Security, Privacy and Architecture of Sales Cloud, Service Cloud, Community Cloud, Chatter, Lightning Platform (including Force.com)[1], IoT Explorer (including IoT Plus), Site.com, Database.com, Einstein Analytics (including Einstein Discovery), Work.com, Messaging, Financial Services Cloud, Health Cloud, and Salesforce CPQ and Salesforce Billing

Published: May 16, 2019

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.

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, (1) Salesforce Services (the services branded as Sales Cloud, Service Cloud, Community Cloud, Chatter, Lightning Platform (including Force.com), Site.com, and Database.com), (2) the services branded as IoT Explorer (including IoT Plus), Einstein Analytics[2] (formerly branded as Analytics Cloud), Einstein Discovery (provisioned after October 16, 2018), Work.com, Messaging, and (3) the managed packages branded as Salesforce CPQ and Salesforce Billing (together formerly branded as Salesforce Quote-to-Cash) as well as Health Cloud and Financial Services Cloud[3] (collectively, for the purposes of this document only, the "Covered Services"). For purposes of clarification, this documentation also applies to the foregoing services and managed packages when sold as part of the packages branded as Employee Apps or App Cloud.

Reliability and Backup, Disaster Recovery, Return of Customer Data, and Deletion of Customer Data sections of this documentation do not apply to the temporary developer testing environments branded as "Scratch Orgs." The "Playground" demonstration environment related to Einstein Analytics is not part of the Einstein Analytics services provided under a customer's agreement with Salesforce. Customers may choose to use related products and features branded as Sales Cloud Einstein, Salesforce Inbox, High Velocity Sales, Einstein Prediction Builder, Einstein Activity Capture, Einstein Bots, Service Cloud Einstein, and Account Intelligence; use of these services is subject to both this documentation and the "Einstein Platform" documentation. This documentation does not apply to other Salesforce services that may be associated with or integrate with the Covered Services, such as Einstein Discovery Classic, IoT Cloud, LiveMessage, Marketing Cloud, and Quip. The Einstein Analytics Plus and Einstein Prediction services are

[1] This documentation does not apply to Lightning Platform Developer Edition and its associated products and services that are provided for free.

[2] Rights of ALBERT EINSTEIN are used with permission of The Hebrew University of Jerusalem. Represented exclusively by Greenlight.

[3] The services covered as Salesforce Services for Japan CS Gold certification remain Sales Cloud, Service Cloud, Community Cloud, Chatter, Force.com, Site.com, Database.com, Einstein Analytics, Work.com, Industry Cloud and Salesforce Quote-to-Cash(QTC).

subject to the Einstein Analytics, Einstein Discovery, and Einstein Prediction Builder documentation. Documentation for those services is available in the Trust and Compliance Documentation.

The Einstein Discovery service is provided on the infrastructure described in this documentation for all Customers who were first provisioned Einstein Discovery on or after October 16, 2018. For Customers who were first provisioned before October 16, 2018, please refer to the Einstein Discovery Classic documentation.

Architecture and Data Segregation

The Covered Services are 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 customer-specific "Organization IDs" 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 Customer Data is described in the "Infrastructure and Sub-processors" documentation available here.

Certain customers may have the option to subscribe to Covered Services hosted on the infrastructure of a public cloud provider ("Public Cloud Infrastructure"). This infrastructure is described in the "Infrastructure and Sub-processors" documentation. For customers who elect Public Cloud Infrastructure, this will mean the underlying physical infrastructure on which your Customer Data is stored will be with a public cloud provider for what is commonly referred to as Infrastructure as a Service, and the Covered Services will run on top of the public cloud provider. Unless otherwise noted in this documentation, customers who choose Public Cloud Infrastructure will receive the same services, software functionality and operational processes as described 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 their processing activities. 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 describes the sub-processors and certain other entities material to Salesforce's provision of the Covered Services.

Third-Party Functionality

Certain features of the Covered Services use functionality provided by third parties. The Account Intelligence feature in Sales Cloud uses third-party architecture to locate and host content, such as news articles, that is rendered to your users. Although the name or website of an account being queried is transmitted to such third party, your name and your organization's name are not associated. Customers can disable this feature.

When customers use Messaging to transmit or receive mobile messages, such as SMS messages, the content of those messages and related information about those messages are received by (a) aggregators – entities that act as intermediaries in transmitting mobile messages or provisioning mobile numbers, and (b) carriers – entities that provide wireless messaging services to subscribers via wireless or wireline

telecommunication networks. Such aggregators and carriers access, store, and transmit message content and related information to provide these functions. For over-the-top messaging services, such as Facebook Messenger, the content of messages sent or received via such service and related information about such messages are received by entities that enable such over-the-top messaging services.

Audits and Certifications[4]

The following security and privacy-related audits and certifications are applicable to the Covered Services.

