Security, Privacy and Architecture of Sales Cloud, Service Cloud, Experience Cloud (formerly Community Cloud), Chatter, Lightning Platform (including Force.com), Salesforce Private Connect, IoT Explorer (including IoT Plus), Site.com, Database.com, Tableau CRM (including Einstein Discovery and Salesforce Data Pipelines), WDC, Intelligent Form Reader, Messaging, Employee Productivity, Financial Services Cloud, Health Cloud, IT Service Center - IT Agent, Privacy Center, Sustainability Cloud, Consumer Goods Cloud, Manufacturing Cloud, Loyalty Management, Emergency Program Management, Public Sector Solutions, Service Cloud Voice, Salesforce CPQ and Salesforce Billing, Salesforce Maps, Workplace Command Center, Shift Management, Salesforce Order Management, B2B Commerce on Lightning Experience, and the Salesforce.org, LLC ("Salesforce.org") services branded as Salesforce Advisor Link, foundationConnect, Accounting Subledger, Salesforce.org Insights Platform: Data Integrity, Nonprofit Cloud Case Management, Grants Management, Admissions Connect, and Student Success Hub

Published: May 7, 2021

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 the following services and managed packages (collectively, for the purposes of this document only, the "Covered Services"):

(1) Salesforce Services branded as:

- Chatter,
- Database.com,
- Experience Cloud (formerly Community Cloud),
- Lightning Platform (including Force.com)[1],
- Sales Cloud,
- Salesforce Private Connect,

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

- Service Cloud, and
- Site.com, and

(2) the services branded as:

- B2B Commerce on Lightning Experience[2],
- Consumer Goods Cloud,
- Emergency Program Management,
- Intelligent Form Reader,
- IoT Explorer (including IoT Plus),
- Loyalty Management,
- Manufacturing Cloud,
- Messaging,
- Public Sector Solutions[3],
- Service Cloud Voice,
- Tableau CRM[4][5],
- WDC[6], and

(3) the managed packages branded as:

- Employee Productivity,
- Financial Services Cloud,
- Health Cloud,
- IT Service Center - IT Agent,
- Privacy Center,
- Salesforce CPQ and Salesforce Billing (together formerly branded as Salesforce Quote-to-Cash),
- Salesforce Maps,
- Salesforce Order Management[7],
- Shift Management,
- Sustainability Cloud,
- Workplace Command Center, and

(4) the Salesforce.org, LLC ("Salesforce.org") services branded as:

- Accounting Subledger,
- Admissions Connect,
- foundationConnect[8],
- Grants Management,
- Nonprofit Cloud Case Management,

---

[2] This documentation only applies to B2B Commerce On Lightning Experience provisioned on or after July 20, 2020.

[3] Some purchases of Public Sector Solutions may include a license for Emergency Program Management, Vlocity, or both. Emergency Program Management is included in this documentation. Vlocity licenses are subject to the Vlocity Trust and Compliance Documentation.

[4] Tableau CRM refers to Services formerly branded as Einstein Analytics. It includes the Einstein Discovery and Salesforce Data Pipelines features.

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

[6] WDC refers to Services formerly branded as Work.com provisioned before May 1, 2020.

[7] Any reference to Salesforce Order Management in this Documentation describes the Security, Privacy and Architecture of the version of Order Management released on February 19, 2020 ("Salesforce Order Management"). For versions of Order Management released prior to the release of Salesforce Order Management ("B2C Commerce Order Management"), such versions shall continue to be governed by the B2C Commerce Documentation.

[8] This documentation only applies to foundationConnect provisioned on or after August 19, 2019.

- Salesforce Advisor Link,
- Salesforce.org Insights Platform: Data Integrity ("Insights Platform"), and
- Student Success Hub

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. References to "Salesforce" includes salesforce.com, inc. and its Affiliates, including Salesforce.org.

The Covered Services include the Field Service managed package ("FSMP"), which is a feature of Service Cloud.[9] FSMP includes optional scheduling optimization functionality ("Click FS Optimizer"). 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 Covered Services also include Salesforce Connect, which is a feature of Lightning Platform (including force.com). All data presented in Salesforce Connect is retrieved real-time by Salesforce Connect from external data sources and is not copied into the Customer's org, so for clarity, any terms relating to stored Customer Data contained in this documentation do not apply to such data.

