Salesforce Security White Paper for Salesforce Government Cloud

Overview

An ever-growing list of federal, state, local government agencies, and government contractors trust Salesforce to deliver critical business applications, in large part because of Salesforce's commitment to security and privacy. This white paper provides an overview of Salesforce's principles of trust and compliance specifically for the Salesforce Government Cloud in the context of the Federal Risk and Authorization Management Program (FedRAMP). Subsequent sections of this paper provide an introduction to the security and privacy features inherent to the Force.com Platform, Salesforce Services, and Analytics Cloud that customers can use to build and secure their applications and Customer Data. The security and privacy features that help achieve compliance with the FedRAMP moderate baseline controls, derived from NIST SP 800-53 rev. 4, are referenced throughout this document.

Principles of Trust

Salesforce's vision is to be the government's trusted cloud Platform as a Service (PaaS) and Software as a Service (SaaS) provider, based on the values of maintaining confidentiality, integrity and availability of Customer Data. Salesforce's methods to fulfill this vision are built upon an executive commitment to maintain and continuously improve the security of Salesforce's services and include:

- Defense-in-depth: Whenever possible, multiple controls and technologies are applied to limit the possibility of any single point of failure;
- Investment: Invest in personnel, tools, and technologies to manage, analyze, and improve security effectiveness; and
- Transparency: Trust cannot be maintained without open communications regarding service performance and reliability. Salesforce strives to be industry leaders in transparency. See trust.salesforce.com for further details.

Federal Risk and Authorization Management Program

As the government's trusted cloud provider, Salesforce's information security program for the Salesforce Government Cloud is aligned with the FedRAMP requirements. On May 23, 2014, Salesforce achieved a FedRAMP Agency Authority to Operate (ATO) at the moderate impact level issued by Health and Human Services (HHS) for the Salesforce Government Cloud. The Salesforce Government Cloud is a portion of Salesforce's multi-tenant community 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). The Salesforce Government Cloud information system and authorization boundary, is comprised of the Force.com Platform, Analytics Cloud, Salesforce Services (Sales Cloud, Service Cloud, Chatter, Work.com, as well as, features of these applications including Content, Ideas, Knowledge, Chatter messenger, Chatter files, customer facing Chatter groups, Chatter answers, Salesforce Platform Encryption, Event Monitoring) and Salesforce Industry Applications, as well as, the backend infrastructure (servers, network devices, databases, storage arrays) that support the operations of these products, referred to as the General Support System (GSS). A complete list of current in-scope Salesforce products included in the authorization boundary for the FedRAMP ATO can be provided to customers upon request.

To obtain compliance with FedRAMP, Salesforce conducted security assessment and authorization activities in accordance with FedRAMP guidance, NIST 800-37, and HHS guidance. As part of this process, Salesforce documented a System Security Plan (SSP) for the Salesforce Government Cloud service offering. The SSP is developed in accordance with NIST SP 800-18, Guide for Developing Federal Information System Security Plans. The SSP identifies control implementations for the GSS and in-scope customer facing products (Force.com Platform, Salesforce Services, Analytics Cloud) according to the FedRAMP moderate baseline and HHS security control parameters. A security assessment of the information system was conducted by a third party assessment organization (3PAO) in accordance with NIST 800-53A and FedRAMP requirements. The security assessment testing determined the adequacy of the management, operational, and technical security controls used to protect the confidentiality, integrity, and availability of the Salesforce service and the Customer Data it stores, transmits and processes.

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 at least annual independent assessment of a selection of security controls. In May 2015, as part of our FedRAMP annual assessment, Salesforce completed the transition to revision 4 of NIST 800-53.

Cloud Computing Security Assurance

As a SaaS and PaaS leader, data security is very important for Salesforce. Salesforce serves over 150,000 customers and processes over four billion transactions a day. The organizations that use Salesforce include customers in heavily regulated industries such as financial services, healthcare, insurance, and public sector that require strict adherence to security and privacy requirements. Salesforce raises the bar of security to meet the security needs of our customers.

In May 2008, Salesforce became the first publicly traded SaaS vendor to receive the prestigious ISO/IEC 27001 Security Certification (ISO 27001) company-wide and service-wide, addressing applicable controls including our data centers and major offices worldwide. As the only internationally accepted security standard, ISO 27001 ensures security best practices and a managed approach to business information protection, and helps us to provide a consistent, reliable and secure operating environment to our customers worldwide. In addition, Salesforce has undergone SSAE 16 SOC 1 (previously known as SAS 70 Type II) examinations semi-annually since 2004. Salesforce also completes SOC 2 and SOC 3 for Service Organizations audits and has achieved compliance with PCI-DSS Level 1.

