salesforce

Data Protection and SECURITY

Managing Salesforce Environments for Government and Government Contractors

TABLE OF CONTENTS

DISCLAIMER

The information provided in this white paper is strictly for the convenience of our customers and is for general informational purposes only. Publication by Salesforce does not constitute an endorsement. Salesforce does not warrant the accuracy or completeness of any information, text, graphics, links, or other items contained within this white paper. Salesforce does not guarantee you will achieve any specific results if you follow any advice in the white paper. It may be advisable for you to consult with a professional such as a lawyer, accountant, architect, business advisor, or professional engineer to get specific advice that applies to your specific situation. The implementations, procedures, and policies of Salesforce, FedRAMP, NIST, and the DoD Cloud Computing SRG are subject to change and may impact the analysis reflected in this document. This document is subject to the Salesforce Safe Harbor Statement.

Why data security is more important than ever

With the increasing number and sophistication of cyber attacks around the world, governments, agencies, and departments are taking new measures to protect and safeguard the systems and data they rely on. New regulations, contracting terms, and requirements have been introduced to protect sensitive data and reduce the vulnerability of IT systems.

To comply with these emerging requirements, your organization and the cloud services you depend on may need to implement appropriate measures to attempt to reduce the likelihood and consequences of loss, misuse, modification, or unauthorized access to information.

Many of these provisions may be derived from the security controls in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 Protecting Controlled Unclassified Information in Non-federal Information Systems and Organizations.

An ever-growing number of Federal, Department of Defense (DoD), and Aerospace & Defense customers entrust their missions and business to Salesforce enterprise applications. This document provides those responsible for protecting and safeguarding critical customer data with an overview of how the Salesforce Government Cloud service offerings may assist in meeting data security and protection requirements.

A comprehensive cloud offering

Salesforce is a Cloud Service Provider (CSP) that provides both Software as a Service (SaaS) and Platform as a Service (PaaS) offerings for customers to develop and deploy applications and associated data. The Salesforce Government Cloud is part of our multi-tenant public cloud infrastructure and is specifically for use by U.S. federal, state, and local government customers, U.S. government contractors, and Federally Funded Research and Development Centers (FFRDCs).

The Salesforce Government Cloud information system and authorization boundary includes:

- Force.com platform
- Analytics cloud
- Salesforce services (Sales Cloud, Service Cloud, Chatter, and Work.com, as well as features of these applications including Content, Ideas, Knowledge, Chatter messenger, Chatter files, customer-facing Chatter groups, Chatter answers, Salesforce platform encryption, and event monitoring)
- Salesforce industry applications (Health Cloud and Financial Services Cloud)
- Backend infrastructure (servers, network devices, databases, storage arrays) that support the operations of these products, referred to as the General Support System (GSS)

Powerful authorizations

In May 2016, as Salesforce's FedRAMP authorizing agency, the Department of Health and Human Services (HHS) approved the Salesforce Government Cloud authorization package based on annual attestation requirements and adherence to updated FedRAMP Moderate requirements based on NIST SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*[1], as well as continued efforts to maintain compliance since the initial FedRAMP ATO at the moderate impact level granted by HHS in May 2014.

To obtain the initial ATO from HHS, Salesforce conducted security assessment and authorization activities in accordance with FedRAMP guidance against the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations,* moderate baseline control set consistent with requirements set forth in the Federal Information Security Management Act (FISMA) of 2002[2], NIST SP 800-37 Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*[3]*,* and HHS guidance.

This approach also allowed Salesforce to receive a FISMA ATO at the moderate impact level from the U.S. General Services Administration (GSA) for the Force.com platform, Customer Relationship Management (CRM) applications, Chatter, and the supporting Salesforce infrastructure on May 26, 2011.

Hosting PII and PHI

With a FedRAMP ATO at the moderate baseline, Salesforce can store customer data up to the moderate impact level; your organization should ensure that data stored in Salesforce does not exceed that level. When determining the types of data to be hosted, privacy information including Personally Identifiable Information (PII) should generally fall into the moderate range per NIST SP 800-60 Revision 1 Volume 1, *Guide for Mapping Types of Information and Information Systems to Security Categories.*[4]

When hosting Protected Health Information (PHI) as a covered entity or business associate using Salesforce services, your organization is responsible for complying with the Health Insurance Portability and Accountability Act (HIPAA) of 1996's Privacy Rule and Security[5] and the Health Information Technology for Economic and Clinical Health (HITECH) Act[6]. Salesforce features allow you to customize use per a compliance program for HIPAA (including the HITECH Act), and many customers store PHI on our platform.

