THE UNIVERSITY OF ARIZONA.

**Standard Title:** Application Security
**Standard Number:** IS-S801
**Responsible Office:** Information Security Office

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. IT *owners* and *custodians*, *data stewards*, lead researchers, *system administrators* and application developers are expected to use their professional judgment in managing risks to *data*, systems and applications they use and/or support. The Information Security Office is an important resource to help with questions or clarification of these standards. Adherence to this standard will increase the security of applications and help safeguard *university resources*.

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. If any of the standards cannot be met for applications handling or managing *confidential university data*, an exception must be obtained (see the Exceptions Procedure). Refer to the Data Classification Standard or the Information Security Terms Guideline (IS-G100) for the definition of *confidential university data*.

The number and level of security controls should be proportional to the *confidentiality, integrity*, and *availability* requirements of the *data* processed by the system:

- *Confidentiality* controls only allow access to *data* for which the user is permitted.
- *Integrity* controls ensure *data* are not tampered or altered by unauthorized users.
- *Availability* controls ensure systems and *data* are available to authorized users when they need it.

| **Standard** | **Practice** | ***Confidential University Data*** | **All Other *Data*** |
|---|---|---|---|
| 1. | Classify the *university data* handled or managed by the application according to the Data Classification Standard (IS-S302). | Required | Required |
| 2. | Establish ownership and stewardship of application and *data* as appropriate. | Required | Required |
| 3. | Use threat modeling to characterize people, groups and automated processes that may be able to attack the application. Consider application features that permit or could permit access and consider questions like:<br>• Is there anything about the process supporting input or access that is flawed?<br>• How would I abuse this feature if I were so inclined?<br>• Is the feature required to be on by default? If so, are there limits or options that could help reduce the risk from this feature? | Required | Required for all internet accessible applications |

| Standard | Practice | *Confidential University Data* | All Other *Data* |
|---|---|---|---|
| 4. | Follow UA Minimum Security for Networked Devices Standard and the Server Security Standard and require third parties receiving *university data* to also secure systems by UA standards. Ensure that third-party contracts address breach notification responsibilities and destruction of *university data* at end of contract. | Required | Required |
| 5. | Utilize OWASP top 10 guidelines during web/application development. See http://www.owasp.org for guidance on how to minimize attack surface area, establish secure defaults, utilize defense in depth, fail securely and manage services and sessions securely. | Required | Required |
| 6. | Ensure applications processing *data* follow logical access guidelines and use existing UA centralized *authentication* and *authorization* tools where technically possible. Where applications that work with *confidential university data* cannot meet this requirement, contact the Information Security Office for additional guidance. | Required | Recommended |
| 7. | Make use of secure storage for *university data* as required by *confidentiality, integrity* and *availability* needs. Where technical tools and solutions exist for file types and *data* structures, *Personal information* must be *encrypted* (see the Encryption Guideline). Security for all other *data* 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. | Required where tools exist, otherwise use multiple layers of controls. | Recommended |
| 8. | Application databases should follow secure practices including, but not limited to:<br>• Limiting backend database access to the web server whenever possible.<br>• Authenticating connections from the web server.<br>• Reading passwords from a protected configuration file instead of from scripts.<br>• Using fully qualified paths to files used by the application. Use parameters or other identifiers in conjunction with secure configuration files containing allowed directories and paths.<br>• Specifying read-only mode when opening configuration files, input *data* files as read-only, output *data* files as write-only or append-only and *log* files as append-only. | Required | Required |

| Standard | Practice | *Confidential University Data* | All Other *Data* |
|---|---|---|---|
| | • Placing *data* files only in directories that **can't** be accessed from a web browser. | | |
| 9. | Implement encrypted communications for services or applications, as required by *confidentiality* and *integrity* needs. | Required | Recommended |
| 10. | Implement the use of application *logs* to the extent practical, given the limitations of certain systems to store large amounts of *log data*. When logging access to *university data*, store *logs* of all users and times of access for at least 14 days. | Required | Recommended |
| 11. | Implement backup procedures for applications and *data* as required for *integrity* and *availablity* requirements. Test "restore" procedures and document *business continuity* processes for critical *university resources*. | Required | Recommended |
| 12. | Conduct peer code-level security reviews for all programming changes in applications. | Required | Required for all internet accessible applications |
| 13. | Conduct security scans of new, upgraded or significantly modified applications before they are released to a production environment. | Required | Required for all internet accessible applications |
| 14. | Conduct security reviews and tests of applications as per related guidelines (IS-P802). | Required | Required for all internet accessible applications |
| 15. | Ensure that obsolete applications, or portions of applications, are removed from any possible execution environment. | Required | Recommended |
| 16. | Implement and maintain a change management process for changes to existing software applications. | Required | Recommended |

**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)
Minimum Security for Networked Devices Standard (IS-S602)
Server Security Standard (IS-S603)
Access Control Standard (IS-S702)
Web Application Security Assessment Procedure (IS-P801)
Web Application Security Review Procedure (IS-P802)

Business Continuity and Disaster Recovery Planning Standard (IS-S900)
Payment Card Industry Data Security Standard Requirement 6.6
OWASP Top Ten

**Reference**

Portions adapted from "Minimum Standards for Application Development and Administration", with permission from ITS, The University of Texas at Austin, Austin, Texas 78712-1100 and "UF Guidelines to Develop Applications for Secure Deployment", with permission from Information Technology, University of Florida, Gainesville, FL 32611

All *italicized* terms used in this standard are defined in the Information Security Terms Guideline (IS-G100).

**Revision History**

| | |
|---|---|
| Initial Draft | 11/6/08 |
| UA-ISAC Review of Initial Draft | 4/2/09 |
| Effective Date of Initial Standard | 7/1/09 |
| UA-ISAC Review of Rev. 1 Draft | 10/6/09 |
| Effective Date of Rev. 1 Standard | 10/6/09 |
| UA-ISAC Review of Rev. 2 Draft | 5/11/10 |
| Effective Date of Rev. 2 Standard | 5/11/10 |
| UA-ISAC Review of Rev. 2 Draft | 8/3/10 |
| Sent to UA-ISAC for review after revision | 8/16/10 |
| Effective Date | 8/16/10 |