



Information Resources Security Operations Manual

[1. Overview](#)

[2. Audience](#)

[3. Acceptable Use](#)

[4. Account Management](#)

[5. Administrative/Special Access](#)

[6. Backups](#)

[7. Change Management](#)

[8. Computer Virus Prevention](#)

[9. E-mail](#)

[10. Incident Management](#)

[11. Incidental Use](#)

[12. Internet Use](#)

[13. Information Services Privacy](#)

[14. Network Access](#)

[15. Network Configuration](#)

[16. Passwords](#)

[17. Physical Access](#)

[18. Portable Computing and Remote Access](#)

[19. Security Monitoring](#)

[20. Security Training](#)

[21. System Hardening](#)



[22. Software Licensing](#)

[23. Enterprise Development and Deployment](#)

[24. Vendor Access](#)

[25. Disciplinary Actions](#)

1. Overview

The Information Resources Security Operations Manual provides guidance and defines procedures relating to the operational implementation of the *Information Resources Use and Security Policy*, as well as *UT System UTS-165*. For ease of reference both documents share the same organizational structure and a common table of contents. These two documents along with *Information Resources Acceptable Use Policy* comprise the policy and procedures foundation for the University of Texas at Dallas computer security program.

Technical terms referred to in this document are defined in the Glossary.

Last Reviewed: April 12, 2007

Last Edited: April 12, 2007

[Back to top](#)

2. Audience

The Information Resources Security Operations Manual provides guidance for all individuals that have, or may require, access to University of Texas at Dallas information technology resources and those with responsibility for maintaining these resources at the University of Texas at Dallas. All University of Texas at Dallas colleges, schools, and business units are required to comply with the policy statements instituted by UT System and The University of Texas at Dallas.

[Back to top](#)

3. Acceptable Use

Before an individual is provided access to a University of Texas at Dallas technology resource, he or she must acknowledge the *Information Resources Acceptable Use Policy*.

[Back to top](#)



4. Account Management

Proper management and use of computer accounts are basic requirements for protecting the University of Texas at Dallas information technology resources. All account passwords are to be constructed and managed in accordance with the University of Texas at Dallas password requirements included in this manual and the Acceptable Use Policy. The following account management practices are required:

- All accounts that access non-public University of Texas at Dallas information technology resources must follow an account creation process. This process must associate the individual with the account, the purpose the account was created for, and who approved the creation of the account. All accounts wishing to access non-public university information technology resources must have the approval of the owner of these resources. These measures also apply to accounts created by/for use of outside vendors (see Section 24). For employees and affiliates of UTD, this is accomplished by filling out a Computer Account Request form that includes a sponsor and approval by the appropriate Dean or Department Head. Approval by the Owner of the information for the assigned access to information technology resources for the position and duties of the individual is necessary for administrative applications.
- All Users are required to sign the following agreements annually:
 - Non-Disclosure Acknowledgment
 - Information Resources Use and Security Policy
 - Information Resources Acceptable Use Policy
 - Family Education Rights and Privacy Act
- Each account must adhere to the University of Texas at Dallas password requirements (see [Section 16](#))
- All accounts that are used for local administration of computers must be associated with an individual or group of individuals that are authorized to use that account and must be approved by Information Security (see the Security Exception Request).
- Accounts with access to administrative applications that have not been accessed for more than 30 days will be disabled.
- Accounts of individuals who have had their status, roles, or affiliation with the university change must be updated to reflect their current status.



- Accounts must be reviewed annually to ensure their current status is correct.
- Password aging and expiration dates must be enabled, where supported by the underlying account mechanism, on all accounts.
- Documented justification for deviations from the minimum expectations is required (see the Security Exception Request).

[Back to top](#)

5. Administrative/Special Access

All users of administrative/special access accounts must be made aware of the privileges granted to their accounts, especially those that could impact access to information technology resources or that allow them to circumvent controls in order to administer the information resource. Abuse of such privileges will not be tolerated. Anyone using accounts with privileges of this type must adhere to the following access requirements.

- Individuals that use accounts with special privileges must use these accounts only for their intended administrative purposes.
- Individuals that use accounts with special privileges may **only** perform investigations relating to potential misuse of information technology resources by an individual user under the direction of the Chief Information Security Officer.
- The University of Texas at Dallas departments must submit a list of administrative contacts to the Information Security Office for any systems connected to the University of Texas at Dallas network.
- All individuals whose accounts have special privileges must complete a Position of Special Trust form that acknowledges the responsibilities associated with those privileges.
- Each account used for administrative/special access must adhere to the UTD password requirements, including semi-annual expiration (see [Section 16](#)).
- The password for a shared administrator/special access account must change when any individual knowing the password leaves the department or the University of Texas at Dallas, or changes role, or upon a change in the vendor personnel assigned to the University of Texas at Dallas contracts.
- For all systems serving out information technology resources, there must be a password escrow procedure in place to enable someone other than the



administrator to gain access to the system in an emergency situation.
Individual user passwords are not escrowed.

