

# Minimum Security Standards for Application Development and Administration

---

1. Purpose .....	1
2. Scope.....	1
3. Audience .....	2
4. Minimum Standard .....	2
5. Non-Compliance and Exceptions .....	4
6. Related Policies, Procedures, Best Practices and Applicable Laws.....	5
7. Revision History .....	5
8. Approvals .....	6

## 1. Purpose

This minimum standard serves as a supplement to the [Information Resources Use and Security Policy](#), which was drafted in response to [Texas Administrative Code 202](#) and [UT System UTS-165](#). Adherence to the standard will increase the security of applications and help safeguard university information technology resources.

Compliance with these requirements does not imply a completely secure application or system. Instead, these requirements should be integrated into a comprehensive system security plan.

## 2. Scope

This standard applies to all software applications that are being developed or administered by the audience referenced in Section III and that are running on devices, physical or virtual, where university data are classified as Category I, II, or III (see [Data Classification Standard](#)).

### 3. Audience

All faculty, staff, student employees, contractors, and vendors developing or administering applications designed to handle or manage university data.

### 4. Minimum Standard

This section lists the minimum standards that should be applied to the development and administration of applications working with Category-I, -II, or -III data. Standards for Category-I are generally required.

If a solution is not available for a specific requirement, then the specific requirement is waived until an appropriate solution is made available. In such cases a security exception shall be filed ([see part V below](#)). 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 information, 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.

#### 4.1. Application Development

#	Practice	Cat-I	Cat-II/III
4.1.1	Classify the university data handled or managed by the application (see Data Classification Standard).	Required	Required
4.1.2	Prominently display a <a href="#">Confidential Record banner</a> to the screen or interface in use by the application, depending on the type of data being accessed (for example, FERPA, HIPAA, etc.). Do not display Category-I data that has been specifically restricted by law or policy (for example, Social Security Numbers, Protected Health Information, or Credit Card data) unless permitted by the university's <a href="#">Office of Institutional Compliance</a> .	Required	Recommended
4.1.3	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, such possibilities as cross-site scripting, buffer overflow errors, and injection flaws. See <a href="http://www.owasp.org/">http://www.owasp.org/</a> for more information and examples.	Required	Recommended
4.1.4	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 <a href="http://www.owasp.org/">http://www.owasp.org/</a> for more information and examples.	Required	Recommended

**Minimum Security Standards for Application Development and Administration**  
**Document Version: Approved**

#	Practice	Cat-I	Cat-II/III
4.1.5	Ensure applications processing data properly authenticate users through central authentication systems, specifically, UT Direct, Austin Active Directory, TAM (uTexas Access Manager, forthcoming), EID Fat Cookie, or Shibboleth.	Recommended	Recommended
4.1.6	Establish authorizations for applications by affiliation, membership, or employment, rather than by individual.	Recommended	Recommended
4.1.7	If individual authorizations are used, these should expire and require renewal on a periodic (at least annually) basis.	Required	Recommended
4.1.8	Provide automated review of authorizations where possible.	Recommended	Recommended
4.1.9	Use central authorization tools where possible, and if additional functionality is needed, coordinate development with Information Technology Services (ITS).	Recommended	Recommended
4.1.10	Ensure applications make use of secure storage for university data as far as system administrators, in accordance with the provisions of the <a href="#">Minimum Security Standards for Systems</a> , provide such storage.	Required	Recommended
4.1.11	Services or applications running on systems manipulating Category-I data should implement secure (that is, encrypted) communications as required by confidentiality and integrity needs.	Required	Recommended
4.1.12	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
4.1.13	Conduct code-level security reviews with professionally trained peers for all new or significantly modified applications; particularly, those that affect the collection, use, and/or display of confidential Category-I data, documenting the actions that were taken.	Required	Recommended
4.1.14	Conduct annual security tests of Internet applications. Request annual <a href="#">security scans of Internet applications</a> (EID authentication required).	Recommended	Recommended
4.1.15	Ensure that obsolete applications, or portions of applications, are removed from any possible execution environment.	Required	Recommended