Cloud Computing and Information Security Governance

Information security governance is a term that encompasses all the tools, people, and business processes an organization uses to ensure the security and privacy of the data that its systems maintain. Because cloud computing is a business model that can include a layered set of providers, secure cloud computing happens only when there is a commitment to information security governance from both the underlying platform provider as well as application providers that use the platform to deploy applications and manage data.

Figure 1 summarizes the security governance realms of cloud platform providers and cloud application providers. The platform provider's security governance realm includes the design and maintenance of a secure platform and policies that protect the privacy of its direct customers and data. Meanwhile, an application provider's security governance realm includes the use of platform features to build secure applications and the implementation of security and privacy policies that ultimately protect end-user Customer Data from threats and privacy concerns. Salesforce provides both PaaS (Force.com Platform) and SaaS (Salesforce Services, Analytics Cloud) services to its customers. Salesforce's approach to information security governance is structured around the ISO 27002 framework and consistent with the requirements identified in NIST SP 800-53 Rev. 4, and includes many components:

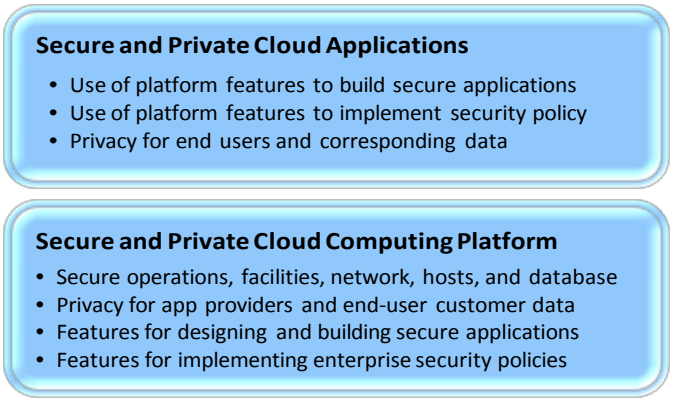

Figure 1: Secure, private cloud computing requires security governance from both the platform provider and application providers that use the platform

- **Employees** – Employees receive regular information security training. Employees in data-handling positions receive additional role-based training specific to their roles *[AT-2, AT-3].*
- **Security Staff** – Salesforce has dedicated security staff supporting the system, including a Chief Trust Officer and a full staff of certified professionals (i.e. Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker (CEH) *[PM-2].*
- **Counsel** – Salesforce has a team of Privacy Counsel, Compliance, and Government Contracts Attorneys who are responsible for ensuring compliance with global privacy laws, international regulatory regimes, and federal procurement regulations.
- **Assessments** – Salesforce regularly conducts both internal vulnerability assessments (for example, architecture reviews by security professionals, vulnerability scans) as well as external third party audits and external vulnerability assessments (for example, vulnerability assessments by managed security services providers, or MSSPs) *[RA-5, SI-2].*
- **Policies and Procedures** – Detailed internal policies dictate how Salesforce handles various aspects of the security and compliance governance. Examples of security policies and procedures include: Incident Response Plan, Datacenter Access Procedures, Configuration Management Plan, etc. *[IR-1, PE-1, CM-1].*

In particular, Salesforce incorporates security into its development processes at all stages. From initial architecture considerations to post-release, all aspects of software development incorporate security. Figure 2 summarizes some of the standard practices Salesforce employs, which have made it the trusted provider that it is today.

- **Design phase** – Guiding security principles and security training help ensure Salesforce engineers make the best security decisions possible. Threat assessments on high-risk features help to identify potential security issues as early in the development lifecycle as possible *[SA-3, SA-8].*
- **Coding phase –** Salesforce addresses standard vulnerability types through the use of secure coding patterns and anti-patterns, and uses static code analysis tools to identify security flaws *[SA-10].* Secure code development during design, development, and release is controlled through a secure code repository.
- **Testing phase –** Internal Salesforce staff and independent security consultants use scanners and proprietary tools along with manual security testing to identify potential security issues *[SA-11].*
- **Prior to release** – Salesforce validates that the functionality being developed and maintained meets its internal security requirements. Code is tested and approved prior to release. Post-release, Salesforce uses independent security service providers to analyze and monitor the product for potential security issues. These reports are made available to prospects and customers under a non-disclosure agreement *[SA-11].*