- When special privileges are needed for auditing, software development, software installation, or other defined need, they:
 - Must be authorized by the appropriate department or entity.
 - Must be created with an expiration date, when supported by the system.
 - Must be removed or disabled when work is complete.

[Back to top](#)

6. Backups

Backups are a business requirement to enable the recovery of data and applications in the case of events such as natural disasters, system disk drive failures, espionage, data entry errors, human error, or system operations errors. The University of Texas at Dallas requires the following backup practices, as warranted by the *Data Classification Standards*:

- The information resource data or server owner is responsible for having a backup procedure in place for that resource.
- The server owner and data owner are responsible for determining and establishing the operational responsibility for backup for a server connected to the UTD network based on the *Data Classification Standards* and a risk assessment.
- Each department or entity responsible for a server(s) maintains a recovery plan that includes the following:
 - Requirements for off site storage.
 - Physical access controls for onsite and offsite storage.
 - Processes to ensure backups can be recovered.

The University of Texas at Dallas Office of Internal Audit periodically reviews the backup and recovery plans.

[Back to top](#)

7. Change Management



The information technology resources infrastructure at the University of Texas at Dallas is constantly changing and evolving to support the mission of the organization and its departments. Computer networks, servers, and applications require planned outages for upgrades, maintenance, and fine-tuning. To ensure reliable and stable operations, change management controls are required and will be enforced across all departments. The following change management procedures are required:

- All changes to applications and infrastructure within the production environment must be formally managed, logged, evaluated and authorized prior to implementation and reviewed against planned outcomes following implementation to reduce the risks of negatively impacting the stability or integrity of the production environment.
- The institution shall communicate and enforce enterprise change management and testing policies and procedures to handle all requests (including maintenance and patches) for changes to applications, system and service parameters, and the underlying platforms that have an impact on operations and financial reporting. These procedures will ensure that:
 - All requests for change are documented, categorized, prioritized and evaluated for impacts on the operational system and its functionality. This evaluation should include categorization and prioritization of changes. Prior to migration to production, changes are authorized by the appropriate stakeholder.
 - All requests for change are tracked in a system that allows for keeping change requestors and relevant stakeholders up to date about the status of the change to applications, procedures, processes, system and service parameters, and the underlying platforms.
 - Approval of the change is documented and testing documents are retained.
 - Testing changes occur in a separate test environment and programmers do not have update access to the production environment.
 - When changes are made by third parties or vendors, the audit trails and processes are formally reviewed.
 - Associated system and user documentation and procedures are updated whenever system changes are implemented.



- Changes are reviewed to ensure complete implementation.
- Any deviations from these procedures are approved and documented.
- The procedures shall also include a process for defining, requesting, assessing and authorizing emergency changes that do not follow the established change process. Documentation and testing should be performed even if this occurs after implementation of the emergency change.

[Back to top](#)

8. Computer Virus Prevention

A variety of technologies and practices are required to protect the University of Texas at Dallas network infrastructure and other information technology resources from threats posed by computer viruses, worms, and other types of hostile computer programs.

- Each responsible department or individual must install current virus protection software on all University of Texas at Dallas computers on the University of Texas at Dallas network. Exceptions may be requested by completing a Security Exception Request.
- E-mail gateways must utilize properly maintained e-mail virus protection software.
- Any computer identified as a security risk due to lack of virus protection may be disconnected from the network or the respective network access account may be disabled until adequate protection is in place.

[Back to top](#)

9. E-mail

Electronic mail (E-mail) is an essential tool for communicating within the University of Texas at Dallas. It is important that unimpeded e-mail services be available at all times and that e-mail be used in a manner that achieves its purpose without exposing the University of Texas at Dallas to unnecessary technical, financial, or legal risks. The following practices are required:

- All e-mail is subject to logging and review.



- To reduce spam and protect the e-mail environment from malicious viruses, worm or other threats, Information Resources (IR) may filter, block, and/or strip potentially harmful code from messages.

