

This standard applies to all software applications being developed or administered by faculty, staff, student employees, contractors and vendors that are designed to handle or manage university *data* and that are running on *devices*, physical or virtual. Adherence to this standard will increase the security of applications and help safeguard *university resources*.

The minimum standards applicable to the development of applications designed to handle or manage university *data* are listed below. All listed standards are generally required for applications designed to handle or manage *confidential university data* and are either required or recommended for all other applications. Refer to the Data Classification Standard or the Information Security Terms Guideline (IS-G100) for the definition of *confidential university data*.

If any of the minimum standards cannot be met for applications handling or managing *confidential university data*, an exception must be obtained (see the Exceptions Procedure). IT *owners* and *custodians*, *data stewards*, *lead researchers*, *system administrators* and application developers are expected to use their professional judgment in managing risks to the *data*, systems and applications they use and/or support. All security controls should be proportional to the confidentiality, integrity, and availability requirements of the *data* processed by the system.

Standard	Practice	<i>Confidential University Data</i>	All Other Data
1	Classify the university <i>data</i> handled or managed by the application according to the Data Classification Standard (IS-S302).	Required	Required
2	Prominently display a “Confidential Record” banner to the screen or interface in use by the application, depending on the type of <i>data</i> being accessed (for example, <i>data</i> protected by FERPA, HIPAA, etc.).	Recommended	Recommended
3	Display no <i>data</i> that have been specifically restricted by law or policy (for example, Social Security Numbers, protected health information or payment cardholder <i>data</i>) unless permitted by the <i>UIISO</i> .	Required	N/A
4	Ensure applications validate input properly and restrictively, allowing only those types of input that are known to be correct. Examples include, but are not limited to,	Required	Recommended

Standard	Practice	<i>Confidential University Data</i>	All Other Data
	cross-site scripting, buffer overflow errors, and injection flaws. See http://www.owasp.org for more information and examples.		
5	Ensure applications execute proper error handling so that errors will not provide detailed system information, deny service, impair security mechanisms, or crash the system. See http://www.owasp.org for more information and examples.	Required	Recommended
6	Ensure applications processing <i>data</i> properly authenticate users through central authentication systems (WebAuth, CatNet Active Directory or Shibboleth), where possible.	Required	Recommended
7	Establish authorizations for applications by affiliation, membership, or employment, rather than by individual, where possible. NOTE: UA NetID authentication is not authorization.	Required	Recommended
8	Use central authorization tools (Enterprise Directory Service or Shibboleth; WebAuth or CatNet Active Directory for rudimentary authorization decisions with appropriate configuration) where possible, and if additional functionality (such as attribute or grouping) is needed, coordinate development with University Information Technology Services.	Required	Recommended
9	Provide automated review of authorizations where possible.	Recommended	Recommended
10	Set any individual authorizations to expire and require their renewal on a periodic basis, at least annually.	Required	Recommended
11	Ensure applications make use of secure	Required	Recommended

Standard	Practice	<i>Confidential University Data</i>	All Other Data
	<p>storage for university <i>data</i> as required by confidentiality, integrity and availability needs. <i>Personal information</i> must be encrypted (see the Encryption Guideline). Security for all other <i>data</i> can be provided by means such as, but not limited to, encryption, access controls, file system audits, physically securing the storage media, or any combination thereof as deemed appropriate.</p>		
12	<p>Implement encrypted communications for services or applications, as required by <i>confidentiality</i> and <i>integrity</i> needs.</p>	Required	Recommended
13	<p>Implement the use of application logs to the extent practical, given the limitations of certain systems to store large amounts of log <i>data</i>. When logging access to university <i>data</i>, store logs of all users and times of access for at least 14 days.</p>	Required	Recommended
14	<p>Conduct code-level security reviews with peers for all new or significantly modified applications; particularly, those that affect the collection, use, and/or display of <i>confidential university data</i>, documenting the actions that were taken. Use threat modeling to prioritize the review.</p>	Required	Recommended
15	<p>Conduct security tests of new Internet applications before they are released to a production environment.</p>	Required	Recommended
16	<p>Conduct annual security tests of and obtain annual security scans of Internet applications.</p>	Recommended	Recommended
17	<p>Ensure that obsolete applications, or portions of applications, are removed from any possible execution environment.</p>	Required	Recommended

Standard	Practice	<i>Confidential University Data</i>	All Other Data
18	Implement and maintain a change management process for changes to existing software applications.	Required	Recommended
19	Require third parties providing software and/or receiving university <i>data</i> to enter into written agreements with the University to secure systems and <i>data</i> according to the provisions of the Minimum Security for Networked Devices Standard, the Server Security Standard and this standard.	Required	Recommended

All italicized terms used in this standard are defined in the Information Security Terms Guideline.

Related Guidance

Information Security Policy (IS-100)
Information Security Terms Guideline (IS-G100)
Exceptions Procedure (IS-P100)
SSN Usage (IS-S301)
Data Classification Standard (IS-S302)
Critical Device Scanning Procedure (IS-P601)
Minimum Security for Networked Devices Standard (IS-S701)
Server Security Standard (IS-S702)
Web Application Security Assessment Procedure (IS-P801)
Encryption Guideline (IS-G801)
Payment Card Industry Data Security Standard Requirement 6.6
OWASP Top Ten, http://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

Reference

Portions adapted from “Minimum Standards for Application Development and Administration” (<http://www.utexas.edu/its/policies/opsmanual/appstd.php>), with permission from ITS, The University of Texas at Austin, Austin, Texas 78712-1100.

Revision History

Initial Draft	11/6/08
UA-ISAC Review of Initial Draft	4/2/09
Effective Date of Initial Draft	7/1/09
UA-ISAC Review of 1 st Revised Draft	10/6/09
Effective Date of 1 st Revised Draft	10/6/09