliance audits.

Control Area	Control ID	Control Specification	Control Notes
Infrastructure & Virtualization Security *OS Hardening and Base Controls*	IVS-07	Each operating system shall be hardened to provide only necessary ports, protocols, and 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.	Salesforce has a formal process for placing a system into production for the Salesforce Services (including the hardware, software and appropriate configuration). This procedure includes a build checklist, server hardening checklist and pre-production testing. Baseline configurations for servers, network devices, and databases are consistent with industry-accepted CIS (Center for Internet Security) system hardening guidelines that address known security vulnerabilities. Prior to go-live with new infrastructure, management approval is required and the decision is based upon the results of the pre-production testing.
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.	Development/QE environments for the Salesforce Services are physically and logically segregated from production environments. Administrative access to these environments follows the Segregation of Duties Policy.

Control Area	Control ID	Control Specification	Control Notes
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 • Compliance with legal, statutory and regulatory compliance obligations	Salesforce's multitenant architecture and secure logical controls for the Salesforce Services address the separation of Customer Data. Salesforce does not use dedicated servers used for a specific customer. The infrastructure for the Salesforce Services is divided into a modular architecture based on instance. Each instance is capable of supporting several thousand customers in a secure and efficient manner.
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.	Not applicable. Salesforce does not utilize virtualization in the provision of the Salesforce Services.

Control Area	Control ID	Control Specification	Control Notes
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).	Not applicable. Salesforce does not utilize virtualization in the provision of the Salesforce Services.

Control Area	Control ID	Control Specification	Control Notes
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 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	System and network configuration (including the use of perimeter firewalls), use of encryption, and rogue wireless detection for the Salesforce Services are required by Salesforce's internal policies and standards and are audited regularly against applicable compliance frameworks.

Control Area	Control ID	Control Specification	Control Notes
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.	Salesforce implements a multi-tiered network architecture for the Salesforce Services. Multilevel security products from security vendors and security practices help ensure network security. To help prevent malicious attacks through unmonitored ports, external firewalls allow only http and https traffic on ports 80 and 443, along with ICMP traffic. Switches help ensure that the network complies with the RFC 1918 standard, and address translation technologies further enhance network security. IDS sensors help protect all network segments. Internal software systems are protected by two-factor authentication, along with the extensive use of technology that controls points of entry. All networks are certified through third-party vulnerability assessment programs.

Control Area	Control ID	Control Specification	Control Notes
Interoperability & Portability *APIs*	IPY-01	The provider shall use open and published APIs to ensure the broadest support for interoperability between components and to facilitate migrating applications.	There are a number of integration points on the Force.com platform, which is part of the Salesforce Services. From a developer perspective, customers can invoke web services from the platform, or expose classes on the platform as web service endpoints. Customers can also interact with external HTTP endpoints, react to incoming email messages, and have automated outbound messages sent when certain events occur. Customers can use the Force.com Web Services API. There is a SOAP-based web services API, as well as a REST-based web services API, that provide direct access to data within a customer's organization. Using these APIs, a client can be created to integrate with Force.com from a customer's language of choice. Toolkits that wrap around this API provide utility classes that make this integration even easier for a range of languages, including Java, .NET, PHP, Objective C, Ruby and Adobe Flex. View additional details on this topic here: http://bit.ly/SalesforceAPI

Control Area	Control ID	Control Specification	Control Notes
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).	Several methods exist to export data from the Salesforce Services. • Direct Export - Data can be exported directly into CSV (comma separated values) file, or Excel files with a button click. This can be done from either a standard or custom list view, or from a report. This is the most common method utilized by end users. • Excel Connector - Salesforce provide an Excel Connector to push and pull data from Excel to Salesforce Services and vice versa. • Salesforce API - Data can be exported to and from the system though Salesforce's API at any time or via a number of built in features. • Salesforce Data Loader - The Salesforce Apex Data Loader is a free tool which is used specifically for importing/updating/exporting data in Salesforce Services. • Partner Tools - There are also many pre-integrated partner tools, some of which you may already own that may be leveraged. Examples of these include, but are not limited to, Informatica, Pervasive, CastIron, Boomi, etc. The Salesforce Services also offer a *weekly export service* (WES) for those customers requiring a local backup copy of their data or a data set for import into other applications (such as an ERP system). Unstructured data is provided in the same file format as the original data, e.g. .jpg, .pdf, .docx.

