Security, Privacy and Architecture of Government Cloud Plus

Published: September 11, 2020

Salesforce's Corporate Trust Commitment

Salesforce is committed to achieving and maintaining the trust of our customers. Integral to this mission is providing a robust security and privacy program that carefully considers data protection matters across our suite of services, including protection of Customer Data as defined in Salesforce's Master Subscription Agreement or in Salesforce's Terms of Service (for customers purchasing Government Cloud Plus through a reseller).

Services Covered

This documentation describes the architecture of, the security- and privacy-related audits and certifications received for, and the administrative, technical, and physical controls applicable to the services branded and sold as Government Cloud Plus.

Architecture and Data Segregation

Government Cloud Plus is operated in a multitenant architecture that is designed to segregate and restrict Customer Data access based on business needs. The architecture provides an effective logical data separation for different customers via a customer-specific unique identifier and allows the use of customer and user role-based access privileges. Additional data segregation is ensured by providing separate environments for different functions, especially for testing and production.

The specific infrastructure used to host and process Customer Data is described in the "Infrastructure and Sub-processors" documentation available here.

Control of Processing

Salesforce has implemented procedures designed to ensure that Customer Data is processed only as instructed by the customer, throughout the entire chain of processing activities by Salesforce and its sub-processors. In particular, Salesforce and its affiliates have entered into written agreements with their sub-processors containing privacy, data protection and data security obligations that provide a level of protection appropriate to the processing activities provided by them. Compliance with such obligations as well as the technical and organizational data security measures implemented by Salesforce and its sub-processors are subject to regular audits. The "Infrastructure and Sub-processors" documentation linked to above describes the sub-processors and certain other entities material to Salesforce's provision of Government Cloud Plus.

Audits and Certifications

The following security- and privacy-related audits and certifications are applicable to Government Cloud Plus, as described below:

- **FedRAMP High Provisional Authority to Operate (P-ATO):** Salesforce's information security control environment applicable to Government Cloud Plus undergoes an annual, independent evaluation in accordance with FedRAMP program requirements. Salesforce's FedRAMP High P-ATO is issued by the FedRAMP Joint Authorization Board (JAB). Salesforce's most recent FedRAMP package is available upon request by completing and submitting a FedRAMP Package Access Request Form to the FedRAMP Program Management Office (PMO).
- **ISO 27001/27017/27018 certification**: Salesforce operates an information security management system (ISMS) for Government Cloud Plus in accordance with the ISO 27001 international

standard and aligned to ISO 27017 and ISO 27018. Salesforce has achieved ISO 27001/27017/27018 certification for its ISMS from an independent third party. The Salesforce ISO 27001/27017/27018 Certificate and Statement of Applicability are available upon request from your organization’s Salesforce account executive.
- **System and Organization Controls (SOC) report**: Salesforce’s information security control environment applicable to Government Cloud Plus undergoes an independent evaluation in the form of SOC 1 (SSAE 18 / ISAE 3402) and SOC 2 audits. Salesforce’s most recent SOC 1 (SSAE 18 / ISAE 3402) and SOC 2 reports are available upon request from your organization’s Salesforce account executive.
- **APEC Privacy Recognition for Processors (PRP):** Customer Data submitted to Government Cloud Plus is within the scope of Salesforce's PRP certification under the APEC Privacy Framework. The current certification is published in the PRP Compliance Directory at http://cbprs.org/compliance-directory/prp/.

Additionally, Government Cloud Plus undergoes security assessments by internal personnel and authorized third parties, which may include vulnerability and other security assessments of the infrastructure, application and production environment.

As further described in the “Infrastructure and Sub-processors” documentation, Salesforce uses infrastructure provided by a third party, Amazon Web Services, Inc. (“AWS”), to host and process Customer Data submitted to Government Cloud Plus. Information about security- and privacy-related audits and certifications received by AWS, including information on ISO 27001 certification and Service Organization Control (SOC) reports, is available from the AWS Security website and the AWS Compliance website.

Security Controls

Government Cloud Plus includes a variety of configurable security controls that allow customers to tailor the security of Government Cloud Plus for their own use. Please see additional information on such controls in the Salesforce Security Guide.

Government Cloud Plus uses AWS, as described above; further information about security provided by AWS is available from the AWS Security website, including AWS’s overview of security processes.