Certain products and features run on multiple infrastructures. When using any of these products and features independently or in conjunction with the Covered Services, as applicable, this Documentation and the following Documentation applies:

(1) Einstein Platform Documentation for Account Intelligence, Einstein Activity Capture, Einstein Article Recommendations, Einstein Bots, Einstein Case Classification, Einstein Case Wrap-up, Einstein Conversation Insights, Einstein Object Detection, Einstein Opportunity Scoring, Einstein Prediction Builder[10], Einstein Recommendation Builder, Einstein Referral Scoring, High Velocity Sales, Sales Cloud Einstein, Salesforce Inbox, Service Cloud Einstein;
(2) Customer 360 Audiences Documentation for Customer 360 Audiences;
(3) Salesforce Anywhere (including Quip) Documentation for Salesforce Anywhere (including Quip);
(4) 'LiveMessage, myTrailhead, Salesforce Anywhere (including Quip), Salesforce.org Philanthropy Cloud and Salesforce.org Elevate' Documentation for Microsoft Teams Integration (a feature of Sales Cloud and Service Cloud, as further described here) and Service Cloud Voice.

This documentation does not apply to other Salesforce services that may be associated with or integrate with the Covered Services, including, without limitation, B2C Commerce, IoT Cloud, LiveMessage[11], and Marketing Cloud.

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. For Salesforce Maps, the architecture also provides an effective logical data separation via customer-specific "Tenant IDs." Additional data segregation is ensured by

[9] The term FSMP refers to the feature formerly called the Field Service Lightning managed package.
[10] Einstein Prediction Builder is included in several Tableau CRM SKUs, including Customer Lifecycle Analytics, Tableau CRM for Consumer Goods, Tableau CRM for ERM, Tableau CRM for Financial Services, Tableau CRM for Healthcare, Tableau CRM for Manufacturing Cloud, Tableau CRM Plus, and Einstein Predictions. The Tableau CRM Services run on infrastructure described by this Documentation, and the Einstein Prediction Builder Service runs across infrastructure described in this Documentation and the Einstein Platform Documentation.
[11] For clarity, Messaging and LiveMessage are different services. This documentation does apply to Messaging.

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. For those customers who choose the option of having Covered Services hosted on Salesforce's Government Cloud Plus Service, the Government Cloud Plus documentation will also apply.

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 — Account News, Lightning News, Account Logos, and Account Autofill — work by sending standard fields from Customers' Account object to Salesforce's Einstein Platform infrastructure, currently hosted by AWS, where this data is matched to Content, such as news articles, made available through Sales Cloud. Customers can disable the Account Intelligence features.

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 and WhatsApp, 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

The following security and privacy-related audits and certifications are applicable to one or more of the Covered Services, as described below.

- **APEC Privacy Recognition for Processors (PRP)**: Customer Data submitted to the Covered Services 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/.

- **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 Consumer Goods Cloud, Manufacturing Cloud, Sustainability Cloud, Salesforce Connect, Salesforce Private Connect, Identity, Messaging, Salesforce Maps, FSMP, Click FS Optimizer, Emergency Program Management, Public Sector Solutions, Salesforce Order Management, Salesforce Advisor Link, foundationConnect, Accounting Subledger, Insights Platform, Nonprofit Cloud Case Management, Workplace Command Center, Shift Management, Employee Productivity, IT Service Center - IT Agent, Privacy Center, Service Cloud Voice, Intelligent Form Reader, Loyalty Management, Privacy Center, Admissions Connect, and Student Success Hub. Salesforce's most recent ASIP Santé certification is available upon request from your organization's Salesforce account executive.
- **Cloud Computing Compliance Controls Catalogue (C5) certification:** Salesforce has obtained the German C5 certification for the Covered Services with the exclusion of Consumer Goods Cloud, Sustainability Cloud, Salesforce Connect, Identity, Messaging, Salesforce Maps, FSMP, Click FS Optimizer, Public Sector Solutions, Salesforce Order Management, Salesforce Advisor Link, foundationConnect, Accounting Subledger, Insights Platform, Nonprofit Cloud Case Management, Workplace Command Center, Shift Management, Employee Productivity, IT Service Center - IT Agent, Privacy Center, Service Cloud Voice, Grants Management, Intelligent Form Reader, Loyalty Management, Privacy Center, Admissions Connect, and Student Success Hub. Salesforce's most recent C5 certification is available upon request from your organization's Salesforce Account Executive.
- **EU and UK Binding Corporate Rules (BCR) for Processors**: Customer Data submitted to the Covered Services is within the scope of the Salesforce EU and UK BCR for Processors (except when hosted on the Public Cloud Infrastructure). The most current versions of the Salesforce EU and UK BCR for Processors are available on Salesforce's website, currently located at https://www.salesforce.com/company/privacy/.
- **EU-U.S. and Swiss-U.S. Privacy Shield certification**[12]: 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."
- **HITRUST certification:** Salesforce has obtained HITRUST CSF Certification for the Covered Services with the exclusion of Salesforce CPQ and Billing, Consumer Goods Cloud, Manufacturing Cloud, Sustainability Cloud, Salesforce Connect, Salesforce Private Connect, Identity, Messaging, Salesforce Advisor Link, foundationConnect, Salesforce Maps, FSMP, Click FS Optimizer, Emergency Program Management, Public Sector Solutions, Salesforce Order Management, Accounting Subledger, Insights Platform, Nonprofit Cloud Case Management, Workplace Command Center, Shift Management, Employee Productivity, IT Service Center - IT Agent, Privacy Center, Service Cloud Voice, Grants Management, Intelligent Form Reader, Loyalty Management, Privacy Center, Admissions Connect, and Student Success Hub. A copy of Salesforce's HITRUST letter of certification is available upon request from your organization's Salesforce Account Executive.