Protections and security awareness training

Your organization can also place a variety of protections on electronic data and information submitted to Salesforce and for access within their instance, such as user profiles, sharing settings/rules, role based access controls, and platform encrypted fields (128-bit keys and Advanced Encryption Standard (AES) Federal Information Processing Standards (FIPS) 140-2 validated encryption).

To protect customer data in the Salesforce Government Cloud, we've implemented comprehensive security awareness training for support staff. Before access is granted, all people requesting logical or physical access to systems that process, store, or transmit customer data must complete annual security awareness training. This is provided through an online learning management system, must be done annually, and includes topics such as:

- What information security is and why it's needed
- Protections against virus and malicious code intrusion
- Physical access restrictions, common security threats, and confidentiality
- Resources for information security including policy documentation, an awareness program, and security contacts

Get more details in the Salesforce Government Cloud white paper.

Managing Salesforce environments securely

We offer a wide variety of services and configuration options to help your organization securely access your Salesforce applications, data, and logic. These security features are designed to protect data and logic from unauthorized access, both external and internal. The Salesforce platform is built around a robust and flexible security architecture that provides you with a high degree of control over users, network, and data, including IP restrictions, two-factor authentication, SMS identity confirmation, and session timeout thresholds.

U.S. government operations and contract support customers may be required to implement procedures to properly handle data access, data spillage, data preservation, incident reporting, and facility access. The Salesforce Government Cloud offers a number of capabilities that may help you meet these requirements.

Provisional authorization for DoD IL2 and IL4

For many Salesforce customers, the DoD Cloud Computing Security Requirements Guide (SRG) is an important security and compliance benchmark. The Salesforce Government Cloud has been granted a provisional authorization for Impact Level 2 (IL2) based on our FedRAMP Moderate ATO[7] and Impact Level 4 (IL4) based on a review by the DISA Security Control Assessors (SCA) and provisional authorization (PA) by the DISA Authorizing Official (AO).

Data maintained in the U.S.

Customer data in the Salesforce Government Cloud is stored in two U.S. data center locations. The Salesforce service is collocated in dedicated spaces at top-tier data centers, and our infrastructure is located inside secure server rooms designated to Salesforce.

Precautions for data access, use, and disclosure

We're dedicated to helping our customers be more secure when accessing our service. With the evolving threat landscape, we encourage you to take action to help prevent unauthorized access to your Salesforce environment. We recommend that Salesforce administrators consider taking steps to make the experience as secure as possible for Salesforce users and data. To learn more about the additional layers of end-user validation and authentication we provide, see Stay Current on Security.

Salesforce also allows your organization to manage roles and relationships within our applications with an easy-to-read page showing roles hierarchy. All users and application-level security are defined and maintained by your administrator, not by Salesforce. Your organization's sharing model sets users' default access to data; a combination of roles, privileges, field-level security, and sharing rules provide a broad set of capabilities to meet your data access, use, and disclosure requirements.

To review and recommend improvements to your Salesforce security settings, we provide the Security Health Check tool. For more details about Salesforce security and configurations, please see Salesforce Data Security and Security Best Practices.

As defined in the Salesforce Master Subscription Agreement (MSA), your organization provides a license for us to use your customers' data to provide Salesforce services, and we contractually agree to keep that data confidential. Your Salesforce representative can answer any questions you have.

Access to the production environment infrastructure is restricted to a limited number of full-time Salesforce employees needed to manage the service. These employees do not have login access to your organization, and with Salesforce's multi-tenant infrastructure, they don't have access to assembled customer data, either.

Cyber incident reporting

Users of online services are potential targets for those attempting to steal login credentials and other sensitive information. These threats may include scam emails (phishing and malware) and phone calls to gather information that could be used to gain unauthorized access or privileged knowledge. If your Salesforce environment experiences a suspected or known cyber incident, your organization is responsible for taking the necessary steps per your reporting procedures, and we encourage you to immediately contact our security team at Salesforce Security Contact Help.

