UTSA Institutional Compliance
Office of Information Security

OIS 21 – Standard for Minimum Security for Computer Systems

I. STANDARD STATEMENT

Adherence to this standard will increase the security of systems and help safeguard UTSA information technology resources. These minimum standards exist in addition to all other university policies and federal and state regulations governing the protection of university data.

Compliance with these requirements does not imply a completely secure system.

II. RATIONALE

This standard supports HOP Policy 8-12 Information Resources Use and Security Policy

III. SCOPE

This standard applies to all UTSA faculty, staff, and students.

IV. CONTACTS

The Office of Information Security
informationsecurity@utsa.edu

V. PROCEDURES

A. Minimum Standards
   1. 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 UTSA network. Standards for Category I are generally required.
   2. 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.
   3. Data Owners and Data Custodians, lead researchers, and/or system 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.

B. Backups

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

C. Change Management

Practice	Cat I	Cat II & III
There must be a change control process for systems configuration. This process must be documented.	Required	Recommended
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

D. Computer Virus Protection

Practice	Cat I	Cat II & III
Anti-virus software must be installed and enabled.	Required	Required
Install and enable anti-spyware software. Installing and enabling anti-spyware software is required if the machine is used by	Recommended	Recommended

administrators to browse Web sites not specifically related to the administration of the machine.		
Anti-virus and, if applicable, anti-spyware software should be configured to update signatures daily.	Required	Recommended
Systems administrators should maintain and keep available a description of the standard configuration of anti-virus software.	Required	Recommended

E. Physical Access

Practice	Cat I	Cat II & III
Systems must be physically secured in racks or areas with restricted access. Portable devices shall be physically secured if left unattended.	Required	Recommended
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

F. System Hardening

Practice	Cat I	Cat II & III
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
Operating system and application services security patches should be installed expediently and in a manner consistent with change management procedures.	Required	Required
If automatic notification of new patches is available, that option should be enabled.	Required	Required
Services, applications, and user accounts that are not being utilized should be disabled or uninstalled.	Required	Recommended
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

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
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.	Required	Recommended
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
Integrity checking of system accounts, group memberships, and their associated privileges should be enabled and tested.	Required	Recommended
The required university warning banner should be installed.	Required	Recommended
Whenever possible, all non-removable or (re-) writable media must be configured with file systems that support access control.	Required	Recommended
Access to non-public file system areas must require authentication.	Required	Recommended
Strong password requirements will be enabled, as technology permits.	Required	Required
Apply the principle of least privilege to user, administrator, and system accounts.	Required	Recommended

G. Security Monitoring

Practice	Cat I	Cat II & III
If the operating system comes with a means to log activity, enabling and testing of those controls is required.	Required	Recommended
Operating system and service log monitoring and analysis should be performed routinely. This process should be documented.	Required	Recommended
The systems administrator must follow a documented backup strategy for security logs (for example, account management, access	Required	Recommended

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).		
All administrator or root access must be logged.	Required	Recommended

H. Security Review for New Security Software and Appliances

Departments evaluating the implementation of new security software or appliances, involving Category I data, should request a security review by sending a written description of the proposed implementation to the Office of Information Security (OIS) 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.

I. Non-compliance and Exceptions

1. For all system administrators—if any of the minimum standards contained within this document cannot be met on systems manipulating Category I or Category II data that you support, an Exception Process must be initiated that includes reporting the non-compliance to OIS, along with a plan for risk assessment and management. 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.
2. UTSA 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, UTSA employees are required to comply with state laws and regulations.

J. Related UTSA 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.)