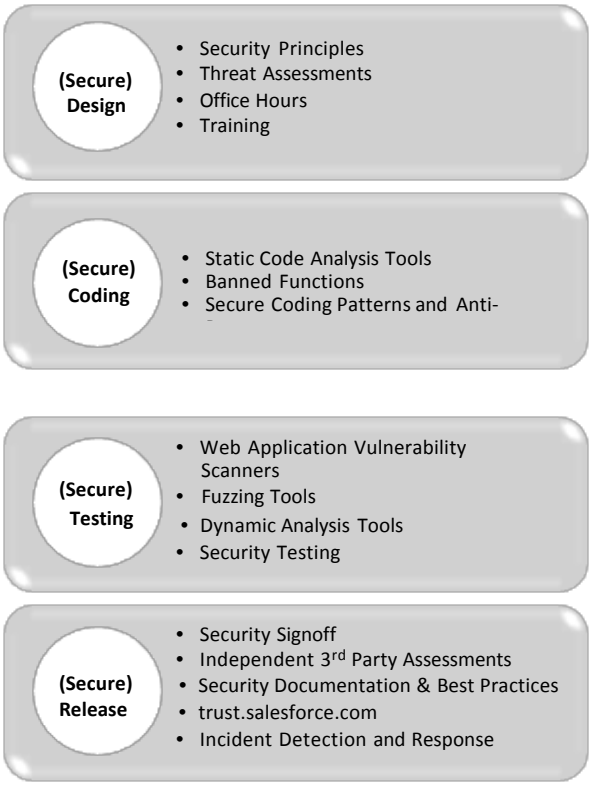

Figure 2: Salesforce incorporates security into every phase of its development lifecycle to ensure the security of its platform.

Platform Security

Figure 3 illustrates the many layers of defense the Force.com Platform uses to resist various types of threats and achieve compliance with security frameworks such as FedRAMP, SSAE 16 SOC 1, SOC 2, SOC 3, ISO 27001, and PCI-DSS Level 1—all without sacrificing application performance.

At the infrastructure layer, Salesforce strictly manages access to its facilities and the work engineers can perform once inside a facility *[PE-2].* Before being granted access, employees must pass a thorough Salesforce background check *[PS-2].* Once a person is authorized for logical access, the engineer can access the production network using secure methods of production access private networks, and stringent segregation of duties and least privileges *[AC-2, AC-5, AC-6, IA-2].*

Qualified Personnel

For the Salesforce Government Cloud, additional controls have been implemented around personnel management. Access to systems inside of the Salesforce Government Cloud storing U.S. government, U.S. government contractors, and FFRDC Customer Data that potentially permit access to Customer Data will be restricted to Qualified U.S. Citizens. Qualified US Citizens are individuals who are United States citizens, are physically located within the United States when accessing the Salesforce Government Cloud systems; and have completed a background check as a condition of their employment with Salesforce. Research and development personnel and personnel that provide Administration Services under Government Cloud Premier + Success Plan support, that have logical access to Customer Data, and infrastructure support personnel that provide Government Cloud Premier + Success Plan support that have physical access to the Salesforce Government Cloud infrastructure, will be Qualified US Citizens. All other personnel, including Customer Success Managers, Success Account Managers, Customer Success Technologists and any other personnel engaged in customer success roles and providing customer success services (collectively referred to as "Success Representatives") will not be Qualified U.S. Citizens and will not have access to Customer Data unless Customer provides such personnel a User ID or otherwise enables the sharing of Customer Data with such personnel *[PS-2, PS-3].*

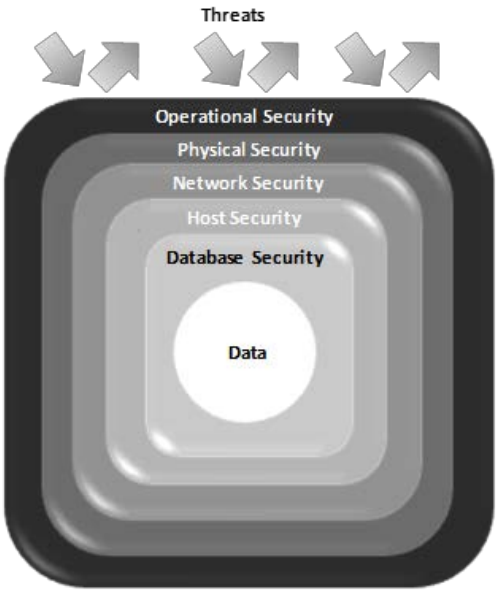

Figure 3: Salesforce incorporates security at multiple layers to protect against threats.