- **Binding Corporate Rules (BCR) for Processors**: Customer Data submitted to the services branded as Sales Cloud, Service Cloud, Chatter, Community Cloud, Einstein Analytics, Force.com, Health Cloud, or Financial Services Cloud is within the scope of the Salesforce BCR for Processors (except when hosted on the Public Cloud Infrastructure). The most current version of the Salesforce BCR for Processors is available on Salesforce's website, currently located at http://www.trust.salesforce.com.
- **EU-U.S. and Swiss-U.S. Privacy Shield certification**: Customer Data submitted to the Covered Services is within the scope of an annual certification to the EU-U.S. Privacy Shield Framework and the Swiss-U.S. Privacy Shield Framework as administered by the U.S. Department of Commerce, as further described in our Privacy Shield Notice. The current certification is available at https://www.privacyshield.gov/list by searching under "Salesforce."
- **ISO 27001/27017/27018 certification**: Salesforce operates an information security management system (ISMS) for the Covered Services in accordance with the ISO 27001 international standard and aligned to ISO 27017 and ISO 27018 with the exclusion of Messaging, Identity, Platform Events (including Change Data Capture), and Salesforce Connect. 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.
- **Service Organization Control (SOC) reports**: Salesforce's information security control environment applicable to the Covered Services undergoes an independent evaluation in the form of SOC 1 (SSAE 18 / ISAE 3402), SOC 2 and SOC 3 audits with the exclusion of Messaging, Identity, Platform Events (including Change Data Capture), and Salesforce Connect. 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.
- **TRUSTe certification**: Salesforce's Website Privacy Statement and privacy practices related to the Covered Services are assessed by TRUSTe annually, for compliance with TRUSTe's Certification and Verification Assessment Criterias. For more information on the status of Salesforce's certification/verification status, click here.
- **Payment Card Industry (PCI)**: For the Covered Services, Salesforce has obtained an Attestation of Compliance ("AoC") demonstrating Level 1 compliance with the applicable Payment Card Industry (PCI) Data Security Standard (DSS), with the exclusion of Messaging, Identity, Platform Events (including Change Data Capture), and Salesforce Connect. A copy of Salesforce's AoC is available upon request from your organization's Salesforce account executive. Customers must use either "Platform Encryption" for supported field types and file attachments or the "Classic Encryption" custom fields feature when storing personal account numbers ("PAN" or "credit card numbers") to benefit from Salesforce's PCI DSS AoC. Additionally, to benefit from Salesforce's PCI DSS AoC, customers should not implement the deterministic encryption option when using Platform Encryption. Information about "Platform Encryption" and "Classic Encryption" is available in the

[4] This section does not apply to Salesforce Connect, Identity, and Messaging.

Salesforce Security Guide.

- **HITRUST certification:** For the Covered Services (excluding IoT Explorer (including IoT Plus), Salesforce CPQ and Billing, Messaging, Identity, Platform Events, and Salesforce Connect), Salesforce has obtained HITRUST CSF Certification. A copy of Salesforce's HITRUST letter of certification is available upon request from your organization's Salesforce Account Executive.
- **ASIP Santé certification:** ASIP Santé certification: Salesforce has obtained the French health data hosting certification (ASIP Santé certification) that enables Salesforce to host French health data for the Covered Services with the exclusion of Messaging, Identity, Platform Events (including Change Data Capture), and Salesforce Connect. Salesforce's most recent ASIP Santé certification is available upon request from your organization's Salesforce account executive.

Additionally, the Covered Services undergo security assessments by internal personnel and third parties, which include infrastructure vulnerability assessments and application security assessments, on at least an annual basis.

Security Controls

The Covered Services include a variety of configurable security controls that allow customers to tailor the security of the Covered Services for their own use. Please see additional information on such controls in the Salesforce Security Guide.

Security Policies and Procedures

The Covered Services are operated in accordance with the following policies and procedures to enhance security:

- Customer passwords are stored using a one-way salted hash.
- 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 there is suspicion of 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.
- Data center physical access logs, system infrastructure logs, and application logs will be kept for a minimum of 90 days. Logs will be kept in a secure area to prevent tampering.
- Passwords are not logged.
- Certain administrative changes to the Covered Services (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.
- 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.

Intrusion Detection

Salesforce, or an authorized third party, will monitor the Covered Services for unauthorized intrusions using network-based and/or host-based intrusion detection mechanisms. Salesforce may analyze data collected by users' web browsers (e.g., device type, screen resolution, time zone, operating system version, browser type and version, system fonts, installed browser plug-ins, enabled MIME types, etc.) for

security purposes, including to detect compromised browsers, to prevent fraudulent authentications, and to ensure that the Covered Services function properly.

Security Logs

All systems used in the provision of the Covered Services, including firewalls, routers, network switches and operating systems, log information to their respective system log facility or a centralized syslog server (for network systems) in order to enable security reviews and analysis.