[Back to top](#)

10. Incident Management

Incident management is needed to assure continued operations in the event of a security breach or incident involving a computer virus, worm, attack against university information systems, or misuse of information technology resources. The Information Security Office is required to establish and follow Incident Management Procedures to ensure that each incident is reported, documented and resolved in a manner that restores operation quickly and if required, maintains evidence for further disciplinary, legal, or law enforcement actions. The following standard operating procedure will be followed:

- The University of Texas at Dallas will have a Computer Incident Response Team (CIRT) that, in the event of a computer security incident, will initiate and follow the Incident Management Procedures. The members of this team will have defined roles and responsibilities which, based on the severity of the incident, may take priority over normal duties.
- The Information Security Office will report the incident to the appropriate university, state, and federal agencies and departments as required by governing laws, rules, and procedures.
- Information Security Office, working with the selected CIRT members, will determine if a widespread University of Texas at Dallas communication is required, the content of any such communication, and the method of distribution. The Office of the Vice President for Communications will handle any communications to the general public.
- The Chief Information Security Officer will be responsible for maintaining a chain of evidence on incidents it investigates, or participates in investigating, in case the incident needs to be referred to law enforcement or other legal proceedings.
- The Information Security Office is responsible for determining the physical and electronic evidence to be gathered as part of the incident investigation, except in cases involving appropriate law enforcement personnel, where the University



Police Department or other law enforcement agencies will make these determinations.

- Technical staff, from the CIRT led by the Chief Information Security Officer, are responsible for ensuring that any damage from a security incident is repaired or mitigated and that the vulnerability is eliminated or minimized.
- The Information Security Office is responsible for communicating new issues or vulnerabilities to vendors as needed, and for working with the vendors to eliminate or mitigate the vulnerabilities.
- The Information Security Office is responsible for initiating, completing, and documenting the incident investigation with assistance from the CIRT
- The Chief Information Security Officer serves as liaison with the UTD Police Department and other law enforcement organizations.

[Back to top](#)

11. Incidental Use

Incidental personal use by University of Texas at Dallas affiliates of Information technology resources is permitted per the *Information Resources Acceptable Use Policy*. Information Resources or the appropriate department or entity is permitted to monitor the incidental personal use of information technology resources to ensure that:

- Use is restricted to only those individuals granted access.
- Use does not result in a direct cost to The University of Texas at Dallas.
- Use does not expose The University to unnecessary risks.

[Back to top](#)

12. Internet Use

The University of Texas at Dallas network Users must adhere to prudent and responsible Internet practices to mitigate risks associated with the Internet. The following practices are required:

- Software and operating systems utilizing the university network are expected to be kept up to date and to have features that enhance network security enabled.



- Content on all University of Texas at Dallas departmental Web sites must relate to university business, research, service, and/or academics and must be approved by the appropriate department or entity publishing the information.
- Purchases for the University of Texas at Dallas handled via the Internet are subject to the University of Texas at Dallas procurement rules.
- Personal commercial advertising may not be posted on University of Texas at Dallas Web sites.
- All confidential, personally identifiable, protected health information, certain financial data, or certain student data transmitted over any network must be encrypted in accordance with Data Classification Standards published by Information Security.

[Back to top](#)

13. Information Services Privacy

To manage systems and enforce security, the University of Texas at Dallas may log, review, and otherwise utilize any information stored on or passing through its information resource systems in accordance with the provisions and safeguards provided in the [Texas Administrative Code 202.1-8](#), Information Resource Standards.

In cases of suspected abuse of information technology resources, the contents of any e-mail or file may be reviewed by the Chief Information Security Officer in accordance with provisions defined in Disciplinary Actions (see [Section 25](#)).

Access to data and information associated with such actions will be handled using standards of privacy and confidentiality required by law and university policy.

[Back to top](#)

14. Network Access

Access to the network is managed to ensure the reliability of the network and the integrity and appropriate use of information contained within the network. The following network access procedures are required:

- Only network addresses issued by University of Texas at Dallas may be used on the University of Texas at Dallas network.



- No network hardware (router, switch, hub, firewall, wireless access point, or other network appliance) may be installed on the University of Texas at Dallas network without prior approval of IR and Network Services.
- Systems attaching to the university network must operate in a manner that poses no internal/external security or operational hazard. Owners of systems that do not meet these criteria must cooperate fully with university staff in correcting the problems.
- To ensure compatibility with the University of Texas at Dallas network, all computers, PDAs and office productivity software purchased by the University of Texas at Dallas should adhere to system standards endorsed by IR.

Network Security Information

- All wireless access requires user authentication, only users with UTD authorized network accounts can access the wireless networks.
- All wired access requires registration with IR, including MAC address and asset tag number.
- All devices requiring public addresses must have prior approval from IR, must be registered in the Server Registry and must comply with all UTD IR security policies, including those pertaining to patching and anti-virus protection.
- Unauthorized devices are subject to immediate removal from the network without prior notice.