Multi-tenancy

The Salesforce service is delivered using a multi-tenant model. The multi-tenant architecture and secure logical controls address separation of Customer Data.

The Salesforce infrastructure is divided into a modular architecture based on “instances”. Each instance is capable of supporting several thousand customers in a secure and efficient manner. Salesforce uses the instance architecture to continue to scale and meet the demands of our customers. There are appropriate controls in place designed to prevent any given customer’s implementation of Salesforce from being compromised. This functionality has been designed and undergoes robust testing through an on- going process by both Salesforce and its customers *[AC-2, SC-4].*

Salesforce Government Cloud

To support the security and compliance needs of our U.S. public sector customers, Salesforce launched the Salesforce Government Cloud. The Salesforce Government Cloud is a portion of Salesforce’s multi-

tenant community 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). The isolated Production infrastructure supporting the Salesforce Government Cloud Customer Data ensures that the physical hardware in Salesforce's colocation data centers that process, store, and transmit unencrypted Government Customer Data are separate from hardware supporting other customers. While isolated, the underlying infrastructure supporting the Salesforce Government Cloud is the same trusted architecture model that supports Salesforce's multi-tenant public cloud offering and over four billion customer transactions a day.

Physical and Environmental Controls

Customer Data, as defined in the Salesforce Master Subscription Agreement available at https://www.salesforce.com/company/legal/, for customers in Salesforce's Government Cloud is stored in two of our U.S. data center locations. Our service is collocated in dedicated spaces at top-tier data centers. Salesforce's hardware is located inside of secure server rooms designated to Salesforce and separated by concrete walls from other data center tenants. Individual racks inside of the data center are secured with a lock. Specific racks are allocated for hardware supporting the Salesforce Government Cloud. Access to the racks supporting the Salesforce Government Cloud hardware is restricted to Qualified U.S. Citizens as described in the section above.

Data centers provide only power, environmental controls, and physical security. Salesforce employees manage all other aspects of the service at the data centers. Colocation data center personnel do not have network or logon access to the Salesforce systems. Colocation personnel have physical access to the Salesforce secure server room in the event of an emergency, but do not have keys to the individual racks containing hardware. Data centers maintain a common baseline of physical and environmental controls across data centers.

The exterior perimeter of each anonymous data center building is bullet resistant, has concrete vehicle barriers, closed-circuit television coverage, alarm systems, and manned 24/7 guard stations that together help defend against non-entrance attack points. Inside each building, multiple biometric scans and guards limit access through interior doors and to the Salesforce secure rooms at all times.

Access to Salesforce's secure server rooms in the datacenter is authorized based on position or role. Additional access controls enforced by an electronic key box are implemented for the dedicated Salesforce Government Cloud racks to ensure that access is limited to Qualified U.S. Citizens. Salesforce has an established process to review data center access logs to the server room. Additionally, an at least annual assessment of the data center is performed to ensure the data centers are meeting Salesforce's security control requirements *[PE-2, PE-3].*

In addition to securing the data center locations, it is critical that the data center facilities maintain robust critical infrastructure to support Salesforce through the following services:

Temperature and Humidity Controls *[PE-14]*

- Humidity and temperature control
- Redundant (N+1) cooling system

Power ***[PE-11]***

- Underground utility power feed
- Redundant (N+1) CPS/UPS systems
- Redundant power distribution units (PDUs)
- Redundant (N+1) diesel generators with on-site diesel fuel storage

Secure Network Logistics ***[CP-8, PE-4]***

- Concrete vaults for fiber entry
- Redundant internal networks
- Network neutral; connects to all major carriers and located near major Internet hubs
- High bandwidth capacity

Fire Detection and Suppression ***[PE-13]***

- VESDA (very early smoke detection apparatus)
- Dual-alarmed, dual-interlock, multi-zone, pre-action dry pipe water-based fire suppression

Network Protection

Salesforce secures its network on many different fronts. For example:

