Purpose and Summary

This standard supports ISO-1300 Secure Application Development and Administration Policy and applies to the design, development, administration, and maintenance of applications and systems managed by the University and that store, transmit or process University data classified as Confidential or Regulated and systems considered to be critical to the business of the University.

Definitions

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information System</td>
<td>A major application or general support system for storing, possessing, or transmitting University Information. An Information System may contain multiple subsystems. Subsystems typically fall under the same management authority as the parent Information System. Additionally, an Information</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>System</td>
<td>System and its constituent subsystems generally have the same function or mission objective, essentially the same operating characteristics, the same security needs, and reside in the same general operating environment.</td>
</tr>
<tr>
<td>ISO</td>
<td>The University's Information Security Office, responsible for coordinating the development and dissemination of information security policies, standards, and guidelines for the University.</td>
</tr>
<tr>
<td>Unit</td>
<td>A college, department, school, program, research center, business service center, or other operating Unit of the University.</td>
</tr>
<tr>
<td>University Information</td>
<td>Any communication or representation of knowledge, such as facts, data, or opinions, recorded in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual, owned or controlled by or on behalf of the University.</td>
</tr>
</tbody>
</table>

**Statements of Standard**

A. Software and system architects, of applications and systems managed by the University and that store, transmit or process University data classified as Confidential or Regulated and systems considered to be critical to the business of the University, must design their applications and systems to adequately cover risks from typical usages and from attack by defining an appropriate security architecture. Security architecture refers to a carefully considered set of features, controls, and processes that contribute to the security posture, or security status, of the system. The following requirements must be met, at minimum:

1. When an application architect devises a security architecture for an application or system, some fundamental principles must be considered, and where appropriate, incorporated into the security architecture. The following list represents the minimum set of such principles and shall not be considered exhaustive:
   a) Defense in Depth: Utilize multiple layers of security so if an attempt is made to exploit a vulnerability, other compensating controls are in place to prevent a successful compromise.
   b) Positive Security Model: Define application constraints and allowed inputs while implicitly denying parameters not defined in the positive model. A positive model (knowing what to allow) is more effective than trying to guess all possible ways the application can be exploited.
   c) Fail securely: Security mechanisms have three possible outcomes: allow the operation, disallow the operation, or exception. Design security mechanisms so that a failure will follow the same execution path as disallowing the operation.
   d) Least privilege: Accounts should have the least amount of permissions required to complete their business function.

2. Additionally, the software or system architect responsible for the security architecture must ensure the application or system is aligned with these constraints:
a) Determine and communicate to users or consumers the classifications of University data, as defined in the University's Data Classification and Handling Standard, the application or system is designed to store, process, or transmit.
b) Generate application log data in a manner consistent with the requirements of the Logging and Monitoring Standard.
c) Achieve approval or validation of claims for compliance with specific regulations from the corresponding regulatory Compliance Office or approved third-parties at least annually.
d) Prominently display, where appropriate, a confidential record indicator on the screen or interface in use by the application, where appropriate for the type of data being accessed.
e) Do not display Regulated data or Personally Identifying Information (e.g. Social Security Numbers, Protected Health Information, Credit Card data), in plaintext, without first acquiring review and approval by the ISO and all relevant information security and privacy compliance offices.
f) Adhere to all requirements of relevant ISO policies or request and obtain approval for exceptions, where needed.

B. Application and system developers, of applications and systems managed by the University and that store, transmit or process University data classified as Confidential or Regulated and systems considered to be critical to the business of the University, must use secure coding practices and adopt security informed development procedures. Security efforts must continue beyond the specification of a security architecture. During implementation, security informed practices help ensure adherence to the planned security posture. The following practices must be adopted, at minimum:

   a) Incorporate secure coding practices for application and system development in all phases of the Systems Development Life Cycle (SDLC). Ensure applications and systems handling University data:
      i. Validate input properly and restrictively, allowing only those types of input that are known to be correct and sanitize or reject invalid user input.
      ii. Execute proper error handling so that errors will not provide detailed system information, deny service, impair security mechanisms, or crash the system.
      iii. Protect web applications against the current Open Web Application Security Project (OWASP) top ten vulnerabilities, at minimum.
   b) Ensure applications handling University data do not use the following type of information in the URL/URI: credentials, access tokens, serial numbers or record numbers, Personally Identifying Information, or Protected Health Information.
   c) Ensure applications handling University data properly authenticate users either through the preferred method of using central authentication systems (NetId+) or through other UA ISO Policy compliant mechanisms.
   d) Ensure applications handling University data use attribute-based (affiliation, role, membership, etc.) authorization methods, rather than individual authorizations, where possible. Where individual authorizations are used, implement and enforce authorization expiration (periods not to exceed one year).

2. Software Development Process
a) Document and implement a secure software development process that integrates security into different phases including requirements, design, implementation, and testing.

b) Conduct code-level security reviews with professionally trained peers for all new or significantly modified critical applications and those that store, transmit, or process Confidential or Regulated data.

c) Implement and maintain a change management process for changes to existing software applications.

d) Implement separate development and production environments.

e) Review and test web applications for security vulnerabilities using an automated web application scanning tool. Application review shall include source code and run time analysis.

f) Ensure only authorized access to source code.

g) Ensure individuals who engage in programming or analysis of software are University employees or Designated Campus Colleagues (DCCs) and have undergone a background check with fingerprinting consistent with the Pre-Employment Screening Policy.

h) Implement a training plan for application developers and system administrators to be aware of latest best practices.

C. Application and system administrators, of applications and systems managed by the University and that store, transmit or process University data classified as Confidential or Regulated and systems considered to be critical to the business of the University, must implement security controls designed to support secure operation. The following practices must be adopted, at minimum:

1. Maintain a full inventory of all applications and systems; which includes descriptions of authentication and authorization systems, the intended data classification and level of criticality for each application, and the custodian(s) assigned to each application.

2. Document clear rules and processes for vetting and granting authorizations.

3. On at least a semi-annual basis, review and remove all authorizations for individuals who have left the University, transferred to another department, or assumed new job duties within the department.

4. Ensure individuals who administer applications and systems are University employees or Designated Campus Colleagues (DCCs) and have undergone a background check with fingerprinting consistent with the Pre-Employment Screening Policy.

5. Replace default passwords, of system components, with robust passphrases and never use clear text for service account passwords.

6. Configure runtime environments so that they do not reveal native framework errors (e.g., .Net, J2EE) to the screen/browser and set up custom error pages for framework errors.

7. Force HTTPS for all browser connections and disable HTTP.

8. Use the most current encryption and hashing algorithms to protect machine-to-machine connections, wherever possible.

9. Authenticate and encrypt the session when software involves the transmission of University Information classified as Confidential or Regulated.

10. Apply requirements in the Vulnerability Management Standard and review and remediate findings, as needed.

11. Establish normal change controls and maintenance cycles for resources.
12. Ensure that system administrators apply all current maintenance and security vulnerability patches.

13. Ensure that only essential application services and ports are enabled and opened in the system’s firewall and on servers.

14. Sanitize equipment to remove all Confidential or Regulated University Information from associated media, following proper procedure, when the Information System or any of its components require offsite Information System security maintenance or repairs or is removed from service.

15. Collect application log data and review for security events as mandated in the Logging and Monitoring Standard.

Related Documentation/Resources

- Exception Process/Procedure
- Data Classification and Handling Standard
- Encryption Standard
- Vulnerability Management Standard
- Logging and Monitoring Standard
- Secure Web Application Development Training
- Pre-Employment Screening Policy