

Minimum Security Standards for Systems

1. Purpose	1
2. Scope.....	1
3. Audience	1
4. Minimum Standards.....	2
5. Security Review for New Security Software and Appliances	4
6. Non-Compliance and Exceptions	5
7. Related UT Austin Policies, Procedures, Best Practices and Applicable Laws	5
8. Revision History	5
9. Approvals	8

1. Purpose

These minimum standards serve 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 standards will increase the security of [systems](#) and help safeguard university information technology resources. These minimum standards exist in addition to all other university policies and federal and state regulations governing the protection of the university's data.

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 networks](#) through a physical, wireless, or VPN connection where data is classified as Category I, II, or III (see [Data Classification Standard](#)).

3. Audience

All users with systems connected to the university network as in Sec. II, above.

4. Minimum Standards

This section lists the minimum standards that should be applied and enabled in Category I, II, and III data systems that are connected to the university network. Standards for Category I 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](#) will be filed.

[IT Owners](#) and [IT 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](#) requirements of the data processed by the system. A current list of recommended software is maintained on the [ITS BevoWare Web site](#).

4.1. Backups

#	Practice	Cat I	Cat II & III
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	Cat I	Cat II & III
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	Cat I	Cat II & III
4.3.1	Anti-virus software must be installed and enabled.	Required	Required

#	Practice	Cat I	Cat II & III
4.3.2	Install and enable anti-spyware software. 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	Cat I	Cat II & III
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	Cat I	Cat II & III
4.5.1	Systems must be set up in a protected network environment or by using a method that assures the system is not accessible via a potentially hostile network until it is secured.	Required	Recommended
4.5.2	Operating system and application services security patches should be installed expediently and in a manner consistent with change management procedures.	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 Category-I data should implement secure (that is, encrypted) communications as required by confidentiality and integrity needs. (See Data Encryption Guidelines .)	Required	Recommended

Minimum Security Standards for Systems

Document Version: Approved

#	Practice		
4.5.7	Systems will provide secure storage for Category-I data as required by confidentiality, integrity, and availability 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
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-) writable 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	Recommended
4.5.13	Strong password requirements will be enabled, as technology permits, based on the category of data the account is allowed to access .	Required	Required
4.5.14	Apply the principle of least privilege to user, administrator, and system accounts.	Required	Recommended

4.6. Security Monitoring

#	Practice	Cat I	Cat II & III
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, etc.). Security logs should retain at least 14 days of relevant log information (data retention requirements for specific data should be considered).	Required	Recommended
4.6.4	All administrator or root access must be logged.	Required	Recommended

5. Security Review for New Security Software and Appliances

Departments evaluating the implementation of new security software or appliances, involving **Category-I** 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 **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 these standards may result in revocation of system or network access, notification of supervisors, and reporting to the Office of Internal Audit.

University of Texas at Austin 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, University of Texas at Austin employees are required to comply with state laws and regulations.

7. Related UT Austin 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.)

[Information Resources Use and Security Policy](#)

[UT Austin Acceptable Use Policy](#)

[UT Austin Data Classification Standard](#)

[UT Austin Information Security Exception Process](#)

8. Revision History

Version	Date	New	Original
Minimum Security Standards for Systems	3/1/2011	Converted web page to PDF. Updated numbering in tables to Level 3 numbers (4.4.1, 4.4.2, etc).	Tables were originally numbered 4.1, 4.2, etc.
	10/14/2009	Added a reference to the Minimum Security Standards for Systems Worksheet.	

Minimum Security Standards for Systems

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.	
	3/19/2009	Updated section 3.2 to improve the clarity of the standard.	"Anti-spyware software must be installed and enabled if the machine is used by administrators to browse Web sites not specifically related to the administration of the machine. In addition, anti-spyware software must be installed if users are able to install software. "
	9/14/2007	Changed reference from BPM 53 to UTS 165	"BPM 53"
	4/5/2007	Added "(See Data Encryption Guidelines.)" to System Hardening standards 5.6 and 5.7.	No reference previously.
	3/6/2007	<p>Changed Section I, first sentence to read "These minimum standards serve as a supplement to the IT Security Operations Manual, which was drafted in response to Texas Administrative Code 202 and UT System BPM 53."</p> <p>Added "This minimum standard exists in addition to all other university policies and federal and state regulations governing the protection of the university's data." to the end of the same paragraph.</p> <p>Also revised all references to "standard" to read "standards."</p>	"This minimum standard serves as a supplement to the IT Security Operations Manual, The University of Texas at Austin's implementation of UT-System BPM 53."

Version	Date	New	Original
	12/02/2006	Added practice 5.14: "Apply the principle of least privilege to user, administrator, and system accounts." Cat I: Required; Cat II/III: Recommended	New
	11/02/2006	Edited Practice 5.7 to say "Systems will provide secure storage for Category-I data as required by confidentiality, integrity, and availability needs. Security 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."	Systems will provide secure (that is, encrypted) storage for Category I data as required by confidentiality and integrity needs.
	10/20/2006	Edited Practice 5.6 to say "Services or applications running on systems manipulating Category I data should implement secure (that is, encrypted) communications as required by confidentiality and integrity needs."	"Services or applications running on systems manipulating Category I data should implement secure (that is, encrypted) communications to ensure Category I data does not traverse the Internet in clear text."
	10/20/2006	Added Practice 5.13, "Strong password requirements shall be enabled, as technology permits, based on the category of data the account is allowed to access ." Required for all data categories.	New

Minimum Security Standards for Systems

Document Version: Approved

Version	Date	New	Original
	7/11/2006	<p>Changed title to "Minimum Security Standards for Systems" in this and all documents referencing the title. The phrase "Associated with Category I, II, or III Data" relates to all IT Security policies, and the change will make it easier to incorporate "Minimum Security Standards" documents for other IT resource types.</p> <p>Added links to appropriate definitions in the ISO Technical and Security Glossary.</p> <p>Added Change Log for transparency.</p>	"Minimum Security Standards for Systems Associated with Category I, II, or III Data."
	7/11/2006	<p>Added the Exception Reporting Process to this sentence...</p> <p>"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.</p>	"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."
	7/11/2006	<p>Changed "Primary Investigators" to "Lead Researchers," per BPM-75 language.</p>	"IT owners and custodians, Primary Invesigators (PIs), and/or systems administrators are expected to use their professional judgment in managing risks to the information and systems they use and/or support."

9. Approvals

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