- **End-to-end TLS (v 1, 1.1, 1.2)** cryptographic protocols encrypt network data transmissions from the customer to Salesforce *[SC-8(1)].*
- **Perimeter firewalls and edge routers** block unused protocols. External traffic that does not conform to the firewall rules is blocked. The edge routers are configured with access control lists (ACLs) to filter unwanted network traffic and if necessary apply traffic rate limits. Traffic that is allowed by the ACL is routed to the external firewalls. All external firewalls are configured by default to deny all traffic and allow by exception *[CM-7, SC-7, SC-7(3)].*
- **Stateful packet inspections** (SPI) firewalls inspect all network packets and prevent unauthorized connections *[SC-7].*
- **Intrusion detection sensors** placed throughout the network monitor traffic and report events to a security logging and alerting system for logging, alerts, and reports *[AC-4, SC-7, SI-4].*
- **Secure routing and traffic flow policies** ensure that customer traffic is encrypted entering Salesforce until the load balancer decrypts the traffic. The load balancers decrypting the traffic are FIPS 140-2 compliant and are located inside of the Salesforce Government Cloud isolation boundary. Network devices enforce traffic flow policies in the Salesforce Government Cloud *[SC-4, SC-5, SC-7, SC-7(3), SC-7(4), SC-8, SC-8(1)].*
- **Denial-of-Service (DoS) protection** is provided using a multi-layered approach utilizing high availability, traffic monitoring, anomaly detection, and a third party DoS mitigation service. Salesforce uses multiple Internet Service Providers (ISPs) to ensure redundancy of connections and increased availability. Monitoring is performed continuously and we have a contract with a third party DoS mitigation service should an active DoS attack be discovered *[SC-5].*

Logical Access Controls

Salesforce has implemented strong logical access controls for the production network including:

- **Authorized users** are granted production access after manager approval and based on business justification. Terminated users are removed in a timely manner *[AC-2].*
- **Two-factor authentication processes** verify the authentication of access requests to internal systems *[IA-2(1), IA-2(2)].*
- **Bastion Hosts** act as hardened barriers between the authentication perimeter and core servers *[AC-2, IA-2, IA-2(1)].*
- **Segregation of duties and least privilege** is enforced to ensure that employees are granted only the necessary level of access to the Production network to perform their assigned job functions based on role *[AC-5, AC-6].*
- **Infrastructure logging** is enabled to capture system activity and logs are forwarded to a central logging system *[AU-2].*

Configuration and Change Management

Salesforce implements industry-accepted best practices to harden underlying systems that support the various software layers of the service *[CM-2, CM-6].* For instance, hosts are configured with non-default software configurations and minimal processes, user accounts, and network protocols. Hosts log their activity in a remote, central location for safekeeping. Salesforce has performed a review of device configurations against the Center for Internet Security Benchmarks (where available) to ensure devices are configured securely *[CM-6, CM-6(1)].*

Change Management processes dictate that system changes and maintenance are documented in Salesforce's internal ticketing system. Changes require approval, testing, and security impact analysis prior to deployment *[CM-3, CM-4].* In addition, any changes that constitute a significant change, per Salesforce's significant change definition, require analysis and an impact assessment to determine impact to the Salesforce Government Cloud Authority to Operate *[CA-6].*

Database Security

The underlying database layer plays a significant role in platform security. For example, the database protects customer passwords by storing them via the SHA algorithm with a 256-bit one-way hash. Salesforce enforces strict control of database administrator access to only authorized individuals with a business justification for access *[AC-2, IA-2(8), IA-5, IA-5(1), IA-5(6), IA-5(7)].* Databases are configured in accordance with security benchmarks provided by the Center for Internet Security *[CM-6].* Databases undergo periodic vulnerability assessments to check the databases for known vulnerabilities *[RA-5].*

Operational Monitoring

The Salesforce application and website are monitored on a 24x7 basis for reliability and performance.

- The Site Reliability (SR) team monitors the service and has subject matter experts (SME's) in various disciplines. The SR handles first-and second-tier support, with technical engineers providing escalation support.
- Overall system monitoring is provided by a variety of tools and alerts are aggregated.
- Monitoring tools are automated and route issues, warnings, and problems to the Site Reliability teams.

- Alerts of events of significance are routed to the on-call personnel as well as the engineering teams.

