1.0 Introduction

This guideline outlines the security requirements for web and mobile application development. The Information Security Office should be engaged before development begins, throughout the process, and after the application is published per the established guideline.

Policy Reference:

Information Security Risk Management: ICSUAM 8020.00

Information Systems Acquisition, Development and Maintenance: ICSUAM 8070.00

Standard Reference:

Application Security Standard: ICSUAM 8070.S000

Sacramento State Vulnerability Management Standard: Vulnerability Management Standard

Development Guidelines Reference:

OWASP Guidelines: https://owasp.org/www-pdf-archive/OWASP_SCP_Quick_Reference_Guide_v2.pdf

2.0 Scope

This guideline applies to all applications developed by Sacramento State personnel or hosted on premises at Sacramento State.

This excludes applications solely developed for academic purposes that do not include university data.

3.0 Roles and Responsibilities

Information Security Office (ISO)

- Development review.
- Identify non-compliant applications and contact application owners and business area administrators prior to removal from campus network.
- Manage the removal of non-compliant applications from campus network and/or block and segment.
- Document security exceptions for non-compliant applications where risk will be accepted.
- Review to ensure there are no existing enterprise applications that meet the same need.

- Ensure the proposed application is not already in development elsewhere on campus or within the CSU.
- Review the application to ensure it will be able to meet all applicable information security requirements and perform a risk review.
- Suggest alternatives for the storage of Level 1 and 2 data within the application or access by the application.
- Review application to ensure security measures are in place for security of all Level 1 and Level 2 data.
- Ensure the data owners have been engaged and have provided approval.
- Ensure Web and application development procedures are on file.
- Ensure the web application meets OWASP guidelines.

Application Developers

- Ensure the application meets the security requirements outlined in this guideline document.
- Ensure data is handled according to the requirements outlined in this guideline document.
- Initiate a risk review via a service request ticket.
- Provide an architecture diagram that describes client/server and related back-end servers, and protocols
- Get data owner approval if data is stored or accessed by the application. Data owners list available at: https://www.csus.edu/information-resources-technology/it-governance/data-security-governance.html
- Ensure the data is handled according to established data policies: https://www.csus.edu/information-resources-technology/it-governance/data-security-governance.html
- Ensure the application can meet the established records retention policy: https://www.csus.edu/information-resources-technology/it-governance/data-security-governance.html

Application Owners

- Review vulnerability scan reports and ensure known vulnerabilities are patched according to the Vulnerability Management Standard. https://www.csus.edu/information-resources-technology/information-security/_internal/_documents/sac-vulnerabilitymanagementstandard.pdf
- Ensure necessary or out of band/emergency patching is performed (e.g. zero day vulnerability).
- Enter a change control item with IRT Change Control for application upgrades, patching, and major changes.

4.0 Development Review

Developers anticipating or planning to work on web or application projects hosted on the Sacramento State network or application projects located off campus that include handling of Level 1 or Level 2 data

must notify the Information Security Office prior to beginning development. The Information Security Officer or a designee will review the proposed development to ensure:

- There are no existing enterprise applications that meet the same need.
- The proposed application is not already in development elsewhere on campus or within the CSU.
- The application will be able to meet all applicable information security requirements.
- Alternatives to direct use of Level 1 and 2 data have been considered.
- Security measures are in place for security of all Level 1 and Level 2 data.
- Web and application development procedures are on file.
- Ensure web applications meet OWASP guidelines.

Applications may not be added to the campus network until approval is received from the Information Security Office. Work should not begin on application or web development using Level 1 and Level 2 data until approval is received from the Information Security Office.

5.0 Campus Web and Application Development Architecture

Web and application development should have separation between development, testing, and production environments.

