The University of Texas at El Paso
Information Security Office
Minimum Security Standards for Applications Development and Administration

Contents

Purpose

This Minimum Security Standard for Standards for Applications Development and Administration[1] serves as a supplement to The University of Texas at El Paso Information Resources Use and Security Policy, which was drafted in response to Texas Administrative Code 202 and UT System 165. Adherence to the standard will increase the security of applications and help safeguard the University's Information 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.

Scope

This standard applies to all software applications that are being developed or administered by the audience referenced under "Audience" below and that are running on devices, physical or virtual, where university data are classified as Confidential, Controlled, or Published (see Standard 9: Data Classification).

Audience

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

Minimum Standards

This section lists the minimum standards that should be applied to the development and administration of applications working with Confidential, Controlled, or Published data. Standards for Confidential data 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 below-Non Compliance and Exceptions). Information Technology 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.

[1] Adapted from "Minimum Security Standards For Application Development and Administration" (https://security.utexas.edu/policies/standards_application), with permission from ITS, The University of Texas at Austin, Austin, Texas 78712-1110

Application Development

#	Practice	Confidential	Controlled & Published
1.1	Classify the university data handled or managed by the application (see Standard 9: Data Classification).	Required	Required
1.2	Prominently display a Confidential Record Banner (see also Standard 19: Server and Device Configuration and Management §19.6) 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 Confidential 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 Chief Information Security Officer.	Required	Recommended
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 https://www.owasp.org/index.php/Main_Page for more information and examples.	Required	Recommended
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 http://www.owasp.org/ for more information and examples.	Required	Recommended
1.5	Ensure applications processing data properly authenticate users through central authentication systems; specifically, UT Direct, Miners Active Directory, Single Sign On, Shibboleth, etc.	Recommended	Recommended
1.6	Establish authorizations for applications by affiliation, membership, or employment, rather than by individual.	Recommended	Recommended
1.7	If individual authorizations are used, these should expire and require renewal on a periodic (at least annually) basis.	Required	Recommended

1.8	Provide automated review of authorizations where possible.	Recommended	Recommended
1.9	Use central authorization tools where possible, and if additional functionality is needed, coordinate development with Information Technology (IT).	Recommended	Recommended
1.10	Ensure applications make use of secure storage for university data as far as system administrators, in accordance with the provisions of the Minimum Security Standards for Systems, provide such storage.	Required	Recommended
1.11	Services or applications running on systems manipulating Confidential data should implement secure (that is, encrypted) communications as required by confidentiality and integrity needs.	Required	Recommended
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 90 days.	Required	Recommended
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 data, documenting the actions that were taken.	Required	Recommended
1.14	Conduct security tests of Internet applications and sites. Request security scans of Internet applications and sites.	Required	Recommended
1.15	Ensure that obsolete applications, or portions of applications, are removed from any possible execution environment.	Required	Required
1.16	Implement and maintain a change management process for changes to existing software applications. (see Standard 7: Change Management)	Required	Recommended
1.17	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 Standard 21 of The UTEP Information Resources Use and Security Policy.	Required	Recommended

Applications Administration

#	Practice	Cat-I	Cat-II/III
2.1	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.	Required	Recommended
2.2	Document clear rules and processes for vetting and granting authorizations.	Required	Recommended
2.3	On at least an 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
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 criminal background check (see UTEP Handbook of Operating Procedures, 21.1 Criminal Background Check Requirements), and (b) acknowledge these minimum standards on at least a two year cycle.	Required	Recommended

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 Reporting Process) 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/ the Office of Institutional Compliance.

Employees of The University of Texas at El Paso 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, The University of Texas at El Paso employees are required to comply with state laws and regulations.

Related UTEP 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 UTS165 – Information Resources Use and Security Policy

UTEP Information Resources Use and Security Policy

UTEP Standard 2: Acceptable Use Policy

UTEP Standard 9: Data Classification

UTEP Standard 13: Control and Protection of Social Security Numbers

UTEP Security Exception Reporting Process

UTEP Standard 13: Control and Protection of Social Security Numbers

UTEP Standard 13: Control and Protection of Social Security Numbers

Revision History

Created:	September 28, 2007
Revised:	March 8, 2008
Revised:	February 14, 2012
Revised:	October 12, 2018 Corrections to numbering; replace Category I-II with Confidential, Controlled and Published; fixed broken links; incorporate minor changes to require pentests for applications processing Confidential data per recent HB8 (85th Legislature).
Approved:	October 12, 2018 by the Chief Information Security Officer