OKLAHOMA
Office of Management
& Enterprise Services

Salesforce Development and Administration Standard

Introduction

Salesforce is the standard platform for customer relationship management for the State of Oklahoma.

Purpose

The purpose of this document is to provide a roadmap of standard policy and best practices when developing on the Salesforce platform for the state. This standard defines and outlines the procedures Salesforce developers should use when building applications, forms and workflows for OMES.

Standard

- General configuration.
  - Environment – To satisfy the state's security requirements for various classifications of data, all Salesforce applications are deployed into the Government Cloud Plus.
  - Editions – When creating a new Salesforce org, the edition must match the expected usage limits.
- Architecture.
  - All integrations must follow the OMES reference architecture and any integration should be loosely coupled.
  - All proposed integrations must be reviewed and approved by the application services architecture team before development begins.
  - All proposed data models and data elements must be reviewed by the OMES architecture team and Salesforce team.
- Orgs and org maintenance.
  - The state adheres to the Salesforce org configuration best practices.
  - To reduce technical debt and stay current with Salesforce, any new org and functionality must be built solely on the Lightning Experience and not use Salesforce Classic functionality or Visualforce.
  - Any new org creation proposed must be reviewed and approved by the application services architecture team before development begins.
  - All critical/release updates and end-of-life announcements must be resolved within one sprint of notification from Salesforce or have a resolution plan that will be implemented two sprints prior to mandatory date.
  - All Apex code must have their API version numbers update to match the latest version after a Salesforce release.
  - Any vendor/system integrator chosen to maintain an application is also responsible for org maintenance. Such activities include, but are not limited to the following technical audit properties:
    - Patch and package updates/upgrades.
    - SSL certificate renewals.
    - Safe and recommended session settings.
    - Password policies.
    - Login access policies.
    - Sharing settings.
    - File upload and download security settings.

        - Remote site settings.
    - All orgs must have a GitHub repository to store metadata and code from the Salesforce org.
- Users and licenses.
    - All orgs must have an expected yearly user count and monthly visitor count to properly plan out efficient license purchases.
    - Profiles must properly adhere to license contractual agreement. If a potential breach may occur, reach out to the OMES Salesforce team to determine a path of resolution.
- Pre-development project work.
    - All projects must have a business requirements document.
    - User stories must be generated from the business requirements document prior to vendor outreach.
    - Every user story must have a story point estimate from the vendor along with a statement of work. Story points are based on the Fibonacci sequence.
    - Every project must have a design document that includes a description of the application and its processes, as well as the following documents:
        - Sequence diagrams.
        - Mocks of any custom user interfaces.
        - Entity relationship diagrams, if new objects are being created.
        - Architecture landscape diagrams for integrations.
- Development.
    - Salesforce application projects must follow the scrum methodology. Vendors may use project management tools of their choosing, but appropriate access must be granted to all active project team members. Azure DevOps and Atlassian are current toolsets used by the state.
    - All code must follow a forked version of the NimbleUser Apex Style Guide.
    - All code must follow separation of concerns and single responsibility for methods.
    - Customizations must be scalable with limited coupling.
    - All Apex and relevant metadata are stored in a GitHub repository owned by the OMES Salesforce team.
    - All code must have corresponding unit tests that properly assert expected outcomes and negative tests.
    - All code is built on the latest API version and uses native Lightning Experience frameworks.
    - All code shall be reviewed by PMD Static Analysis and warnings must be resolved prior to promotion. Refer to the PMD Apex rules.
    - All code and metadata changes require a pull request to be opened with the OMES Salesforce team for review prior to promotion.
    - No third party/solution integrator code or metadata is used or deployed without review and approval from the Salesforce team.
    - No third-party components/independent software vendors are used or deployed without review and approval from the application services team and the state's security team.
    - Proposed use of any third-party product must not be deployed anywhere in the state's Salesforce ecosystem without the security team issuing an Authority to Operate order.
- Project handoff.
    - All projects must include a data dictionary provided to the state.
    - A regression testing document must be provided for any functionality built.
    - Training documentation must be provided for any custom functionality built.

- Deploying Salesforce features and changes.
    - The state does not currently employ any third party DevOps tools or continuous integration/continuous delivery pipelines, so standard process for code promotion is used.
    - All deployments must follow the Salesforce DX Developer Guide.
    - The systems integrator must publish and communicate a release schedule for any applications with backlog activities.
- Security.
    - Ensure that any user granted admin roles/access truly has the need for such roles.
    - Salesforce guest site users for sites and experiences (formerly communities) shall have no direct access through CRED (create, read, edit, delete) and sharing rules, or ownership to Salesforce records.
    - All Salesforce event log files must be replicated and stored to Google Cloud Platform for at least 18 months.

Compliance

This standard shall take effect upon publication and is made pursuant to Title 62 O.S. §§ 34.11.1 and 34.12 and Title 62 O.S. § 35.8. OMES IS may amend and publish the amended standards policies and standards at any time. Compliance is expected with all published policies and standards, and any published amendments thereof. Employees found in violation of this standard may be subject to disciplinary action, up to and including termination.

Rationale

To coordinate and require central approval of state agency information technology purchases and projects to enable the chief information officer to assess the needs and capabilities of state agencies as well as streamline and consolidate systems to ensure that the state delivers essential public services to its citizens in the most efficient manner at the lowest possible cost to taxpayers.

References

- OMES reference architecture.
- Salesforce org configuration best practices.
- NimbleUser Apex Style Guide.
- PMD Apex rules.
- Salesforce DX Developer Guide.

Revision history

This standard is subject to periodic review to ensure relevancy.

Effective date: 07/08/2022	**Review cycle:** Annual
Last revised: 05/24/2022	**Last reviewed:** 7/18/2023
Approved by: Joe McIntosh, Chief Information Officer	