## Minimum Security Standards for Application Development and Administration

Document Version: Approved

#	Practice	Cat-I	Cat-II/III
4.1.17	Implement and maintain a <a href="#">change management process</a> for changes to existing software applications.	Required	Recommended
4.1.18	Third parties, for example, vendors, providing software and/or receiving university data must enter into written agreements with the university to secure systems and data according to the provisions of <a href="#">section 24 of the IT Security Operations Manual</a> .	Required	Recommended

### 4.2. Application Administration

#	Practice	Cat-I	Cat-II/III
4.2.1	Maintain a full inventory of all applications, using the Information Security Office's Application Registry ( <a href="https://appreg.security.utexas.edu">https://appreg.security.utexas.edu</a> ), which includes descriptions of authentication and authorization systems, the data classification and level of criticality for each application, and the custodian(s) assigned to each application.	Required	Recommended
4.2.2	Document clear rules and processes for vetting and granting authorizations.	Required	Recommended
4.2.3	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.	Required	Recommended
4.2.4	Individuals who administer computer systems associated with university data or engage in programming or analysis of software that runs on such systems must: (a) undergo a background check and completion of the <a href="#">Security Sensitive Form</a> , and (b) acknowledge these minimum standards on at least a two year cycle.	Required	Recommended

## 5. Non-Compliance and Exceptions

For all application developers and administrators – if any of the minimum standards contained within this document cannot be met for applications manipulating Category I or II data that you support, an Exception Process must be initiated that includes reporting the non-compliance to the Information Security Office, along with a plan for risk assessment and management. (See [Security Exception Report](#).) Non-compliance with this standard may result in revocation of developer or administrator access, notification of supervisors, and reporting to the Office of Internal Audit and/or the Office of Compliance.

Employees of The University of Texas at Austin are required to comply with both institutional rules and regulations and applicable UT System rules and regulations. In addition to university and System rules and regulations, University of Texas at Austin employees are required to comply with state laws and regulations.

## 6. Related Policies, Procedures, Best Practices and Applicable Laws

The policies and practices listed here inform the application development and administration practices described in this document. You should be familiar with these documents. (This is not a complete list of policies and procedures that affect IT resources.)

[UT System UTS-165, Information Resources Use and Security Policy](#)

[UT Austin Information Resources Use and Security Policy](#)

[UT Austin Acceptable Use Policy](#)

[UT Austin Data Classification Guidelines](#)

[UT Austin Information Security Exception Process](#)

[ITS-Applications Security Sections of Analyst Training Program Challenges](#)

## 7. Revision History

Version	Date	New	Original
<b>Minimum Security Standards for Application Development and Administration</b>	2/28/2011	Converted web page to PDF	No changes
	7/22/2010	On July 02, 2010, the Business Services Committee (BSC), part of the campus-wide IT governance structure ( <a href="http://www.utexas.edu/cio/itgovernance">http://www.utexas.edu/cio/itgovernance</a> ) endorsed the Chief Information Security Officer's proposal for the university to standardize on one enterprise method for inventorying applications -by using the ISO's Application Registry. The Application Registry has been in production for some time and is widely used, but this change will eliminate confusion in the development community. This change will be made effective immediately and will be communicated to the campus IT development community.	Maintain a full inventory of all applications with descriptions of authentication and authorization systems, along with the data classification and level of criticality for each application. Ensure a custodian(s) is assigned to each application.

**Minimum Security Standards for Application Development and Administration**

**Document Version:** Approved

Version	Date	New	Original
	10/1/2009	Updated visual appearance to new template. Corrected any out of date links to ensure they are pointing to the most current policy documents.	
	6/20/2008	Added link to University Login Banner page.	No link.
	9/14/2007	Added this Change Log. Changed reference in section I. Purpose and References sections to UTS-165. Removed reference to BPM 66 (consolidated into UTS 165).	"BPM 53"

## 8. Approvals

Name	Role	Members	Date
Chief Information Security Officer	Approval	Cam Beasley	March 3, 2011