Security Policies and Procedures

Government Cloud Plus is operated in accordance with the following policies and procedures to enhance security:

- Customer passwords are stored using a one-way salted hash. Customers can optionally configure and use multi-factor authentication mechanisms.
- Salesforce personnel will not set a defined password for a user. Passwords are reset to a random value (which must be changed on first use) and delivered automatically via email to the requesting user.
- Passwords are not logged.
- User access log entries will be maintained, containing date, time, user ID, URL executed or entity ID operated on, operation performed (created, updated, deleted) and source IP address. Note that source IP address might not be available if NAT (Network Address Translation) or PAT (Port Address Translation) is used by Customer or its ISP.
- If a customer suspects inappropriate access, Salesforce can provide customers log entry records and/or analysis of such records to assist in forensic analysis when available. This service will be

provided to customers on a time and materials basis.

- System infrastructure logs and application logs will be retained in compliance with FedRAMP requirements. Logs will be kept in a secure area to prevent tampering.
- Certain administrative changes to Government Cloud Plus (such as password changes and adding custom fields) are tracked in an area known as the "Setup Audit Trail" and are available for viewing by a customer's system administrator. Customers may download and store this data locally.

Further information about security provided by AWS is available from the AWS Security Website, including AWS's overview of security processes.

Intrusion Detection

Salesforce, or an authorized third party, monitors for unauthorized intrusions using network-based and/or host-based intrusion detection mechanisms. Salesforce may analyze data collected by users' web browsers for security purposes, including to detect compromised browsers, to prevent fraudulent authentications, and to ensure that Government Cloud Plus functions properly.

Security Logs

All Salesforce systems used in the provision of Government Cloud Plus log information to their respective system log facilities or a centralized logging service (for network systems) in order to enable security reviews and analysis. These logs are only accessible from within the Government Cloud Plus environment and only by Qualified US Citizens. "Qualified US Citizens" are individuals who: (a) are United States citizens; (b) are physically located within the United States while performing support for Government Cloud Plus; and (c) have completed a background check as a condition of their employment with Salesforce.

Incident Management

Salesforce maintains security incident management policies and procedures. Security incident management for Government Cloud Plus is performed by Qualified US Citizens on Salesforce's Government Computer Security Incident Response Team that is responsible for monitoring and rapid response to computer security incidents for Government Cloud Plus 24/7.

Salesforce publishes system status information on the Salesforce Trust website. Salesforce typically notifies customers of significant system incidents by email, and for availability incidents lasting more than one hour, may invite impacted customers to join a conference call about the incident and Salesforce's response.

User Authentication

Access to Government Cloud Plus requires authentication via one of the supported mechanisms as described in the Salesforce Security Guide, including user ID/password, SAML- based Federation, OpenID Connect, OAuth, Social Login, certificate-based authentication, or Delegated Authentication as determined and controlled by the customer. Following successful authentication, a random session ID is generated and stored in the user's browser to preserve and track session state.

Physical Security

Production data centers used to provide Government Cloud Plus have access control systems. These systems permit only authorized personnel to have access to secure areas. These facilities are designed to withstand adverse weather and other reasonably predictable natural conditions, are secured by around-the-clock guards, two-factor access screening, and escort controlled access, and are also supported by on-site back-up generators in the event of a power failure.

Further information about security provided by AWS is available from the AWS Security Website and the AWS Data Centers Controls Website.

Reliability and Backup[1]

All networking components, network accelerators, load balancers, Web servers and application servers are configured in a redundant configuration. All Customer Data submitted to Government Cloud Plus is stored on a primary database server with multiple active clusters for higher availability. All Customer Data submitted to Government Cloud Plus is stored on highly redundant carrier-class disk storage and multiple data paths to ensure reliability and performance. All Customer Data submitted to Government Cloud Plus, up to the last committed transaction, is automatically replicated on a near real-time basis to the secondary site and backed up to localized data stores. Backups are verified for integrity and stored in the same data centers as their instance. The foregoing replication and backups may not be available to the extent the Health Cloud or Financial Services Cloud is uninstalled by a Customer's administrator during the subscription term because doing so may delete Customer Data submitted to such services without any possibility of recovery.

Disaster Recovery[2]

Production instances are designed to mitigate the risk of single points of failure and provide a resilient environment to support service continuity and performance. Salesforce has disaster recovery procedures in place which provide for backup of critical data and services. A system of recovery processes exists to bring business-critical systems for Government Cloud Plus back online if needed.

Salesforce has disaster recovery plans in place and tests them at least once per year. The scope of the disaster recovery exercise is to validate the ability to failover a production instance from the primary site to the secondary site utilizing developed operational and disaster recovery procedures and documentation.

Viruses

Government Cloud Plus does not scan for viruses that could be included in attachments or other Customer Data uploaded into Government Cloud Plus by a customer. Uploaded attachments, however, are not executed in Government Cloud Plus and therefore will not damage or compromise Government Cloud Plus by virtue of containing a virus.

