The California State University
INFORMATION SECURITY MANAGEMENT

8070.S000 Application Security

Last Revised: 07/12/13

Final 00/00/00

REVISION CONTROL

Document Title: Application Security
Author: Information Security
File Reference: 8070.S000_Application_Security.docx

Revision History

Revision Date	Revised By	Summary of Revisions	Section(s) Revised
8/8/12	Alex Harwood	Copied text from the Sac State Application Standard and made adjustments to make it CSU generic verses Sac State specific.	
2/15/13	Alex Harwood	Major changes done with the team	All
3/1/13	Alex Harwood	Minor changes to the document for final draft	All
6/11/13	Macklin	Updates based on team comments	All
7/2/13	Macklin	Updates based on team comments	All

Review / Approval History

Review Date	Reviewed By	Action (Reviewed, Recommended or Approved)
2/15/13	Dustin DeBrum	Reviewed
3/1/13	Felecia Vlahos	Approved for submission to Policy/Standard/Guideline
3/1/13	Alex Harwood	Approved for submission to Policy/Standard/Guideline
7/18/2013	ISAC	Reviewed, approved and recommended for CISO review

8070.S000 Application Security

Implements:	CSU Policy 8070.0
Policy Reference:	https://csyou.calstate.edu/Policies/icsuam/Pages/8070-00.aspx

1.1 Application Security Standards

This standard applies to all CSU applications and web environments which:

- Are considered mission critical systems,
- Access protected level 1 information,
- Access protected level 2 information and are accessible from the Internet, or
- Provide an official public campus service or presence.

Application and web development environments must comply with CSU and campus standards and procedures. Contracts for services involving application, web development or hosting must incorporate appropriate language (see *8040S000 Third Party Contract Language*).

Campuses must develop and maintain information security criteria for application development. These criteria must apply both to internally developed applications and those developed by contractors or vendors. Criteria must include a process for ensuring that the campus Information Security Office is made aware of applications which access or provide protected level 1 data.

1.2 Application and Web Development Environment Assessment

Campus procedures for local development must ensure that before development begins:

- The planned application and supporting environment have been documented. Documentation must:
  - Adequately describe the purpose and behavior of the application
  - Identify the type and configuration of the supporting systems and networks.
- Risk analysis verifies that:
  - The application and supporting environment will comply with all applicable policies, standards, and procedures
  - Deploying the application will not introduce any unacceptable risks.

1.3 Application Development and Production Architecture

Development and testing must be performed in a non-production environment.

- Production environments for applications with high risk should run on stand-alone dedicated servers or VM server containers.
- Production servers and development servers which store, process or transmit protected data must be housed in a data center that meets physical and logical security control requirements as per CSU Information Security *Policy 8080 Physical Security*.
- Servers must be placed in the appropriate network zone based on the campus approved network architecture plan as per *8045S400 Boundary Protection and Isolation Standard § 2.2*.
- Servers should be “hardened” according to the campus configuration procedures in order to ensure that they are secure.

1.4 Application Coding

Applications must be reviewed, tested, and documented as determined by a risk assessment, before being placed into a production environment to ensure vulnerabilities are addressed, including but not limited to:

- 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

The integrity and availability of source code and/or critical files/folders must be ensured by use of a source code control system and scheduled backups.

1.5 Application Development

1.5.1 Data Security

Within the development environment:

- Application developers must remove all test data and test accounts before deploying an application into a production environment.
- Protected data should be redacted where possible in the development environment.

Within the production environment:

- Sample or example scripts must be removed from production servers.
- Protected data may not be displayed in any documentation.
- Developers must check system, test and development tools and processes to be sure that protected data is not copied or created accidentally. Refer to *CSU Policy 8065 Information Asset Management* along with associate standards.

1.5.2 Logging

Applications should log information as *per 8045S600*.

All log data should be written to an external log server or solution as determined by risk.

Logging should be enabled for operating system, database, network, application server, web server and other components of the application system in order to provide sufficient information for incident or problem analysis. See *8054S600 Logging Elements* for more information about logging requirements.

1.5.3 Applications Collecting Personally-Identifiable Data

CSU Policy 8025.0, Privacy of Personal Information, governs the collection and storage of personal information. Respondents should be informed in advance of the use of "web bugs," URL keywords, or other methods to track respondents' identities. Applications collecting personally identifiable information should, and ecommerce sites must post a web privacy statement describing the type of information collected, how it is to be used, and how it may be disclosed.

1.5.4 Encrypt Protected Information

Applications must encrypt Protected Level 1 information as it is transmitted over the network, including login credentials and session identifiers as *per 8065S000 § 12.3 The SSL/TLS (Secure Sockets Layer)* protocol is the CSU standard for protecting web-based network traffic. Certificates must be used to provide positive identification of applications to users. Servers must have valid certificates, signed by a recognized Certificate Authority.

1.5.5 Application Authentication

Applications that authenticate users must establish sessions using a randomized session identifier that expires after a specified total time or user inactivity.

1.5.6 Access Control

Applications shall implement the philosophy of "default deny". Access application content and environments should be denied except for those users and conditions under which access is specifically permitted.

- Developer access privilege should be limited to the least privilege necessary for development.
- 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.
- Users of applications should be prevented from accessing data to which they have not been granted authorization.

Refer to *8060 – Access Control* and related standards for more information.

1.5.7 Application Management

Each application process should execute with the least set of privileges necessary to complete the job

Any elevated permission (system admin account, dba, etc.) should be protected (on a need to know basis), documented and approved through Access Control Processes. Refer to *8060 – Access Control* and related standards for more information on granting permissions.

1.6 Web and Application Testing and Change Management

The security of applications and information systems must be appropriately documented prior to production deployment.

Developers must test the information system's security controls. These tests must verify that controls are working properly.

Tests should be done from a hacker's point of view, and must be conducted prior to production deployment.

The rigor of the test plan must reflect the risk associated with the application along with the classification of the data being stored or accessed. **NOTE**: The *CSU Data Classification Schedule* is located at http://www.calstate.edu/icsuam/sections/8000/8065_FINAL_DRAFT_Data_Classification_CW_V4.pdf .

Developers must document the test plan(s) and test results.

Previously deployed systems must be tested as part of any significant upgrade or as determined by a risk assessment.

1.6.1 Code Reviews

A code review of application code to locate potential security flaws and functionality problems should be performed before production deployment. Any security flaws found should be documented and tracked to resolution.

1.6.2 Web Application Vulnerability Scanning

Web applications should be scanned with an approved web application scanner prior to production deployment and periodically at a frequency determined by risk.

Security vulnerabilities must be remediated or mitigated based on a risk assessment.

1.6.3 Web and Application Change Management

Change management procedures should be in place for all production application implementations.

1.7 Web and Application Periodic Review

Periodic risk assessment reviews should be performed on the application and supporting infrastructure to ensure no new security risks have been introduced.