Instance/ Environment	Description	Example
Development	Used for building and preliminary testing of application code. Development systems can either be on a workstation or development server.	Development may be used at random or minimal test data from a production system for testing purpose.
Test	Used for testing final application code against production setups and environment. The test environment must be a complete and current snap shot of the production environment and data. These test systems can be accessed by developers using SSL VPN connections.	Test systems must use a copy of production data to ensure the application has been fully tested against a production environment. Confidential data must be redacted where possible.
Production	Used for the final application. Production systems code must never be modified while the system is in production. Applications in production that need changes must follow the process of development and testing before being implemented into production.	Production data must be maintained and protected and must not be modified for testing or development process.

6.0 Development and Testing Server

- If a development or testing system requires exceptions to the above architecture, these exceptions must be documented and approved by the Information Security Office.

- Development and testing servers must be placed in the appropriate network zone as required by the ISO, based on the data they are handling and/or value to the support to the campus.

- Servers should be running minimal services, e.g. not running other web and database services if not needed by the production application.

- Security-sensitive web-based applications must run on stand-alone dedicated servers or VM server containers; most Business and Academic systems may run on shared servers.

- Limit the privileges of system accounts to least necessary access.

- Limit the privileges of web developers to least necessary access.

- If an application needs a system account, an approved and secure service level account must be created and incorporated into the development of the application.

7.0 Development and Testing Systems

Any application development done using IRT-managed server systems must be done in collaboration with the applicable systems administrator from the Operations & System Services team, using the approved ticketing method. This process will ensure that the system administrator can tailor the security of the server and OS system to the needs of the application. Unencrypted Level 1 or Level 2 data is not to be stored on servers that host websites available to the public.

8.0 Web Application Coding

Sacramento State Web Developers must use the secure code guidelines from the Open Web Application Security Project (OWASP). Applications must be reviewed and tested before being placed into a campus production environment to ensure that the following vulnerabilities are addressed:

- Un-validated input
- Inadequate access control
- Inadequate authentication and session management
- Cross-site scripting (XSS) attacks
- Buffer overflows
- Injection flaws
- Improper error handling
- Insecure storage
- Denial of service Standards
- Insecure configuration management

Web Developers must perform appropriate testing as outlined in the web development guidelines. All applications and information systems must be appropriately documented prior to deployment in a

production environment. Application code created by a campus must be appropriately reviewed before being used in a production environment as determined necessary by risk assessment.

9.0 Source Code Control

Source code shall be stored in the campus IRT supported Version Control system, currently BitBucket/Stash.

10.0 Application Development

10.1 Data Security

Applications development on a Sacramento State system with files containing Level 1 or Level 2 data must be hosted in the IRT data center.

Web and application developers must remove all test data before deploying an information system into a production environment and disable test accounts. Once in the production environment, developers/application owners must work with the Information Security Office to conduct regular risk assessments to ensure the system has security controls that appropriately protect the confidentiality, integrity and availability of the system. Confidential data must not be displayed in any user documentation.

10.2 Inadvertent copies of Level 1 or Level 2 data

Developers must check their systems and their development tools to be sure that copies of Level 1 or Level 2 data files are not created without their knowledge.

10.3 Network Encryption

Developers working with Level 1 or Level 2 data and transmitting this information over computer networks between users' browsers and the server must encrypt the traffic as required by the ISO.

10.4 SSL encryption for outside access

The SSL (Secure Sockets Layer) protocol is Sacramento State's standard for protecting web-based network traffic. The SSL protocol protects data from alteration and disclosure while it is in transit. When a new SSL certificate is required, a request must be sent to the manager of the Operations and Systems Services group to be assigned appropriate controls. A service ticket for an SSL cert should be submitted for this request.

10.5 Server to client

Applications that require clients to access Level 1 or Level 2 data must use SSL or another form of encryption during the connection process.

10.6 Application User Authentication

Applications that require users to authenticate to the application must use the central campus authentication systems, as assigned by the ISO. If the application is not compatible with the campus authentication system, the Information Security Office must be notified in advance of acquisition to review and approve authentication methods. Applications that require an account to authenticate to other systems at Sacramento State must use an approved service level account. A service level account can be requested via a service request ticket.