[12] Services that are made generally available after July 16, 2020 will no longer be added to Salesforce's Privacy Shield Certification, including: Salesforce Private Connect, Intelligent Form Reader, Privacy Center, Public Sector Solutions, Service Cloud Voice, Grants Management, Admissions Connect, Student Success Hub, Employee Productivity, and IT Service Center - IT Agent.

- **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 Consumer Goods Cloud, Manufacturing Cloud, Sustainability Cloud, Salesforce Connect, Identity, Salesforce Maps, FSMP, Click FS Optimizer, Emergency Program Management, Public Sector Solutions, Salesforce Order Management, Salesforce Advisor Link, foundationConnect, Accounting Subledger, Insights Platform, Nonprofit Cloud Case Management, Workplace Command Center, Shift Management, B2B Commerce on Lightning Experience, Employee Productivity, IT Service Center - IT Agent, Privacy Center, Service Cloud Voice, Intelligent Form Reader, Loyalty Management, Privacy Center and Admissions 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.
- **Japan CS Gold certification:** The services covered by the Japan CS Gold certification are Sales Cloud, Service Cloud, Experience Cloud (formerly Community Cloud), Chatter, Lightning Platform, Site.com, Database.com, Tableau CRM, WDC, Health Cloud and Financial Services Cloud, Salesforce Configure-Price-Quote (CPQ) and Salesforce Billing.
- **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 Consumer Goods Cloud, Sustainability Cloud, Salesforce Connect, Identity, Messaging, Salesforce Maps, FSMP, Click FS Optimizer, Public Sector Solutions, Salesforce Advisor Link, foundationConnect, Accounting Subledger, Insights Platform, Nonprofit Cloud Case Management, Workplace Command Center, Shift Management, Employee Productivity, IT Service Center - IT Agent, Privacy Center, Service Cloud Voice, Grants Management, Intelligent Form Reader, Loyalty Management, Privacy Center, Admissions Connect, and Student Success Hub. 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 Salesforce Security Guide.
- **System and Organization Controls (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 or SOC 3 audits with the exclusion of Consumer Goods Cloud, Sustainability Cloud, Salesforce Connect, Identity, Messaging, FSMP, Click FS Optimizer, Public Sector Solutions, Salesforce Order Management, Accounting Subledger, Insights Platform, Shift Management, Employee Productivity, IT Service Center - IT Agent, Privacy Center, Service Cloud Voice, Intelligent Form Reader, Loyalty Management, Privacy Center and Admissions Connect. Salesforce's most recent SOC 1 (SSAE 18 / ISAE 3402), SOC 2 and SOC 3 reports are available for download on Salesforce's compliance website.
- **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 Criteria. For more information on the status of Salesforce's certification/verification status, click here.
- **Information System Security Management and Assessment Program (ISMAP)**: The covered services are registered in ISMAP, a program that was established to assess and register cloud services that meet security criteria defined by the Japanese government. This audit is undertaken

annually. The services covered by ISMAP are Sales Cloud, Service Cloud, Salesforce Mobile App(iOS/Android), Community Cloud, Chatter, Lightning Platform (including Force.com), Site.com, Database.com, Tableau CRM Analytics (formerly known as Einstein Analytics), Salesforce Surveys, Salesforce Shield, WDC, Health Cloud, Financial Services Cloud, Manufacturing Cloud, Salesforce Configure Price Quote (CPQ) , Salesforce Billing (formerly known as Salesforce Quote to Cash (QTC)), B2B Commerce (formerly known as CloudCraze), Einstein Prediction Builder, Einstein Case Classification (formerly known as Einstein), Grants Management, Salesforce Private Connect, Einstein Next Best Action and customer data region is limited to Japan.