Salesforce has built extensive monitoring and instrumentation into the application itself, so that the application can accurately report its health and performance to on-call support staff and engineers *[IR-2, MA-3, PM-6].*

Security Monitoring

A variety of tools, third-party resources, and a dedicated Computer Security Incident Response Team (CSIRT) provide comprehensive monitoring of the Salesforce production environment. These include:

- **Intrusion Detection Systems (IDS):** IDS monitor the production network for potentially malicious network traffic *[AC-4, SC-7, SI-4].*
- **Logging and Alerting System:** Activity logs from production devices and servers are sent to a logging and alerting system that reports, and alerts on events *[AC-2(4), AU-2, AU-6, SI-4].*
- **Threat Monitoring:** The Salesforce security team receives and reviews threat alerts from a variety of sources including SANS, United States Computer Emergency Readiness Team (US-CERT), and Open Web Application Security Project (OWASP). Threats that are deemed critical are escalated to the appropriate resource to respond *[SI-5].*
- **Vulnerability Scanning:** Vulnerability scans are performed on a periodic basis to check hosts for known vulnerabilities. Vulnerabilities are remediated in accordance with established remediation timeframes *[RA-5].*
- **Perimeter monitoring:** Third-party security firms provide periodic vulnerability scanning and continuous perimeter monitoring to detect vulnerabilities and alerts on security related incidents *[RA-5, SI-2].*
- **Security Incident Monitoring:** The CSIRT monitors for security incidents. Identified security incidents are handled in accordance with the Incident Response Plan *[IR-4].*

Incident Response

Salesforce maintains an Incident Response Plan and has an established Security Incident Response Process. During a security incident, the process guides Salesforce personnel in management, communication, and resolution activities. Salesforce will notify customers in the event Salesforce becomes aware of 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), and public posting on trust.salesforce.com. *[IR-4, IR-6, IR-8].*

Government customers can report security incidents related to their Salesforce products and offerings via security_gov@salesforce.com. Salesforce will respond accordingly in accordance with the incident response process described above.

Disaster Recovery and Backup

The Salesforce service performs replication at each data center and annual disaster recovery tests for the service verify the projected recovery times and data replication between the production data center and the disaster recovery center. The disaster recovery site is a warm site intended to contain equal capacity of the primary production site (host, network, storage, data). Data is transmitted between the primary and

disaster recovery data centers across encrypted links. Additionally, back-ups of data are performed and data is retained on backups at the geographically separated disaster recovery data center location *[CP-4, CP-6, CP-7, CP-9, MP-5]*.

Media Sanitization

Salesforce has an established process for sanitizing media consistent with industry guidelines and consistent with NIST SP 800-88 Guidelines for Media Sanitization *[MP-6]*.

Platform and Application Security

The Force.com Platform, Salesforce Services, and Analytics Cloud provide extensive features and tools designed to provide security for the data generated by customers. This section introduces many of the features customers can use to implement security policies governing exactly who, what, from where, when, and how users can access specific IT applications and data, along with related auditing requirements.

The default user authentication mechanism for the Force.com Platform, Salesforce Services, and Analytics Cloud requests that a user provide a username and password (credentials) to establish a connection. The Force.com Platform, Salesforce Services and Analytics Cloud do not use cookies to store confidential user and session information *[AC-2, IA-2]*.

Many organizations use single sign-on mechanisms to simplify and standardize user authentication across a portfolio of applications [IA-2(1), IA-2(2), IA-5, IA-5(1)]. The Force.com Platform, Salesforce Services and Analytics Cloud support two single sign-on options:

- **Federated authentication single sign-on** using Security Assertion Markup Language (SAML) allows a session to send authentication and authorization data between affiliated but unrelated Web services.
- **Delegated authentication single sign-on** enables an organization to integrate cloud applications with an authentication method of choice, such as an LDAP (Lightweight Directory Access Protocol) service or authentication using a token instead of a password.

Customers can implement multi-factor authentication by integrating with one of Salesforce's single sign-on capabilities *[IA-2(1), IA-2(2)]*.

The Force.com Platform, Salesforce Services, and Analytics Cloud offer several features to further confirm the identity of a connection request. For example, when a user requests a connection for the first time using a new computer-browser-IP address combination, Salesforce notices this fact, sends an email to the user, and requests that the user confirm his/her identity by clicking on the activation link in the email. The user's browser then maintains an encrypted cookie to expedite future connection requests *[IA-2]*.