Control Area	Control ID	Control Specification	Control Notes
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.	Force.com provides open, standards-based APIs that developers can use to build apps. Both RESTful and Web services (SOAP-based) APIs are available that provide access to Force.com's many features. Salesforce maintains a Developerforce site with details of the APIs supported and Developers guides for the various APIs. Refer here for information on Integration options: http://wiki.developerforce.com/page/Integration Refer here for Developer Guides under the Integration heading: http://wiki.developerforce.com/page/Documentation
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.	Please refer to the responses provided to IVS-06, IPY-01, IPY-02, and IPY-03 above.
Interoperability & Portability *Virtualization*	IPY-05	The provider shall use an industry-recognized virtualization platform and standard virtualization formats (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.	Not applicable. Salesforce does not utilize virtualization in the provision of the Salesforce Services.

Control Area	Control ID	Control Specification	Control Notes
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.	Salesforce provides security awareness training to its employees covering topics such as working remotely, information security policies (which have sections dedicated to acceptable use and mobile security), and mobile devices, including discussion of authorized devices, laptop security, and social media.
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.	Acceptable use of mobile devices and appropriate locations for storage of Customer Data is addressed in Salesforce's Information Security policies applicable to the Salesforce Services. Customer Data is not stored by Salesforce on portable or mobile devices and technical controls are in place to prevent the transfer of Customer Data to portable media by Salesforce users with logical access to manage the Salesforce Services' production systems. Customers control data storage configuration on mobile devices for their users. If data is cached or stored on mobile devices, the data is encrypted on the device.
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.	Salesforce's Information Security policies address the installation of only approved applications and the prohibition of installing un-approved applications on mobile devices. MDM (Mobile Device Management) tools control the installation and use of approved applications.

Control Area	Control ID	Control Specification	Control Notes
Mobile Security *Approved Software for BYOD*	MOS-04	The BYOD policy and supporting awareness training shall clearly state the approved applications and application stores that may be used for BYOD usage.	Acceptable use of BYOD devices is covered under Salesforce's Information Security policies and security awareness training. As previously noted, Customer Data is not stored by Salesforce on portable or mobile devices and technical controls are in place to prevent the transfer of Customer Data to portable media by Salesforce users with logical access to manage the production systems.
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.	Salesforce has a documented mobile device security policy as part of the Company's information security policies. Please also refer to the prior Mobile Security responses above.
Mobile Security *Cloud Based Services*	MOS-06	All 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.	Please refer to the prior Mobile Security responses provided above.
Mobile Security *Compatibility*	MOS-07	The company shall have a documented application validation process to test for device, operating system, and application compatibility issues.	Prior to new mobile devices or different operating system versions being allowed for connection to Salesforce's corporate assets, they must be tested and validated by both Salesforce corporate IT and Trust (Information Security).
Mobile Security *Device Eligibility*	MOS-08	The BYOD policy shall define the device and eligibility requirements to allow for BYOD usage.	Please refer to the prior Mobile Security and BYOD responses provided above.

Control Area	Control ID	Control Specification	Control Notes
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.	Salesforce uses a Mobile Device Management (MDM) solution to manage the distribution of applications, data and configuration settings for mobile devices allowed in the Company's corporate environment. Through the use of MDM technologies, Salesforce maintains an inventory of devices allowed to store and access corporate data. As previously noted, Customer Data is not stored by Salesforce on mobile devices.
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.	Please refer to the response provided to MOS-09 Device Inventory above.
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.	The capability for encryption of data on mobile devices is included in the evaluation and validation of new mobiles devices allowed in the environment and described in response to MOS-07 Compatibility provided above.
Mobile Security *Jailbreaking and Rooting*	MOS-12	The mobile device policy shall prohibit the circumvention of built-in security controls on mobile devices (e.g. jailbreaking or rooting) and shall be enforced through detective and preventative controls on the device or through a centralized device management system (e.g. mobile device management).	Jailbreaking and Rooting is prohibited by the Salesforce mobile device policy. Please also refer to the details around use of MDM technology in response to MOS-07 Compatibility provided above.

