SALESFORCE SECURITY, PRIVACY, AND ARCHITECTURE

Last Updated: September 30, 2015

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 data submitted by customers to our services ("Customer Data").

Services Covered

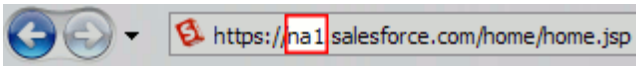
This documentation describes the architecture of, the security and privacy-related audits and certifications received for, and the administrative, technical and physical controls applicable to the services branded as Force.com, Site.com, Database.com, Sales Cloud, Service Cloud, Communities, and Chatter (the "Salesforce Services").

Salesforce Infrastructure

Salesforce owns or controls access to the infrastructure that Salesforce uses to host Customer Data submitted to the Salesforce Services. For information on limited infrastructure functions provided by third parties, see below in "Third-Party Infrastructure."

Each instance of the Salesforce Services (for example, NA1 or CS2) contains many servers and other elements to make it run. Each instance in a primary data center has an exact copy in a secondary data center.

The instance your organization uses is indicated in the browser's address bar, shown highlighted below.



Alternatively, if your organization uses the My Domain feature, you may use the lookup form at https://trust.salesforce.com/trust/domainLookupLaunch/ to find the corresponding instance.

The following instances are currently located in data centers in the following geographies:

Instance Type	Primary Data Center Location	Secondary Data Center
APAC (e.g. AP0)	Japan	United States

EMEA (EU0*, EU2**, EU3**)	United States	United States
EMEA (EU1, EU4)	United Kingdom	Germany
EMEA (EU5)	United Kingdom	United States
EMEA (EU6) Live after Oct. 19, 2015	Germany	United Kingdom
North America (e.g. NA2)	United States	United States
Sandbox (CS5, CS6, CS31)	Japan	United States
Sandbox (CS80, CS81)	United Kingdom	United States
Sandbox (CS82, CS83) Live after Oct. 15, 2015	Germany	United Kingdom
Sandbox (CS86, CS87)	United Kingdom	Germany
Sandbox (all other CS instance types)	United States	United States

* EU0 will migrate to a United Kingdom primary data center and Germany secondary data center on November 21, 2015.
** EU2 and EU3 will migrate to a United Kingdom primary data center and Germany secondary data center on October 3, 2015.

Third-Party Architecture

The Site.com Published Site product uses a third-party optimization service to improve performance and reliability. Customer Data processed by the Site.com Published product may be accessed by providers of optimization services necessary for the operation of the Site.com Published Site product.

Audits and Certifications

The following security and privacy-related audits and certifications are applicable to the Salesforce Services:

- **EU/US and Swiss/US Safe Harbor self-certifications**: Customer Data submitted to the Salesforce Services is within the scope of an annual self-certification to the EU/US and Swiss/US Safe Harbor frameworks as administered by the U.S. Department of Commerce. The current self-certification is available at https://safeharbor.export.gov/list.aspx by searching for "salesforce.com."
- **ISO 27001 certification:** Salesforce is subject to an information security management system (ISMS) in accordance with the ISO 27001 international standard. Salesforce has achieved ISO 27001 certification for its ISMS from an independent third party. The Salesforce ISO 27001 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 Salesforce Services undergoes an independent evaluation in the form of SOC 1 (SSAE 16 / ISAE 3402), SOC 2 and SOC 3 reports. Salesforce's most recent SOC 1 (SSAE 16 / ISAE 3402) and SOC 2 reports are available upon request from your organization's Salesforce account executive.
- **TRUSTe Privacy Seal:** Salesforce has been awarded the TRUSTe Privacy Seal signifying that Salesforce's Web Site Privacy Statement and associated practices related to the Salesforce Services have been reviewed by TRUSTe for compliance with TRUSTe's program requirements, including transparency, accountability, and choice regarding the collection and use of personal data.
- **PCI:** For the Salesforce Services, Salesforce has obtained a signed Attestation of Compliance ("AoC") demonstrating Level 1 compliance with the applicable Payment Card Industry Data Security Standard, as formulated by The Payment Card Industry Security Standards Council ("PCI DSS") as a data storage entity or third party agent from an Qualified Security Assessor that is certified as such by The Payment Card Industry Security Standards Council. A copy of Salesforce's AoC is available upon request from your organization's Salesforce account executive. Customers must use the Salesforce Services' Classic Encrypted Custom Fields feature when storing personal account numbers ("PAN" or "credit card numbers") to benefit from Salesforce's PCI DSS AoC. Information about encrypted custom fields is available in Help & Training here or the Security Implementation Guide.

