Cimulate Security, Privacy, and Architecture

Published: April 15, 2026

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 MSA.

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 as Cimulate (referred to, for the purposes of this document only, the "Covered Services").

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 unique identifiers 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.

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 those 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

Salesforce may use third parties to protect the Covered Services from Distributed Denial of Services ("DDoS") attacks. If an attack occurs, a third party may be used to identify and block malicious online

Audits and Certifications

The following security and privacy-related audits and certifications are applicable to the Covered Services, as described below:

- **Data Privacy Framework Certifications:** Customer Data submitted to the Covered Services is within the scope of annual certifications to the EU-US Data Privacy Framework, UK Extension to the EU-US Data Privacy Framework, and Swiss-US Data Privacy Framework as administered by the US Department of Commerce and further described in our Notice of Certification. The current certifications are available at https://www.dataprivacyframework.gov/s/ by searching under "Salesforce."

- **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. 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/legal/privacy/.
- **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.
- **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/.

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

As further described in the "Infrastructure and Sub-processors" documentation, Salesforce uses infrastructure provided by third parties to host Customer Data submitted to certain Services. Specifically, Salesforce uses infrastructure provided by Google, LLC ("Google") to host Customer Data submitted to the Covered Services. Information about security and privacy-related audits and certifications received by Google, including, but not limited to, ISO 27001 certification and SOC reports, is available from the Google Security website, and the Google Compliance website.

Security Controls

The Covered Services include a variety of configurable security controls for the customer's authorized administrators on the Covered Services platform. These controls include but are not limited to the following:

- Various user access management controls.
- Various password complexity controls.
- User access logs for the Customer's instance are available for review and export, where applicable.
- Multi-factor Authentication for customer code uploads.
- Multi-factor Authentication and Single Sign-On for access to the Covered Services.
- IP-level restriction for application level access

The Covered Services offer other configurable security controls that allow Customers to tailor the security of the Covered Services for their own use.

Security Policies and Procedures

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

- User passwords are not transmitted unencrypted.
- User passwords are stored encrypted or as a derived secret key.
- Internal system accounts are reviewed on a regular basis.
- Logs are stored securely.
- Passwords are not logged.

Intrusion Detection
Salesforce, or an authorized third party, will monitor the Covered Services for unauthorized intrusions using network-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 for incident detection and response, to prevent fraudulent authentication of customer accounts, and to ensure that the Covered Services function properly.

Security Logs
All Salesforce 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 log collection server in order to enable security reviews and analysis.

Incident Management
Salesforce maintains a security incident management program. 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.

User Authentication
Access to the Covered Services requires a valid user ID and password combination, which are encrypted via TLS while in transmission. Passwords and secret keys are stored by a third-party service.

Physical Security
For Covered Services using Infrastructure providers, further information about the physical security provided by the Infrastructure Providers is available from the Infrastructure Providers.

Reliability and Backup
The architecture of the Covered Services is designed to be highly redundant and reliable. Customer Data submitted to the Covered Services is stored across geographically spread availability zones.

Viruses
The Covered Services do not scan for viruses that could be included in attachments or other data uploaded to the Covered Services by Customers. Customers are responsible for scanning Customer Data for malicious code prior to inputting the Customer Data.

Data Encryption
Data submitted to the Covered Services is encrypted at rest.

Return of Customer Data
The Covered Services allow import, export or deletion of Customer Data by authorized users, however, requests for import, export or deletion must be made prior to the termination or expiration of a subscription.

Deletion of Customer Data
Following the termination or expiration of a subscription, Salesforce will delete all Customer Data within 150 business days. Notwithstanding the foregoing, certain data relating to the usage and performance of

Customer's website may be retained for analytics purposes after termination ("Analytics Data"). The Analytics Data will not include any personal data.

Sensitive Data

If the Customer submits sensitive or otherwise regulated data to the Covered Service's Cloud offering, the Customer is responsible for ensuring that its use of the Covered Service's Cloud Offering to process that information complies with all applicable laws and regulations associated with that data including review of the Audits and Certifications section to determine if the Cloud Offering has the necessary Audits and/or Certifications to process that sensitive data.

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. 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.

In addition, Salesforce may, for purposes reasonably required to develop, deliver, and provide ongoing innovation to the Covered Services and other Salesforce Services use Customer Data on an aggregate or anonymous basis ("Anonymized Data") and use Customer Data relating to Customer's website (s) ("Website Data"), including data derived from website management, use of the website, and catalogue data. The Anonymized Data may also be used for marketing and benchmarking, as well as for other research and analysis. None of the resulting Anonymized Data, nor any such Website Data will include personally identifiable information. For clarity, in no event does Salesforce share Customer Data with any other customers. By using the Covered Services, customers consent to this use of their Customer Data.

Interoperation with Other Services

The Covered Services may interoperate or integrate with other services provided by Salesforce. The Security, Privacy, and Architecture documentation for such services 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.