Salesforce maintains security incident response management policies and procedures, and we can discuss our notification procedures with you at your request. We created our security incident response plan and process in accordance with FedRAMP moderate control requirements, which include those derived from NIST SP 800-53, NIST SP 800-61, and the FedRAMP Incident Communications Procedure.

Tools to fight malicious software

The Salesforce Security Source Scanner is a cloud-based source code analysis tool built directly into our platform. We've partnered with Checkmarx to provide free use of the Checkmarx Static Analysis Suite (CxSAST), a valuable addition that can help you build trusted applications. We highly recommend that any Force.com code introduced into your Salesforce environment be source code scanned, security reviewed, and pre-tested in a Salesforce sandbox.

All applications enrolled in the ISVForce or Force.com Embedded partner programs must go through a mandatory periodic security review. This review assesses the security of partner offerings, ensures that applications published on the AppExchange follow industry best practices for security, and promotes trust. Get more details at ISV Security Review Process.

Customer security is the foundation of customer success, so Salesforce continues to implement practices and technologies to detect and prevent phishing and malware. Recent and ongoing actions include:

- Actively monitoring and analyzing logs to proactively alert customers who have been affected by malware
- Collaborating with security vendors and experts on specific threats
- Executing strategies to remove or disable fraudulent sites
- Reinforcing security education and tightening access policies within Salesforce

Get more details at Detecting Malware.

Keep in mind that your organization is ultimately responsible for any code, software, packages, or components that you install into your Salesforce environment and for responding to any malicious software therein, according to your procedures and policies.

If malicious software is detected in systems supporting the Salesforce Government Cloud services, Salesforce will implement its incident response and handling process. Please note that we do not preserve, protect, or share images of any malicious software found.

Preserve, protect, access, and assess data

Salesforce operates a multi-tenant cloud architecture that leverages common, shared IT resources to deliver scalable, cost-efficient, secure cloud services (PaaS and SaaS). Because IT components are shared, individual customers can't preserve the state or contents of individual IT components, media, or equipment. When Salesforce is notified of or detects an incident related to the broader Salesforce Government Cloud environment, we will initiate our incident response and handling process.

As a customer, you can monitor, preserve, and manage your Salesforce environment through a comprehensive set of tools.

Preserving your Salesforce environment

Salesforce provides a multi-layered approach to preserving your Salesforce environment:

Full-copy sandbox: This is a replica of your production organization, including all data (such as object records and attachments) and metadata. Sandboxes are isolated from production, so operations performed in your sandboxes don't affect production, and vice versa. You can preserve your entire production organization by making a full copy into a Salesforce production sandbox, which copies all its data, including standard and custom object records, documents, and attachments.

Keep in mind that Salesforce offers a variety of Sandbox options; evaluating the features of each can help you determine the best fit for your specific operational requirements. Get more details at Lifecycle Mgmt with Sandboxes and Creating a Sandbox.

"Off-platform" copy: You may also want to consider another step that preserves the data and metadata within your Salesforce environment locally to an "off platform", non-Salesforce storage device. You can use data replication APIs to perform a full, partial, or incremental export of your Salesforce environment.

Please note that exports result in a flat file structure (such as .csv) that excludes chatter and event logs and that will have no relational context. Get more details at Backup and Restore and Exporting Salesforce Data.

Detailed event monitoring

Event monitoring is a Salesforce add-on feature that provides granular detail of user events within your Salesforce environment. You can view information about individual events or track event trends to quickly identify abnormal behavior and safeguard data. Salesforce tracks more than 30 different type of events, including:

- Logins
- Logouts
- URI (web clicks)
- UITracking (mobile clicks)
- Visualforce page loads
- API calls
- Apex executions
- Report exports

Events are stored in event log files, which are generated when an event occurs in a Salesforce environment and are available to view and download after 24 hours. Salesforce event monitoring provides read-only, forensically-sound logs that capture every record viewed by a user, every document shared, and more, according to available log event types.

The event types you can access and how long files remain available depend on your edition. Event log data can be integrated with a back-end storage and data mart, so you can correlate data from multiple organizations and across disparate systems. Get more details at Event Monitoring or Event Monitoring/ Trailhead.

