Well-Architected Security Policy Template

Note that all italicized items in the sections below are examples. Remove or modify them and add your own as needed. Add or modify sections as needed and remove any sections that are not relevant to your organization.

Overview and Scope

This document contains security policies to be followed for Salesforce Projects delivered by [Organization]. It specifically covers Salesforce Security related topics. It does not cover [list any exclusions here (example: non-Salesforce systems)]. [Add any additional organization-specific overview text here].

Organizational Security

This section contains information about the policies you should set for overall organizational security, including passwords, domains and IP ranges and login hours. Refer to Secure - Organizational Security for more information.

Password Policies

This section contains information about the password policies you should set within Salesforce to secure manual logins. Note that these policies should be consistent across your organization and should also match the policies that are in use within any third party Identity Provider / Single Sign-On systems. Refer to Secure- Authentication for more information.

Policy	Description	Setting
Password Expiration Period	How often do users need to reset their password?	*90 Days*
Passwords Remembered	How many passwords should the system remember to prevent users from recycling their old passwords?	*8*
Minimum Password Length	How long should passwords be?	*12*
Password Complexity	Combination of alphanumeric, special, upper case and lower case characters	*Must Include Numbers, Upper Case and Lower Case Letters and Special Characters*
Maximum Invalid Login Attempts	How many login attempts before user is locked out?	*10*
Lockout Period	How long will a user be locked out after the maximum number of password attempts is reached?	*15 Minutes*
Require minimum 1 day password lifetime	Prevent users from changing passwords too frequently	☐

Approved Domains and IP Ranges

This section contains a list of approved domains and IP ranges along with their associated descriptions and justification for approval. Refer to Secure - Organizational Security for more information.

Domain Name	Inbound / Outbound	Description
.stripe.com	*Outbound*	*Payment Gateway - Approved for [reason]*
[Insert your own]		

Login Hours

This section contains a list of days and hours when users are authorized to log into your system. Note that login hours may not be applicable for all organizations (such as those offering 24/7 customer support). Refer to Secure - Organizational Security for more information.

Day	Hours
Sunday	*No Access*
Monday	*7am-8pm*
Tuesday	*7am-8pm*
Wednesday	*7am-8pm*
Thursday	*7am-8pm*
Friday	*7am-8pm*
Saturday	*No Access*

Device Policies

This section contains a list of device policies that are applicable to your organization. Refer to Secure - Device Accesss for additional information.

Policy Name	Description
Supported Operating System	*Android [version] or later OR iOS [version] or later*
Device Passwords	*Must comply with organizational password policies*
Device Jailbreaking	*Prohibited*
[Insert your own]	

Auditing

This section contains details about audit levels and frequency for every object in your data model. Refer to Secure - Threat Detection and Response for additional information.

Risk	Audit Frequency and Details
Unauthorized user access to the org	*Review all org access quarterly*
Sensitive account data becoming compromized	*Review access to account fields classified as sensitive on a quarterly basis*
[Insert your own]	

Authentication

This section contains a list of approved authentication methods for both human and non-human users. Refer to Secure-Authentication for more information.

Persona Access

This section contains a list of personas that can access your system along with their approved authentication methods. Refer to Secure- Authentication for more information.

Persona Name	Type	Internal / External	Description	Authentication Method(s)
Sales Users	*Human*	*Internal*	*Field and Internal Sales Team Members*	*Login via SSO + MFA*
Administrators	*Human*	*Internal*	*System Administrators*	*Direct Login + MFA*
Commerce Cloud Integration User	*Non-Human*	*Internal*	*Login for Commerce Cloud Integration*	*Web Server OAuth Flow*
Payment Gateway Integration User	*Non-Human*	*External*	*Login for external payment gateway*	*Web Server OAuth Flow*
Website User	*Human*	*External*	*Customers logging into the website*	*Direct Login + MFA*
[Insert your own]				

Connected Apps

This section contains a list of approved OAuth flows that are used for connections to external systems along with any additional relevant details. Refer to Secure- Authentication for more information.

Connected App Name	OAuth Flow	Token Scope	Persona Access	Notes
Integration with [Web App]	*Web Server Flow*	*Access Content Resources*	*Sales Operations*	*Store credentials securely using the following method: _____*
Integration with [Desktop App]	*User-Agent Flow*	*Access Lightning Applications*	*Persona [X]*	*This is an example*
Direct integration with [Server Name]	*JWT Bearer Flow*	*Access Content Resources*	*Persona [Y]*	*This is an example*
[Insert your own]				

Authorization - High Level Sharing Requirements

Object Name	API Name	Standard / Custom	Description	OWD Internal	OWD External	Access Strategy Internal	Access Strategy External	Ownership Strategy	Comments
Contact	*Contact*	*Standard*	*Standard Contact Object*	*Controlled by Parent*	*Controlled by Parent*	*Matches Account Access*	*Matches Account Access*	*Owned by the record creator*	*This is an example*
Payment	*Payment__c*	*Custom*	*Record of payment*	*Public Read*	*Public Read*	*Read Access*	*Read Access*	*Records initially created by integration user and transferred to the user who owns the corresponding sales order*	*Records created via third party integration*
[Insert your own]		Standard							

Authorization - Security Matrix

This section contains a security matrix that you can use to identify object, field, record and feature level access for human and non-human users. Copy and paste the table below to repeat for each persona defined by your organization. Refer to Secure - Authorization and Secure - Sharing and Visibility for additional information.

Persona Details

- **Persona Name:** *Sales Operations Users*
- **Persona Description:** *Users who support the sales team by evaluating data to determine the effectiveness of sales processes.*
- **Internal / External:** *Internal*
- **Human / Non Human:** *Human*
- **Approximate Number of Users:** *50*
- **High Level Access Requirements:** *View and update accounts, contacts, opportunities and orders; run reports*

Detailed Access Requirements

Data				
Object Name	**Business Requirements (in non-technical terms)**	**Technical Requirements**	**Sharing Approach**	**Comments**
Account	*Users can create and edit account details for their own customers.*	*Create, Read, Update own records*	*OWD = Private Perm Set = CRU*	*This is an example*
Contact	*Users can create ande edit contact details for their own customers and for records where field X = 123*	*Create, Read, Update owned records and records where the value of field X = 123*	*OWD = Private Perm Set = CR Criteria based sharing rule on field x*	*This is an example*
All Other Objects	*No Access*	*No Access*	*No Access*	*This is an example*
[Insert your own]				
Features and Functionality				
Feature Name	**Business Requirements (in non-technical terms)**	**Technical Requirements**	**Comments**	
Application [appname]	*No Access*	*No Access*	*This is an example*	
Apex Class [Class Name]	*No Access*	*No Access*	*This is an example*	
Custom Setting [Setting Name]	*No Access*	*No Access*	*This is an example*	
Custom Metadata Type [Type Name]	*No Access*	*No Access*	*This is an example*	
Connected App [App Name]	*Users can perform [x] action within this app*	*Access via [X] method*	*Refer to the connected apps table for additional details*	
[Insert your own]				

Appendix I - Process to Update These Policies

This section contains the process to request and approve updates of this document.

Appendix II - Change Log

This section contains the revision history of this document.

Date	Description of Change	Change made by
1/1/2022	*Added new device policy*	*Tom Leddy*
[Insert your own]		