THE UNIVERSITY OF TEXAS AT DALLAS
INFORMATION SECURITY

Minimum Security Standards for Systems Associated with Category I, II, or III Data

Effective Date: March 17, 2007

Purpose

Scope

Audience

Minimum Standard

Security Review for New Security Software and Appliances

Non-Compliance and Exceptions

Related UT Dallas Policies, Procedures, Best Practices and Applicable Laws

I. Purpose

This minimum standard serves as a supplement to IR Security Operations Manual, The University of Texas at Dallas' implementation of UT-System UTS 165. Adherence to the standard will increase the security of systems and help safeguard university information technology resources.

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

II. Scope

This standard applies to all devices, physical or virtual, connected to the university network through a physical, wireless, or VPN connection where data is classified as Category I, II, or III (see Data Classification Standards).

III. Audience

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

IV. Minimum Standard

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. Information Resources owners and custodians, Primary Investigators (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. All security controls should be proportional to the confidentiality, integrity, and availability requirements of the data processed by the system.

Backups

#	Practice	Cat I	Cat II & III
1.1	System administrators should establish and follow a procedure to carry out regular system backups.	Required	Recommended
1.2	Backups must be verified at least monthly, either through automated verification, through customer restores, or through trial restores.	Required	Recommended
1.3	Systems administrators must maintain documented restoration procedures for systems and the data on those systems.	Required	Recommended

Change Management

#	Practice	Cat I	Cat II & III

2.1	There must be a change control process for systems configuration. This process must be documented.	Required	Recommended
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

Computer Virus Prevention

#	Practice	Cat I	Cat II & III
3.1	Anti-virus software must be installed and enabled.	Required	Required
3.2	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.	Recommended	Recommended
3.3	Anti-virus and, if applicable, anti-spyware software should be configured to update signatures daily.	Required	Recommended
3.4	Systems administrators should maintain and keep available a description of the standard configuration of anti-virus software.	Required	Recommended

Physical Access

#	Practice	Cat I	Cat II & III
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
4.2	Backup media must be secured from unauthorized physical access. If the backup media is stored off-site, it must be encrypted.	Required	Recommended

System Hardening

#	Practice	Cat I	Cat II & III
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
5.2	Operating system and application services security patches should be installed expediently and in a manner consistent with change management procedures.	Required	Required
5.3	WSUS is the preferred method for updating Windows systems. If this is not used and if automatic notification of new patches is available on the operating system you are running, that option should be enabled.	Required	Required
5.4	Services, applications, and user accounts that are not being utilized should be disabled or uninstalled.	Required	Recommended
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
5.6	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.	Required	Recommended
5.7	Systems will provide secure (that is, encrypted) storage for Category I data as required by confidentiality and integrity needs.	Required	Recommended
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
5.9	Integrity checking of system accounts, group memberships, and their associated privileges should be enabled and tested.	Required	Recommended

5.10	The required University warning banner should be installed.	Required	Required
5.11	Whenever possible, all non-removable or (re-) writeable media must be configured with file systems that support access control.	Required	Recommended
5.12	Access to non-public file system areas must require authentication.	Required	Recommended

Security Monitoring

#	Practice	Cat I	Cat II & III
6.1	If the operating system comes with a means to log activity, enabling and testing of those controls is required.	Required	Recommended
6.2	Operating system and service log monitoring and analysis should be performed routinely. This process should be documented.	Required	Recommended
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
6.4	All administrator or root access must be logged.	Required	Required

Data Disposal

#	Practice	Cat I	Cat II & III
7.1	If the data resides on electronic media (disks, tapes, hard drives, USBs, PDAs, etc.), the data must be rendered unrecoverable or indecipherable. This can be accomplished by shredding the media (UTD has a certified contract for this process), for example: any device that is sent to surplus must have the disk removed and shredded before being shipped off-site. Any media that is being repurposed, for instance, transferred to another person or department, must	Required	Required

	have a Department of Defense level reformat (wipe) performed on the media.		
7.2	Records must be maintained according to the UTD Records Retention Policy	Required	Required.

V. Security Review for New Security Software and Appliances

Departments evaluating the implementation of new security software or appliances, involving **Category I** type data, must 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.

VI. 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 this standard may result in revocation of system or network access, notification of supervisors, and reporting to the Office of Internal Audit.

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

VII. Related UT Dallas 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 resources.)

UTD Information Resources Security Operations Manual

UTD Acceptable Use Policy

UTD Data Classification Guidelines

UTD Information Security Exception Process