Data Encryption

Government Cloud Plus uses industry-accepted encryption products to protect Customer Data and communications during transmissions between a customer's network and Government Cloud Plus, including through Transport Layer Encryption (TLS) leveraging at least 2048-bit RSA server certificates and 128-bit AES symmetric encryption keys at a minimum.

Return of Customer Data[3]

[1] This section does not apply to Scratch Orgs.

[2] This section does not apply to Scratch Orgs.

[3] This section does not apply to Scratch Orgs. This section also does not apply to any Customer Data that

Within 30 days post contract termination, customers may request return of their respective Customer Data submitted to Government Cloud Plus (to the extent such data has not been deleted by Customer, or if Customer has not already removed the managed package in which the Customer Data was stored). Salesforce shall provide such Customer Data via downloadable files in comma separated value (.csv) format and attachments in their native format. Note that Customer Data your organization submits to Einstein Analytics instance groups for analysis is derived from other data to which your organization has access, for example, data stored by your organization using Service Cloud, Sales Cloud, third-party applications, etc. The foregoing return of Customer Data for managed packages may not be available if the packages were removed prior to contract termination.

Deletion of Customer Data[4]

After termination of all subscriptions associated with an environment, Customer Data submitted to Government Cloud Plus is retained in inactive status within Government Cloud Plus for 120 days, after which it is securely overwritten or deleted from production within 90 days, and from backups within 180 days.

Without limiting the ability for customers to request return of their Customer Data submitted to Government Cloud Plus, Salesforce reserves the right to reduce the number of days it retains such data after contract termination. Salesforce will update this Salesforce Security, Privacy and Architecture Documentation in the event of such a change.

Day 0, subscription terminates	Day 0 - 30	Day 30 - 120	Day 121 - 211	Day 121 - 301
	Data available for return to customer	Data inactive and no longer available	Data deleted or overwritten from production	Data deleted or overwritten from backups

The foregoing deletion of Customer Data for managed packages may not be available
if the packages were removed prior to contract termination.

Sensitive Data

Important: Customers must use either "Platform Encryption" for supported field types and file attachments or the "Classic Encryption" custom fields feature, and manage the lifecycle of their encryption keys, when submitting payment cardholder data and authentication data, credit or debit card numbers, or any security codes or passwords to Government Cloud Plus. Customers may not otherwise submit such data to Government Cloud Plus. For other categories of sensitive data, customers should also consider using "Platform Encryption" or "Classic Encryption."

Customers may not submit Federal Taxpayer Information data to Government Cloud Plus. Additionally, for Government Cloud Plus, the following types of sensitive personal data may not be submitted: personal health information, where Customer is a health care provider, health care clearinghouse, health plan, or an entity performing functions on behalf of such entities, except in limited circumstances where, subject

has been encrypted using Platform Encryption Cache-Only Key Service.

[4] This section does not apply to Scratch Orgs.

to restrictions, Salesforce has expressly permitted such submission contractually.

If Customer does submit personal health information or other sensitive or regulated data to Government Cloud Plus, then Customer is responsible for ensuring that its use of Government Cloud Plus to process that information complies with all applicable laws and regulations.

For clarity, the foregoing restrictions do not apply to financial information provided to Salesforce for the purposes of checking the financial qualifications of, and collecting payments from, its customers, the processing of which is governed by Salesforce's Website Privacy Statement.

Analytics

Salesforce may track and analyze the usage of Government Cloud Plus for the purposes of security and of helping Salesforce improve both Government Cloud Plus and the user experience in using Government Cloud Plus. For example, we may use this information to understand and analyze trends or track which of our features are used most often to improve product functionality.

Salesforce may share anonymous usage data with Salesforce's service providers for the purpose of helping Salesforce in such tracking, analysis, and improvements. Additionally, Salesforce may share such anonymous usage on an aggregate basis in the normal course of operating our business, for example, we may share information publicly to show trends about the general use of our services.

Interoperation with Other Services

Government Cloud Plus may interoperate or integrate with other services provided by Salesforce or third parties. Customers are responsible for reviewing and accepting the responsibility of integrating with services that may operate outside of the Government Plus environment. Security, Privacy and Architecture documentation for services provided by Salesforce is available in the Trust and Compliance Documentation. Salesforce also provides a variety of platforms and features that allow Salesforce users to learn about Salesforce products, participate in communities, connect third-party applications, and participate in pilots, testing and assessments, which are outside the scope of this documentation. Salesforce may communicate with users that participate in such platforms and features in a manner consistent with our Privacy Statement. Additionally, Salesforce may communicate with customers and their users for transactional or informational purposes; for instance, through the Adoption Manager program or through system-generated messages, such as Chatter notifications. Salesforce offers customers and users the ability to deactivate or opt out of receiving such messages.