User authentication and identity confirmation determine who can log in, and network-based security features limit where users can log in from and when. The Force.com Platform, Salesforce Services, and Analytics Cloud include the ability to restrict the hours during which users can connect and the range of IP addresses from which they can connect. When an organization imposes IP address restrictions and a connection request originates from an unknown address, the connection is denied, thus helping to protect data from unauthorized access and "phishing" attacks *[SC-7(3), SC-7(4)]*.

To protect established sessions, the Force.com Platform, Salesforce Services, and Analytics Cloud monitor and terminate idle sessions after a configurable period of time. Session security limits help defend system access when a user leaves his/her computer unattended without first disconnecting *[AC-11]*.

Login profiles provide organizations an efficient way to manage system and application access for sets of similar users. First, an administrator creates a profile that controls access to entire applications, specific application tabs (pages), administrative and general user permissions, and object permissions (CRUD (create, read, update, delete)), along with other settings. Then, the administrator assigns each user a login profile. If the common requirements for a set of users change, all that is necessary is an update to the login profile for that group of users (not each individual user) *[AC-2, AC-5, AC-6]*.

To enable users to perform their jobs without exposing data they do not need access to, the Force.com Platform and Salesforce Services provide a flexible, layered sharing design that lets an organization expose specific application components and data sets to different sets of users *[AC-2, AC-5, AC-6, SC-2]*.

- **User profiles** – An organization can control the access its users have to objects by customizing profiles. Within objects, organizations can then control the access users have to fields using field-level security. Sharing settings allow for further data access control at the record level.
- **Sharing settings** – Organization-wide default sharing settings provide a baseline level of access for each object and let the organization extend that level of access using hierarchies or sharing rules. For example, an organization can set the default access for an object to Private when users should only be able to view and edit the records they own, and then create sharing rules to extend access of the object to particular users or groups.
- **Sharing rules** – Sharing rules allow for exceptions to organization-wide default settings that give additional users access to records they don't own. Sharing rules can be based on the record owner or on field values in the record.
- **Manual sharing** – When individual users have specific access requirements, owners can manually share records. Although manual sharing is not automatic like organization-wide defaults, role hierarchies, or sharing rules, it lets record owners share particular records with particular users, as necessary.

By request, the Force.com Platform, Salesforce Services, and Analytics Cloud can also require users to pass a user verification test (CAPTCHA) to export data. This simple text-entry test helps prevent malicious automated programs from accessing an organization's data.

The Force.com Platform and Salesforce Services have a multitude of history tracking and auditing features that provide valuable information about the use of an organization's applications and data, which in turn can be a critical tool in diagnosing potential or real security issues *[AU-2, AU-6, AU-7, AU-11]*. Auditing features include:

Record Modification Fields
All objects include fields to store the name of the user who created the record and who last modified the record. This provides some basic auditing information.

Login History
You can review a list of successful and failed login attempts to your organization for the past six months within Salesforce.

Field History Tracking
You can also enable auditing for individual fields, which will automatically track any changes in the values of selected fields. Although auditing is available for all custom objects, only some standard objects allow field-level auditing.

Setup Audit Trail
Administrators can also view a Setup Audit Trail for the past six months within Salesforce, which logs when modifications are made to your organization's configuration.

While the Login History and Setup Audit Trail are available for six months within Salesforce, audit trails can be downloaded or exported via API and stored locally to meet longer audit log retention requirements *[AU-11]*.

Event Monitoring
Event monitoring provides granular level logging data via an API for monitoring user activity within Salesforce. Administrators can view information about individual events or track trends in events to identify abnormal behavior and safeguard data *[AU-2, AU-6, AU-7].*

Logical Security

The Force.com Platform, Salesforce Services, and Analytics Cloud innovative metadata-driven, multitenant database architecture delivers operational and cost efficiencies for cloud-based applications without compromising the security of each organization's data.

- When a user establishes a connection, the user is assigned a client hash value associated with the session.
- During login, the authenticated user is mapped to their Org and access privileges according to the sharing model *[AC-5, AC-6].*
- Along with the formation and execution of each application request, the application confirms that the user context (an organization ID (orgID)) accompanies each request and includes it in the WHERE clause of all SQL statements to ensure the request targets the correct organization's data. The application validates that every row in the return set of a database query matches the session's orgID *[SC-4]*.
- Before the rendering of a Web page that corresponds to an application request, the application confirms that the calculated client hash value matches the client hash value that was set during the login phase *[SC-4].*
- An error in the query process does not return any data to the client *[SI-11]*.