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.

As further described in the "Salesforce Services Infrastructure and Sub-processors" documentation, Salesforce uses infrastructure provided by Amazon Web Services, Inc. ("AWS") to host or process Customer Data submitted to certain Covered Services and features. Information about security and privacy-related audits and certifications received by AWS, including ISO 27001 certification and SOC reports, is available from the AWS Security website and the AWS Compliance website.

Further, as described in the "Salesforce Services Infrastructure and Sub-processors" documentation, Salesforce uses infrastructure provided by Heroku to host or process Customer Data submitted to certain Covered Services and features. Information about security and privacy-related audits and certifications received by Heroku, including ISO 27001 certification and SOC reports, is available from Heroku's Security, Privacy, and Architecture Documentation.

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. Information on Multi-Factor Authentication and Single Sign-On for access to the Covered Services is set forth in the applicable Notices and License Information (NLI).

Certain Covered Services and features use AWS to host or process Customer Data, as further described in the "Salesforce Services Infrastructure and Sub-processors" documentation; further information about security provided by AWS is available from the AWS Security website, including AWS's overview of security processes.

Certain Covered Services and features use the Heroku platform to host or process Customer Data, as further described in the "Salesforce Services Infrastructure and Sub-processors" documentation; further information about security provided by Heroku is available from Heroku's Security, Privacy, and Architecture Documentation.

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 for use 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 with user activity 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 system-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 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, with the exception of Experience Cloud (formerly Community Cloud) guest users, 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[13]

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 Accounting Subledger, Admissions Connect, Financial Services Cloud, foundationConnect, Grants Management, Health Cloud, Insights Platform, Intelligent Form Reader, Nonprofit Cloud Case Management, Salesforce Advisor Link, Salesforce CPQ or Salesforce Billing managed package, Salesforce Maps, Student Success Hub, or Sustainability Cloud or 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[14]

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

[13] This section does not apply to Scratch Orgs. This section also does not apply to the Click FS Optimizer or Shift Management.

[14] This section does not apply to Scratch Orgs. This section also does not apply to the Click FS Optimizer or Shift Management.

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. Additionally, all data, including Customer Data, is transmitted between data centers for replication purposes across encrypted links utilizing AES-256 encryption.

Return of Customer Data[15]

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, 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. The foregoing return of Customer Data for managed packages may not be available if the packages were removed prior to contract termination, as removing the package may begin the deletion process for associated Customer Data.

Deletion of Customer Data[16]

Except as otherwise stated below, 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

For Salesforce Maps, all Customer Data submitted to AWS (with the exception of CSV files uploaded by Customer via the Salesforce Maps Custom Data Source Portal (“Custom Data Sources”) is retained in AWS for 90 days, after which it is securely overwritten or deleted. Custom data Sources submitted to AWS are

[15] 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.
[16] This section does not apply to Scratch Orgs.

converted into data layer files, and the original CSV files are deleted after 90 days. Any Custom Data Sources returned pursuant to the "Return of Customer Data" section will be in the form of a converted data layer file, not the original CSV file.

For Insights Platform, all Customer Data submitted to AWS is retained in AWS for 30 days, after which it is securely overwritten or deleted, and all Customer Data submitted to Heroku is retained in Heroku for the duration of the applicable subscription term, then deleted 30 days after termination of the applicable subscription term, after which it is securely overwritten or deleted.

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 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."

Additionally, for the Covered Services, 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 to restrictions, Salesforce has expressly permitted such submission contractually. Furthermore, any Customer 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.

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

For Intelligent Form Reader, if a Customer chooses to use any part of this Covered Service in connection with a decision-making process with legal or similarly significant effects, Customer shall ensure that the final decision is made by a human being.

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 of 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.

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. When third-party systems connect to the Covered Services, these external systems supply metadata to the Covered Services for the purpose of maintaining the intended functionality of the integration, for example an external system may supply a third-party record ID, file name, folder name, or similar label intended to identify a record that is being sent to the Covered Services. Salesforce may collect and store such metadata to ensure product functionality, and to assist in debugging, support and for security purposes. Salesforce provides appropriate protections for such metadata and treats it consistently with our Privacy Statement. 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.