Control Area	Control ID	Control Specification	Control Notes
Mobile Security *Legal*	MOS-13	The BYOD policy shall include clarifying language for the expectation of privacy, requirements for litigation, e-discovery, and legal holds. The BYOD policy shall clearly state the expectations over the loss of non-company data in the case a wipe of the device is required.	Please refer to the prior Mobile Security responses above. The mobile security policy addresses the potential for monitoring of activity on BYOD devices with access to corporate data, potential requirements for e-discovery or legal holds, and the potential loss of non-company data in the event a wipe of a BYOD device is required.
Mobile Security *Lockout Screen*	MOS-14	BYOD and/or company owned devices shall require an automatic lockout screen, and the requirement shall be enforced through technical controls.	The mobile security policy addresses automatic password lockout requirements, including, minimum character length, and passlock expiration. The Password format is defined and administered by Corporate IT.
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.	Changes to mobile device operating systems, patch levels, and/or applications are managed via MDM. Please refer to the responses provided to MOS-09 Device Inventory and MOS-07 Compatibility above.
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.	Password policies and password usage for Salesforce personnel using mobile devices are addressed by the mobile security policy, and are enforced by MDM. Please refer to the responses provided to MOS-09 and MOS-14 above.

Control Area	Control ID	Control Specification	Control Notes
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).	The mobile device policy addresses malware concerns for mobile devices and data backups used by Salesforce personnel. The policy prohibits the transmission or storage of Salesforce company and customer information on external devices and systems not procured by the company.
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.	Through the use of MDM, Salesforce may remote wipe its employees' mobile devices. Employees must agree to download the MDM client to corporate-owned or BYOD devices in order to access corporate systems and assets.
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.	Salesforce employees are required to download the latest security patches for mobile devices that have been approved by Corporate IT and Trust. This is managed via MDM. Please refer to the response provided to MOS-07 Compatibility above.
Mobile Security *Users*	MOS-20	The BYOD policy shall clarify the systems and servers allowed for use or access on a BYOD-enabled device.	The mobile security policy addresses what systems and servers are allowed for use or access on a mobile device by Salesforce employees.

Control Area	Control ID	Control Specification	Control Notes
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.	Salesforce liaises with external counsel, security and privacy organizations, and industry associations where appropriate to help ensure security and privacy compliance. Salesforce maintains contacts with law enforcement authorities, including local and federal authorities.
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.	Salesforce has a formal Incident Management Process applicable to the Salesforce Services. During a security incident, the process guides Salesforce personnel in management, communication, and resolution activities. Regular updates are provided to engaged parties until issue resolution. Incident tracking and resolution is documented and managed within an internal ticketing system.

Control Area	Control ID	Control Specification	Control Notes
Security Incident Management, E-Discovery & Cloud Forensics *Incident Reporting*	SEF-03	Workforce personnel and external business relationships shall be informed of their responsibility 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 obligations.	Employees are informed through regular information security trainings that if they know or suspect there is a breach of security, it must be reported to the individual's manager or Information Security. New hire orientation includes the Company Code of Conduct, which states that employees must safeguard Customer Data and report violations of the Code, under consequences of termination of employment and civil and legal action. The new hire process also includes signing a receipt for the Employee Handbook, the Code of Conduct, and signing a confidentiality agreement. Third party suppliers that support the Salesforce Services, with potential access to Customer Data, are contractually required to notify Salesforce of information security events involving Customer Data. Salesforce will promptly notify the Customer in the event of any security breach of the Service resulting in an actual or reasonably suspected unauthorized disclosure of Customer Data. Notification may include phone contact by Salesforce Support, email to customer's administrator and Security Contact (if submitted by customer).

Control Area	Control ID	Control Specification	Control Notes
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.	In the event of a security incident, proper forensic procedures including chain of custody will be performed for collection, retention, and presentation of evidence. In the event of an actual or reasonably suspected unauthorized disclosure of Customer Data, Salesforce will inform affected customers of the details of the incident to the extent legally permissible and any actions being taken to remediate and prevent further breaches from occurring.
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.	The Salesforce CSIRT follows an Incident Response plan, which includes the process for monitoring reports and alerts and responding to security incidents. Incident analysis includes data for response process improvement on an ongoing basis.
Supply Chain Management, Transparency and Accountability *Data Quality and Integrity*	STA-01	Providers shall inspect, account for, and correct data quality errors and risks inherited from partners within their cloud supply-chain. 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.	Third parties engaged in the provision of the Salesforce Services are required to enter into contracts with Salesforce including confidentiality provisions, background screening requirements, training and breach of policy and enforcement provisions.