Additionally, the Salesforce 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 Salesforce Services include a variety of configurable security controls that allow customers to tailor the security of the Salesforce Services for their own use. These controls are set forth in the Security Implementation Guide.

Security Procedures, Policies and Logging

The Salesforce Services are operated in accordance with the following procedures to enhance security:

- User 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 to assist in forensic analysis. This service will be provided to customers on a time and materials basis.
- 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 under any circumstances.

- Certain administrative changes to the Salesforce 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 Salesforce 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 to detect compromised browsers, to prevent fraudulent authentications, and to ensure that the Salesforce Services function properly.

Security Logs

All Salesforce systems used in the provision of the Salesforce 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 promptly notifies impacted customers of any actual or reasonably suspected 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 Salesforce Services requires authentication via one of the supported mechanisms as described in the Security Implementation Guide, including user ID/password, SAML based Federation, 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 Salesforce Services 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, including biometrics, and escort-controlled access, and are also supported by on-site back-up generators in the event of a power failure.

Reliability and Backup

All networking components, SSL accelerators, load balancers, Web servers and application servers are configured in a redundant configuration. All Customer Data submitted to the Salesforce Services is stored on a primary database server with multiple active clusters for higher availability. All Customer Data submitted to the Salesforce Services is stored on carrier-class disk storage using redundant devices and multiple data paths to ensure reliability and performance. All Customer Data submitted to the Salesforce Services, up to the last committed transaction, is automatically replicated on a near real-time basis to the secondary site and is backed up on a regular basis and stored on backup media for an additional 90 days in production environments and 30 days in Sandbox environments after which it is securely overwritten or deleted from the Salesforce Services. Any backups are verified for integrity and stored in Salesforce data centers.

Disaster Recovery

Salesforce has disaster recovery plans in place and tests them at least once per year. The Salesforce Services utilize secondary facilities that are geographically remote 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.

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

Viruses

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

Data Encryption

The Salesforce Services use industry-accepted encryption products to protect Customer Data and communications

during transmissions between a customer's network and the Salesforce Services, including 128-bit TLS Certificates and 2048-bit RSA public keys at a minimum. Additionally, Customer Data is encrypted during transmission between data centers for replication purposes.

Return of Customer Data

Within 30 days post contract termination, customers may request return of their respective Customer Data submitted to the Salesforce Services. Salesforce shall provide such Customer Data via a downloadable file in comma separated value (.csv) format and attachments in their native format.

Deletion of Customer Data

After contract termination, Customer Data submitted to the Salesforce Services is retained in inactive status within the Salesforce Services for 180 days and a transition period of up to 30 days, after which it is securely overwritten or deleted. In accordance with the Reliability and Backup section above, Customer Data submitted to the Salesforce Services (including Customer Data retained in inactive status) will be stored on backup media for an additional 90 days in production environments and 30 days in Sandbox environments after it is securely overwritten or deleted from the Salesforce Services. 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 Salesforce 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.

Tracking and Analytics

Salesforce may track and analyze use of the Salesforce Services for purposes of security and helping Salesforce improve both the Salesforce Services and the user experience in using the Salesforce Services. Salesforce may also use this information and users' e-mail addresses to contact customers or their users to provide transactional information about the Salesforce Services. Salesforce will offer customers and users the ability to opt out of receiving such emails. These communications may be sent using services provided by ExactTarget, Inc., an affiliate of salesforce.com, inc.

Without limiting the foregoing, Salesforce may share anonymous data about Salesforce's customers' or their users' use of the Salesforce Services ("Usage Statistics") to Salesforce's service providers for the purpose of helping Salesforce in such tracking or analysis, including improving its users' experience with the Salesforce Services, or as required by law. Additionally, Salesforce may share such anonymous data with other customers on an aggregate basis. Except when required by law, any such sharing of Usage Statistics will not include any identifying information about Salesforce's customers or

customers' users.

Interoperation with Other Salesforce Services

The Salesforce Services may interoperate with other services provided by Salesforce. The Security, Privacy and Architecture documentation for such services is available in the Trust and Compliance Documentation section of help.salesforce.com.