SOCIAL.COM SECURITY, PRIVACY, AND ARCHITECTURE

Last Updated: February 28, 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 Social.com, under the Salesforce Marketing Cloud brand (“Social.com Services”).

Salesforce Infrastructure

Salesforce owns or controls access to the infrastructure that Salesforce uses to host Customer Data submitted to the Social.com Services except for the functions described under “Third-Party Infrastructure” below. Currently, this infrastructure is located in the United States.

Third-Party Infrastructure

In addition to the Salesforce infrastructure, Salesforce uses a third-party, SoftLayer Technologies, Inc. (“SoftLayer”), to host Customer Data submitted to the Social.com Services. Currently, the infrastructure hosted by SoftLayer in the provisioning of the Social.com Services is located in the United States.

Audits and Certifications

The Social.com 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.

Information about SoftLayer’s Service Organization Control (SOC) reports is available from the SoftLayer Compliance Web site.

The Social.com Services store Customer Data outside the European Economic Area (including in the United States) and are not included within the scope of Salesforce’s self-certification to the EU/US and/or Swiss/US Safe Harbor.
frameworks. To the extent personal data of European Economic Area or Swiss individuals is submitted to the Social.com Services as Customer Data, Customer is solely responsible for legalizing the transfer of such information to the Social.com Services.

**Security Controls**

The Social.com Services include a variety of configurable security controls. These controls include:

- Unique user identifiers (user IDs) to ensure that activities can be attributed to the responsible individual.
- Controls to revoke access after several consecutive failed login attempts.
- Controls on the number of invalid login requests before locking out a user.
- Controls to ensure initial passwords must be reset on first use.
- Controls to terminate a user session after a period of inactivity.
- Password history controls to limit password reuse.
- Password length controls.
- Password complexity requirements (requires letters and numbers).
- The ability to accept logins to the Social.com Services from only certain IP address ranges.

**Security Procedures, Policies and Logging**

The Social.com Services are operated in accordance with the following procedures to enhance security:

- User passwords are stored using a salted hash format and are never transmitted unencrypted.
- 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 to the Social.com Services, 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.
- Logging will be kept for a minimum of 90 days.
- Logging will be kept in a secure area to prevent tampering.
- Passwords are not logged under any circumstances.
- Salesforce personnel will not set a defined password for a user. Users are provided unique links via email. Upon clicking such links, a user must create a password in accordance with password length and complexity requirements.

**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 to the extent permitted by law.

**User Authentication**

Access to the Social.com Services requires a valid user ID and password combination, which are encrypted via TLS while in transmission. Following a 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 Social.com Services have systems that control access to the data center. This system permits only authorized personnel to have access to the data centers. The facilities are designed to withstand adverse weather and other reasonably predictable natural conditions, are secured by around-the-clock guards, physical access screening and escort-controlled access, and are also supported by on-site back-up generators in the event of a power failure.

**Reliability and Backup**

Customer Data submitted to the Social.com Services is stored on a primary database server with a backup database server for redundancy. All Customer Data submitted to the Social.com Services, up to the last committed transaction, is automatically replicated on a near real-time basis at the database layer and is backed up on a regular basis.

**Disaster Recovery**

The Social.com Services’ production systems are protected by disaster recovery plans which provide for backup of critical data and services. A comprehensive system of recovery processes exists to bring business-critical systems back online within the briefest possible period of time. Recovery processes for database security, systems administration, and network configuration and data provide a roadmap for personnel to make processes available after an outage.

**Viruses**

The Social.com Services do not scan for viruses that could be included in attachments or other data uploaded into the Social.com Services by customers. Uploaded attachments are not executable in the Social.com Services and therefore will not damage or compromise the online Social.com Services by virtue of containing a virus. Additionally, the Social.com Services may pull in information from the Internet and links to other Web sites that may contain malicious content. However, such Web sites are not executable in the Social.com Services.
Data Encryption
The Social.com Services use industry accepted encryption products to protect Customer Data and communications during transmissions between a customer’s network and the Social.com Services, including 128-bit TLS Certificates and 2048-bit RSA public keys at a minimum.

Return of Customer Data
Within 30 days post contract termination, to request return of Customer Data submitted to the Social.com Services, contact marketingcloudsupport@salesforce.com.

Deletion of Customer Data
After contract termination, to request deletion of Customer Data submitted to the Social.com Services, contact marketingcloudsupport@salesforce.com. Back-up data will be deleted within 3 months of deletion of Customer Data. This process is subject to applicable legal requirements.

Sensitive Personal Data
Important: The following types of sensitive personal data may not be submitted to the Social.com Services: government-issued identification numbers; financial information (such as credit or debit card numbers, any related security codes or passwords, and bank account numbers); information related to an individual’s physical or mental health; and information related to the provision or payment of health care.

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 the Marketing Cloud Web Site Privacy Statement.

Tracking and Analytics
Salesforce may track and analyze use of the Social.com Services for the purpose of helping Salesforce improve both the Social.com Services and the user experience in using the Social.com Services. Without limiting the foregoing, Salesforce may share anonymous data about Salesforce’s customers’ or their users’ use of the Social.com 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 Social.com Services, or as required by law. Except when required by law, any such sharing of Usage Statistics to Salesforce’s service providers will not include any identifying information about Salesforce’s customers or customers' users.
Additionally, Salesforce uses Customer Data consisting of data and metrics derived from customer’s social accounts with third party social platforms, such as geographic location, time of day of use, greatest period of use by industry, and other metrics including spend rates or click rates by geographic location and by industry to create an aggregated and anonymized data set ("Anonymized Data"). No Customer Data consisting of personally identifiable information is used to create the Anonymized Data, nor any data that would identify customers, their users, customers’ clients, or any individual, company or organization. Salesforce combines the Anonymized Data with that of other customers to create marketing reports and to provide product features. By using the Social.com Services, customers consent to the use and disclosure of their Customer Data to create reports from the Anonymized Data. A sample of an Anonymized Data report can be found at: https://www.salesforcemarketingcloud.com/wp-content/uploads/2013/06/The-Facebook-Ads-Benchmark-Report.pdf

**Interoperation with Other Salesforce Services**

The Social.com 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.