The University of Texas at El Paso

Information Security Office
Minimum Security Standards for Systems

Table of Contents

1. Purpose

The University of Texas at El Paso ("UTEP", also referred to as "the University") Minimum Security Standards for Systems[1] policy serves as a supplement to The University of Texas at El Paso Acceptable Use of Information Resources Policy, which was drafted in response to Texas Administrative Code 202 and UTS165 Information Resources Use and Security Policy. Adherence to the standards will increase the security of systems and help safeguard University Information Resources. These minimum standards exist in addition to all other university policies and federal and state regulations governing the protection of the University's Information Resources.

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

2. Scope

These standards apply to all devices, physical or virtual, connected to the University Network through a physical, wireless, or VPN connection where data is classified as Confidential, Controlled, or Published (see The University of Texas at El Paso Data Classification Standard). Systems that store and/or process credit card information must also comply with UTEP's Minimum Security Standards for Merchant Payment Card Processing requirements.

3. Audience

All users with systems connected to the University Network as in Section 2 above.

4. Minimum Standards

This section lists the minimum standards that shall be applied and enabled in Confidential, Controlled, or Published data systems that are connected to the University Network. Standards for Confidential data are generally required.

If products are not available from reputable commercial or reliable open source communities for a specific requirement, then the specific requirement is waived until an appropriate solution is available. In such cases a Security Exception Report shall be filed (see The University of Texas at El Paso Security Exception Reporting Process).

System owners and custodians, lead researchers, and/or systems administrators are expected to use their professional judgment in managing risks to the information and systems they use and/or support. All security controls should be proportional to the confidentiality, integrity, and availability (CIA) requirements of the data processed by the system.

[1] Adapted from the "Minimum Standards for Security Systems" (https://security.utexas.edu/policies/standards_systems), with permission from ITS, The University of Texas at Austin, Austin, Texas 78712-1110

4.1 Backups

#	Practice	Confidential	Controlled & Published
4.1.1	System administrators should establish and follow a procedure to carry out regular system backups.	Required	Recommended
4.1.2	Backups must be verified at least monthly, either through automated verification, through customer restores, or through trial restores.	Required	Recommended
4.1.3	Systems administrators must maintain documented restoration procedures for systems and the data on those systems.	Required	Recommended

4.2 Change Management

#	Practice	Confidential	Controlled & Published
4.2.1	There must be a change control process for systems configuration. This process must be documented.	Required	Recommended
4.2.2	System changes should be evaluated prior to being applied in a production environment. • Patches must be tested prior to installation in the production environment if a test environment is available. • If a test environment is not available, the lack of patch testing should be communicated to the service subscriber or data customer, along with possible changes in the environment due to the patch.	Required	Recommended

4.3 Computer Virus Prevention

#	Practice	Confidential	Controlled & Published
4.3.1	Anti-virus software must be installed and enabled.	Required	Required
4.3.2	Anti-spyware software must be installed and enabled. Installing and enabling anti-spyware software is required if the machine is used by administrators to browse Web sites not specifically related to the administration of the machine.	Recommended	Recommended
4.3.3	Anti-virus and, if applicable, anti-spyware software should be configured to update signatures daily.	Required	Recommended
4.3.4	Systems administrators should maintain and keep available a description of the standard configuration of anti-virus software.	Required	Recommended

4.4 Physical Access

#	Practice	Confidential	Controlled & Published
4.4.1	Systems must be physically secured in racks or areas with restricted access. Portable devices shall be physically secured if left unattended.	Required	Recommended
4.4.2	Backup media must be secured from unauthorized physical access. If the backup media is stored off-site, it must be encrypted or have a documented process to prevent unauthorized access.	Required	Recommended

4.5 System Hardening

#	Practice	Confidential	Controlled & Published
4.5.1	Systems must be set up in a protected network environment or by using a method that assures the	Required	Recommended

#	Practice	Confidential	Controlled & Published
	system is not accessible via a potentially hostile network until it is secured.		
4.5.2	Operating system and application services security patches should be installed expediently and in a manner consistent with change management procedures. Products no longer receiving security updates from the vendor (e.g., unsupported) are not authorized.	Required	Required
4.5.3	If automatic notification of new patches is available, that option should be enabled.	Required	Required
4.5.4	Services, applications, and user accounts that are not being utilized should be disabled or uninstalled.	Required	Recommended
4.5.5	Methods should be enabled to limit connections to services running on the host to only the authorized users of the service. Software firewalls, hardware firewalls, and service configuration are a few of the methods that may be employed.	Required	Recommended
4.5.6	Services or applications running on systems manipulating Confidential data should implement secure (that is, encrypted) communications as required by confidentiality and integrity needs (see Data Encryption Guidelines).	Required	Recommended
4.5.7	Systems will provide secure storage for Confidential data as required by confidentiality, integrity, and availability (CIA) needs. Security can be provided by means such as, but not limited to, encryption (see Data Encryption Guidelines), access controls, file system audits, physically securing the storage media, or any combination thereof as deemed appropriate.	Required	Recommended
4.5.8	If the operating system supports it, integrity checking of critical operating system files should be enabled and tested. Third-party tools may also be used to implement this.	Required	Recommended