Incident Management

Salesforce maintains security incident management policies and procedures. Salesforce notifies impacted customers without undue delay of any unauthorized disclosure of their respective Customer Data by Salesforce or its agents of which Salesforce becomes aware to the extent permitted by law.

Salesforce publishes system status information on the Salesforce Trust website. Salesforce typically notifies customers of significant system incidents by email, and for 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 Covered Services 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, 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 the Covered Services have access control systems that permit only authorized personnel to have access to secure areas. These facilities are designed to withstand adverse weather and other reasonably predictable natural conditions, utilize redundant electrical and telecommunications systems, employ environmental systems that monitor temperature, humidity and other environmental conditions, and contain strategically placed heat, smoke and fire detection and suppression systems. Facilities are secured by around-the-clock guards, interior and exterior surveillance cameras, two-factor access screening and escort-controlled access. In the event of a power failure, uninterruptible power supply and continuous power supply solutions are used to provide power while transferring systems to on-site back-up generators.

Reliability and Backup[5]

All networking components, network accelerators, load balancers, Web servers and application servers are configured in a redundant configuration. All Customer Data submitted to the Covered Services is stored on a primary database server with multiple active clusters for higher availability. All Customer Data submitted to the Covered Services is stored on highly redundant carrier-class disk storage and multiple data paths to ensure reliability and performance. All Customer Data submitted to the Covered Services, 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, Financial Services Cloud, Salesforce CPQ or Salesforce Billing managed package is uninstalled

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

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[6]

Production data centers are designed to mitigate the risk of single points of failure and provide a resilient environment to support service continuity and performance. The Covered Services utilize secondary facilities that are geographically diverse from their primary data centers, along with required hardware, software, and Internet connectivity, in the event Salesforce production facilities at the primary data centers were to be rendered unavailable.

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 data center to the secondary data center utilizing developed operational and disaster recovery procedures and documentation.

The Covered Services' disaster recovery plans currently have the following target recovery objectives: (a) restoration of the Covered Service (recovery time objective) within 12 hours after Salesforce's declaration of a disaster; and (b) maximum Customer Data loss (recovery point objective) of 4 hours. However, these targets exclude a disaster or multiple disasters causing the compromise of both data centers at the same time, and exclude development and test bed environments, such as the Sandbox service.

Viruses

The Covered Services do not scan for viruses that could be included in attachments or other Customer Data uploaded into the Covered Services by a customer. Uploaded attachments, however, are not executed in the Covered Services and therefore will not damage or compromise the Covered Services by virtue of containing a virus.

Data Encryption

The Covered Services use industry-accepted encryption products to protect Customer Data and communications during transmissions between a customer's network and the Covered Services, including through Transport Layer Encryption (TLS) leveraging at least 2048-bit RSA server certificates and 128 bit symmetric encryption keys at a minimum. Additionally, all data, including Customer Data, is transmitted between data centers for replication purposes across a dedicated, encrypted link utilizing AES-256 encryption.

Return of Customer Data[7]

Within 30 days post contract termination, customers may request return of their respective Customer Data submitted to the Covered Services (to the extent such data has not been deleted by Customer). Salesforce shall provide such Customer Data via a downloadable file 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.

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

[7] This section does not apply to Scratch Orgs. This section also does not apply to any Customer Data that have been encrypted using Platform Encryption Cache-Only Key Service.

Deletion of Customer Data[8]

After termination of all subscriptions associated with an environment, Customer Data submitted to the Covered Services is retained in inactive status within the Covered Services for 120 days, after which it is securely overwritten or deleted from production within 90 days, and from backups within 180 days. Physical media on which Customer Data is stored during the contract term is not removed from the data centers that Salesforce uses to host Customer Data unless the media is at the end of its useful life or being deprovisioned, in which case the media is first sanitized before removal. This process is subject to applicable legal requirements.

Without limiting the ability for customers to request return of their Customer Data submitted to the Covered Services, 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

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 the Covered Services. Customers may not otherwise submit such data to the Covered Services. For other categories of sensitive data, customers should also consider using "Platform Encryption" or "Classic Encryption."

For Salesforce CPQ, Salesforce Billing, Salesforce Connect, and Messaging, the following types of sensitive personal data may not be submitted: information related to an individual's physical or mental health; and information related to the provision or payment of health care. Customers using Public Cloud Infrastructure may not submit to the Covered Services Protected Health Information as defined under the U.S. Health Insurance Portability and Accountability Act.

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 the Covered Services for purposes of security and helping Salesforce improve both the Covered Services and the user experience in using the Covered Services. 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.

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

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 data 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

The Covered Services may interoperate or integrate with other services provided by Salesforce or third parties. 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 contact users to provide transactional information about the Covered Services; 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.