Data Ownership

Salesforce will maintain customer access to Customer Data, however Customer Data is owned by the customer. Customers have the ability to extract their data via Export Services utilities including: weekly export (for applicable products), data loader, APIs, EAI tools, etc.

Data Retention

Active Customer Data stays on disk until the customer deletes or changes it. Customer-deleted data is temporarily available (15 days) to customers online from the Recycle Bin. Backups are rotated every 90

days (30 days for sandboxes), therefore changed or deleted data older than 90 days (30 days for sandboxes) is unrecoverable.

Salesforce customers are responsible for complying with their company's data retention requirements in their use of the Salesforce services. If a Salesforce customer must preserve data and the retention procedures above are insufficient, they may export their data at no charge as part of the Applications' applicable Export Services utilities identified above, or may create a sandbox account for storage of this data. Exports of Customer Data are otherwise available in comma separated value (.csv) format by request via Salesforce's Customer Support department for a fee. In addition, an Org administrator can manually pull many exports detailing system usage and other data.

Protecting PII Information

In accordance with OMB M-07-16, Salesforce has conducted a Privacy Threshold Assessment (PTA) and Privacy Impact Assessment (PIA) for the delivery of the Salesforce service. The Salesforce service is rated as a moderate impact system. As such, Salesforce has implemented security controls aligned with the FedRAMP moderate Rev. 4 security baseline and was assessed against the FedRAMP moderate Rev. 4 baseline *[PL-5].*

Customers are responsible for conducting their own PTA and PIA for Customer Data stored in Salesforce. NIST SP 800-60 Rev. 1 provides guidance to organizations on categorizing an information system and states that for personally identifiable information (PII) the confidentiality impact level should generally fall into the moderate range. Salesforce recommends that federal agencies relying on this FedRAMP ATO determine the Security Categorization of their data to ensure the data stored in Salesforce does not exceed the moderate impact level *[PL-5]*.

As discussed in the previous sections, the Force.com Platform, Salesforce Services, and Analytics Cloud have numerous configurable security features that allow customers to customize security based on the sensitivity of data customers store in the application consistent with the requirements in NIST SP 800-53 Rev. 4 for moderate impact systems. One such security feature is encryption. The Salesforce service provides the ability to encrypt fields and files. Customers can implement Classic Encryption for selected custom fields, or for an additional fee, customers can implement Platform Encryption to encrypt a variety of widely used standard fields, along with some custom fields and many kinds of files. The value of an encrypted field is only visible to users that have the "View Encrypted Data" permission. Encrypted fields utilize AES-128-bit keys for Classic Encryption and AES-256-bit keys for Platform Encryption. The encryption libraries for both Classic Encryption and Platform Encryption are FIPS 140-2 validated *[SC-13, SC-13(1)].* Additional security controls are detailed in Salesforce's Security Implementation Guide: http://login.salesforce.com/help/doc/en/salesforce_security_impl_guide.pdf

Privacy

At Salesforce, there is no higher priority than the privacy and security of our customers' data. We believe that protecting the privacy of our customers' data is integral to our mission of earning and maintaining the trust of each of our customers. We seek to lead the industry as a trusted repository for Customer Data through a world-class privacy program and provide a secure infrastructure and flexible tools that help enable our customers to comply with global privacy and data protection regulations.

Privacy Statement: http://www.salesforce.com/company/privacy/

For detail on privacy protection at Salesforce: http://content.trust.salesforce.com/trust/en/learn/protection/

For information on the Global Privacy Law Landscape: http://www.trust.salesforce.com/trust/learn/laws

Transparency

Salesforce is transparent about security and privacy issues. Real-time system information is available at the company's "trust site" at http://trust.salesforce.com. Here, anyone can find live data on system performance, current and recent phishing and malware attempts, and tips on best security practices.

Conclusion: Government Agencies and Government Contractors Trust Salesforce

Salesforce recognizes and appreciates that government solutions need to address specific high-priority security requirements. We will continue to partner with governments at all levels to demonstrate that the required level of protection can be provided in the cloud environment. For more detailed information on Salesforce's security for the Salesforce Government Cloud, please contact publicsector@salesforce.com.

Document Disclaimer