#	Practice	Confidential	Controlled & Published
4.5.9	Integrity checking of system accounts, group memberships, and their associated privileges should be enabled and tested.	Required	Recommended
4.5.10	The required University warning banner should be installed.	Required	Recommended
4.5.11	Whenever possible, all non-removable or (re-) writeable media must be configured with file systems that support access control.	Required	Recommended
4.5.12	Access to non-public file system areas must require authentication.	Required	Required
4.5.13	Strong password requirements shall be enabled, as technology permits, based on the category of data the account is allowed to access (UTEP Data Classification Standards).	Required	Required
4.5.14	Apply the principle of least privilege to user, administrator, and system accounts.	Required	Recommended

4.6 Security Monitoring

#	Practice	Confidential	Controlled & Published
4.6.1	If the operating system comes with a means to log activity, enabling and testing of those controls is required.	Required	Recommended
4.6.2	Operating system and service log monitoring and analysis should be performed routinely. This process should be documented.	Required	Recommended
4.6.3	The systems administrator must follow a documented backup strategy for security logs (for example, account management, access control, data integrity,	Required	Recommended

#	Practice	Confidential	Controlled & Published
	etc.). Security logs should retain at least 14 days of relevant log information (***NOTE: data retention requirements for specific data should be considered. For example, Payment Card Industry audit trail history and log retention should be retained for at least one year depending on PCI system classification – SAQ-XX, etc.***).		
4.6.4	All administrator or root access must be logged.	Required	Recommended

4.7 Remote Administration

#	Practice	Confidential	Controlled & Published
4.7.1	Systems, including but not limited to servers, desktops, laptops, routers, tablets, etc., accessible from the internet must be securely accessed using two-factor authentication. If two-factor authentication is not available, then it must be accessed using the University's Virtual Private Network (VPN).	Required	Required

5. Security Review for New Security Software and Appliances

Departments evaluating the implementation of new security software or appliances, involving **Confidential** type data, should request a security review by sending a written description of the proposed implementation to the Information Security Office prior to selecting vendors or products. Security reviews tend to be informal and can often be performed quickly, while ensuring that best practices are being considered.

6. Non-Compliance and Exceptions

For all system administrators — if any of the minimum standards contained within this document cannot be met on systems manipulating **Confidential** or **Controlled** data that you support, an Exception Process must be initiated that includes reporting the non-compliance to the ISO, along with a plan for risk assessment and management (See Security Exception Reporting Process). Non-compliance with these standards may result in revocation of system or network access, notification of supervisors, and reporting to the Data Owner and Information Security Office.

7. Related Policies, Procedures, Best Practices and Applicable Laws

The policies and practices listed here inform the system hardening procedures described in this document and with which you should be familiar (This is not an all-inclusive list of policies and procedures that affect information technology resources).

The University of Texas at El Paso employees 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 and federal laws and regulations.

- UTEP Information Resources Use and Security Policy
- Standard 2: Acceptable Use of Information Resources
- Standard 9: Data Classification
- Security Exception Reporting Process
- Protection of Sensitive Digital Research Data
- UTS165 Information Resources Use and Security Policy
- Texas Administrative Code §202

8. Revision History

Version	*Date*	*Author*	*Description of Change*
1.0	September 28, 2007	ISO	Document Created
1.1	March 29, 2010	ISO	Reviewed
2.0	July 20, 2011	ISO	Document revised to reflect current requirements.
3.0	December 22, 2015	ISO	Document revised to reflect standardized Revision History and Approvals. Updated links to point to most current ISO Policy and Standards, and changed terminology to reflect new data classification terms.
3.1	March 23, 2017	ISO	Review document, update links and fix table formatting
3.2	May 23, 2017	ISO	Added section 4.7.1 Remote Access and fixed additional links

9. Approvals

Name	*Title*	*Role*	*Date*
Gerard D Cochrane Jr	Chief Information Security Officer	Approval	09/28/2007
Gerard D Cochrane Jr	Chief Information Security Officer	Approval	03/29/2010
Gerard D Cochrane Jr	Chief Information Security Officer	Approval	07/20/2011
Gerard D Cochrane Jr	Chief Information Security Officer	Approval	12/22/2015
Gerard D Cochrane Jr	Chief Information Security Officer	Approval	03/23/2017
Gerard D Cochrane Jr	Chief Information Security Officer	Approved	05/23/2017