10.7 Validate input of Data

All data must be validated from all un-trusted data sources. Proper input validation can eliminate the vast majority of software vulnerabilities. External data sources, including command line arguments, network interfaces, environmental variables, and user-controlled files must have logging enabled on the application system.

10.8 Sanitize data sent to other systems

All applications must sanitize all data passed to complex subsystems such as command shells, relational databases, and commercial off-the-shelf (COTS) components. Applications must be able to prevent attacks through the use of SQL, command, or other injection attacks.

10.9 Do not store credentials

Mobile or desktop applications should not store log in credentials.

10.10 Access Control

Sacramento State default access to all applications is based on permission rather than exclusion. This means that, by default, access is denied and the protection scheme identifies conditions under which access is specifically permitted. Systems that use a service level account must use an account that authenticates to the central campus Active Directory.

10.11 Limited number of accounts

The number of user accounts on the system should be kept to the minimum necessary. This minimizes threats because it limits the number of accounts capable of attempting to elevate privileges without authorization.

10.12 Principle of least privilege

Each application process should execute with the least set of privileges necessary to complete the job. Any elevated permission should be held closely and access documented and approved through the Access Control Process.

10.13 Testing

All web and application code must undergo appropriate testing and code review before deployment in a production environment. The security of all such applications and information systems must be appropriately documented prior to deployment in a production environment.

Application's security controls must be tested in cooperation with the Information Security Office. This test must verify that controls are working properly and must be conducted prior to deploying the system into a production environment. Test plan(s) and test results should be documented. Previously deployed systems should be tested as part of any significant upgrade or as determined by risk assessment.

10.14 Code Reviews

Code reviews should be performed. A strong development practice includes peer review. The application reviewer should have a strong background in the languages used by the application, as well as training in identifying security flaws.

A code review is the process of reviewing application code to locate potential security flaws and functionality problems. Any security flaws found should be tracked, clearly identified as a security defect, and fixed before the application is released.

10.15 Web Scanning

Web application scanners allow testers and application developers the ability to scan web applications in a fully operational environment and check for many known security vulnerabilities. Web application scanners parse URLs from the target website to find vulnerabilities. These scanners check web applications for common security problems such as SQL injection, cross site scripting, command injection, buffer overflow, session management flaws, and other vulnerabilities. These tools can be used to satisfy code review requirements based on the security checks provided by the tool.

Web applications must be regularly scanned with the Information Security Office's approved web application scanner via an authenticated scan. Credentials to all web application pages must be provided to the Information Security Office. Scan results must be reviewed, remediated, or mitigated by the web developers based on the documented timeline in the Vulnerability Management Standard. Web application scanning should be used on each web application release prior to deployment to a production environment.

10.16 Source Code Access

Source code access should be restricted to those who need access. Source code access should include at least one back up.

10.17 Universal Design

Applications should be developed to meet Universal Design guidelines.

Applications for learning will meet Universal Design for Learning guidelines:
https://www.csus.edu/information-resources-technology/universal-design-for-learning/

11.0 Application Change Control

All production applications are required to follow Sacramento State's change control process. Upcoming changes must be submitted to the Sacramento State Change Control group for review and approval prior to implementation. Change control review is performed weekly. Personnel requesting the change are required to attend.

Information required for Change Control:

- Title of change
- Application or service to be changed
- Person requesting the change
- Implementation date
- Anticipated impact
- Implementation steps
- Back out plan

12.0 Logs

Server logs for applications shall be gathered, stored, and supplied to the Information Security Office as required by the central campus log practice.

Review / Approval History

Review Date	Reviewed By	Action (Reviewed, Recommended or Approved)
1/26/2022	Information Security Office Staff	Draft created
1/26/2022	Information Security Office and Web Services Staff	Reviewed

2/2/2022	Information Security Office and Campus Application Development Manager	Draft finalized
2/9/2022	IT Collaboration Governance Meeting	Draft Reviewed and Finalized