Control Area	Control ID	Control Specification	Control Notes
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).	Salesforce has a formal Incident Management Process. During a security incident, the process guides Salesforce personnel in management, communication, and resolution activities. Regular updates are provided to engaged parties until issue resolution. Incident tracking and resolution is documented and managed within an internal ticketing system. Please refer to the response provided to SEF-03 Timely Reporting of Security Events above.
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.	Salesforce's contracts with its colocation facilities and network service providers for the Salesforce Services include provisions for capacity, resiliency, and service delivery. Please also refer to the responses provided to BCR-01, BCR-03, BCR-09 and IVS-04 above.
Supply Chain Management, Transparency and Accountability *Provider Internal Assessments*	STA-04	The provider shall perform annual internal assessments of conformance and effectiveness of its policies, procedures, and supporting measures and metrics.	Please refer to the response provided to STA-01 Data Quality and Integrity above.

Control Area	Control ID	Control Specification	Control Notes
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 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	Salesforce's customer contracts include many of the topics described. Please refer to the standard Salesforce Services Master Subscription Agreement (MSA) for details: http://www2.sfdcstatic.com/assets/pdf/misc/salesforce_MSA.pdf Salesforce Services Documentation describing the Security and Compliance practices: https://help.salesforce.com/apex/HTViewSolution?urlname=Salesforce-Services-Trust-and-Compliance-Documentation&language=en_US

Control Area	Control ID	Control Specification	Control Notes
		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 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	

Control Area	Control ID	Control Specification	Control Notes
Supply Chain Management, Transparency and Accountability *Supply Chain Governance Reviews*	STA-06	Providers shall review the risk management and governance processes of their partners to ensure that practices are consistent and aligned to account for risks inherited from other members of that partner's cloud supply chain.	Please refer to the response provided to STA-01 Data Quality and Integrity above.
Supply Chain Management, Transparency and Accountability *Supply Chain Metrics*	STA-07	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for maintaining complete, accurate, and relevant agreements (e.g., SLAs) between providers and customers (tenants), with an ability to measure and address non-conformance of provisions and/or terms across the entire supply chain (upstream/downstream), and for managing service-level conflicts or inconsistencies resulting from disparate supplier relationships.	Please refer to the response provided to STA-01 Data Quality and Integrity above.
Supply Chain Management, Transparency and Accountability *Third Party Assessment*	STA-08	Providers shall assure reasonable information security across their information supply chain by performing a regular review. The review shall include all partners upon which their information supply chain depends.	Please refer to the response provided to STA-01 Data Quality and Integrity above.

Control Area	Control ID	Control Specification	Control Notes
Supply Chain Management, Transparency and Accountability *Third Party Audits*	STA-09	Third-party service providers shall demonstrate compliance with information security and confidentiality, service definitions, and delivery level agreements included in third-party contracts. Third-party reports, records, and services shall undergo audit and review at planned intervals to govern and maintain compliance with the service delivery agreements.	Please refer to the response provided to STA-01 Data Quality and Integrity above.
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.	Customer Data is not stored by Salesforce on Salesforce endpoint devices. The production environment for the Salesforce Services is managed via a secure remote client that prevents the ability for malware to traverse from the local client laptop or desktop to the hosted environment. Salesforce has anti-virus programs installed on systems which support the Salesforce Services. Salesforce runs anti-virus software on the production systems, which are Linux or Unix based. Other controls are also used to address malware such as hardening the operating system of servers, firewall configuration to ensure only required ports are open and all others denied, and implementing intrusion detection systems. Access to these systems is restricted to authorized personnel and all these systems, as well as the host platforms, are monitored in real-time through a security event monitoring system.

Control Area	Control ID	Control Specification	Control Notes
Threat and Vulnerability Management *Vulnerability / Patch Management*	TVM-02	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for timely detection of vulnerabilities within organizationally-owned or managed (physical and virtual) applications and infrastructure network and system components, applying a risk-based model for prioritizing remediation through change-controlled, vender-supplied patches, configuration changes, or secure software development for the organization's own software. Upon request, provider shall inform customer (tenant) of policies and procedures, especially if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control.	Salesforce regularly performs self-vulnerability assessments for the Salesforce Services using various tools and techniques, including network-layer vulnerability scans, application-layer vulnerability scans, and local operating system-layer vulnerability scans. Depending on the severity and the risk to Salesforce systems, security patches can be scheduled for immediate deployment or deferred to an appropriate planned maintenance interval.

Control Area	Control ID	Control Specification	Control Notes
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.	Salesforce has controls over mobile code within its corporate environment. Customers have the ability to utilize mobile code and it is their responsibility to secure end-systems and implement a security policy in regards to appropriate use of mobile code.