We also offer fee-based services to assist in researching and providing system event logs associated with your Salesforce environment; just ask your Salesforce representative for more details about these services.

Auditing and compliance

Field Audit Trail is an add-on feature that lets you define a policy to retain and archive select field history data for up to ten years. This can help you comply with industry regulations for audits and data retention. You can use Salesforce metadata API to define a retention policy for field history, then use REST API, SOAP API, and Tooling API to work with the archived data. Get more details at Field Retention and Audit.

Records management and facility access

Salesforce has privacy and security assessments and certifications performed by multiple third parties, including ISO 27001, SSAE 16 SOC 1, SOC 2, SOC 3, FedRAMP, and PCI-DSS. And we can provide contractual assurance to you that the customer data hosted in Salesforce services will be kept confidential. Get more details about our architecture, security, and privacy at Salesforce Trust and Compliance Documentation.

If an additional right to audit is required, we can negotiate and arrange annual site visits at your organization’s expense.

Tools and techniques to address data spillage

Data spillage refers to situations where sensitive, unauthorized data is inadvertently placed in information systems that aren't authorized to process it. This can occur when data that is initially thought to be of lower sensitivity is transmitted to an information system, then subsequently determined to be of higher sensitivity. At that point, corrective action is required. How an organization responds is generally based on several factors: the degree of sensitivity of the spilled information, the security capabilities of the information system, the specific nature of the storage media, and the people with authorized access to the information system.

If there is data spillage within your Salesforce environment, you have a number of tools and techniques available to restrict access, delete, or destroy the data in question:

1. Restrict access to spilled data
Salesforce provides a comprehensive set of administrative controls that allow you to restrict access to objects, fields, and records within your Salesforce environment. Get more details at Restricting Data Access.

2. Delete spilled data
Your Salesforce administrators can perform a selective or mass deletion of data by using the Salesforce Data Loader. Get more details at Deleting Records with Salesforce Data Loader.

3. Destroy spilled data through encryption
Salesforce Shield Platform Encryption is an add-on feature that provides FIPS 140-2 validated encryption for sensitive data at rest (for the Salesforce Government Cloud only). Data stored in many standard and custom fields, as well as in files and attachments, can be encrypted using an advanced HSM-based key derivation system. Also, you can render encrypted fields permanently unreadable by changing or destroying your encryption key.

If additional measures are required, you can file a service ticket with Salesforce to perform a physical deletion of data in your Salesforce environment. We operate a multi-tenant cloud architecture that leverages common, shared IT resources to deliver scalable, cost-efficient, secure cloud services (PaaS and SaaS). Since individual IT components are shared, Salesforce does not provide your organization with the ability to destroy or sanitize media or equipment associated with your Salesforce environment.

Please note that your organization is responsible for evaluating and applying these tools and techniques to meet your policy, procedures, operational, or contractual requirements.

Customer responsibilities

Keep in mind that you and any authorizing authority in your organization are responsible for using the information in this white paper, along with the Salesforce Government Cloud FedRAMP Moderate ATO package and supporting documentation, to assess the risk and compliance of Salesforce services.

Federal government agencies can request access to the Salesforce FedRAMP Agency ATO package by submitting a request to the FedRAMP Program Management Office (PMO)[8]. All other customers can submit a request to Salesforce via their account representative. Customers requesting documentation from Salesforce must have a signed non-disclosure agreement (NDA) in place with Salesforce. Each customer will need to review the documentation and assess that organization's compliance requirements. Customers may need to purchase additional Salesforce and/or third party products and services in order to meet their individual requirements.

Questions? We’re ready to help.

For more details on security for the Salesforce Government Cloud or about our product offerings, please visit Salesforce Government Overview, email **publicsector@salesforce.com,** or contact your Salesforce account representative.

Resources

[1] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NISTSP.800-53r4.pdf

[2] http://csrc.nist.gov/drivers/documents/FISMA-final.pdf

[3] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r1.pdf

[4] http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-60v1r1.pdf

[5] https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/

[6] http://www.gpo.gov/fdsys/pkg/PLAW-111pubI5/htm

[7] http://www.disa.mil/NewsandEvents/2015/CommercialCloud-Service

[8] https://www.fedramp.gov/

salesforce