[Back to top](#)

15. Network Configuration

The University of Texas at Dallas and Networking staff manages the network infrastructure, which includes all cabling and connected electronic devices, to ensure reliability of operations, proper accessibility to resources, and protection of data integrity.

Network and Telecommunications Services:

- Will operate and maintain a reliable network with appropriate redundancies to meet quality of service goals.
- Is responsible for maintaining a list of hosts and parties responsible for those hosts, which are connected to the university network.



- Must install or authorize a contractor to install all cabling and network hardware.
- Approve the specification used to configure all equipment connected to the University of Texas at Dallas network.
- Has the authority over changes to the configuration of active network management devices.
- Sets all protocols and standards used on the University of Texas at Dallas network with input and direction from Information Security.
- Is responsible for all connections of the network infrastructure to external third party data and telephony networks.
- Must install, configure, and maintain the University of Texas at Dallas network firewalls.
- Provides written authorization for the use of departmental firewalls. Their use is not permitted without written authorization.

Information Security:

- All hosts attached to the university network may be scanned by the Information Security Office for potential vulnerabilities without prior notice.

[Back to top](#)

16. Passwords

Strong passwords are required on University of Texas at Dallas accounts. All passwords must be constructed, implemented, and maintained according to the following, as technology permits:

- Passwords for accounts associated with Category I, II & III data types (see Data Classification Standards):
 - Must:
 - Be at least 8 characters in length.
 - Contain at least 3 of the following within the first 8 characters: upper case letters, lower case letters, numbers, and special characters (e.g. ! @ # \$ % & * () - + = < >)
 - Be changed semi-annually.
 - Must not:



- Include personal information such as your name, phone number, social security number, date of birth, or addresses.
 - Contain words found in a dictionary
 - Re-use any of your last 6 passwords
 - Contain a series of the same character
 - Contain your UTD-ID or NetID.
- *University identity credentials (that is, security tokens, smartcards, and other access and identification devices) must be disabled or returned to the appropriate department or entity on demand or upon termination of the relationship with the University of Texas at Dallas. Additional operating guidelines for university ID cards are referenced in the University Comet Card FAQ.*
 - All systems should be configured to allow users to change their own passwords upon demand without third-party involvement.
 - Password requirements must be followed by everyone, including those with special privileges.
 - Unattended computing devices must be secured from unauthorized access. Physical security options include barriers such as locked doors or security cables. Logical security options include screen saver passwords and automatic session time-outs. See the Information Resources policies.

[Back to top](#)

17. Physical Access

The granting, controlling, and monitoring of physical access is an important component of the overall security program:

- All information technology resource facilities must be physically protected in proportion to the criticality, and confidentiality of their function at The University of Texas at Dallas.
- All information technology resources facilities must have physical access controls in proportion to the importance, sensitivity, and accountability requirements of the data and systems housed in that facility.



**THE UNIVERSITY OF TEXAS AT DALLAS
INFORMATION SECURITY**

- Access to information technology resource facilities will only be granted to authorized personnel of The University of Texas of Dallas and other contractors or personnel whose job responsibilities require such action.
- Access cards and/or keys must not be shared or loaned to others.
- Access cards, and/or keys, and badges that are no longer required must be returned to the responsible department contact and campus key management must be notified immediately for deactivation of access. All returned access cards must be forwarded to the responsible campus key management or ID center contact as soon as possible. Cards must not be reallocated to another individual, thereby bypassing the return process.
- Lost or stolen access cards and/or keys must be reported to the appropriate department and campus key management as soon as possible.
- Information technology resources facilities access and log records are the responsibility of the department that manages the facility. Such records will be kept in accordance to the accountability requirements of the data and systems in that facility.
- The department in charge of information technology resources facilities must be notified immediately if individuals who had access to these facilities should no longer need access due to a change in roles, completion of contract or other cause that negates their need for further access.
- Visitors must be escorted in controlled areas of information technology resources facilities.
- The appropriate department, entity or a designee must review access records for secured information technology resource facilities at least every two weeks and investigate any unusual access.
- The appropriate department, entity or a designee must review card and/or key access rights for secured information technology resource facilities on a quarterly basis and remove access for individuals that no longer require access.
- Signage for restricted access rooms and locations must be practical. Minimal discernible evidence of the importance of the location should be displayed.

[Back to top](#)



18. Portable Computing and Remote Access

Computers and devices used to access the University of Texas at Dallas infrastructure must do so in a manner that preserves the integrity, availability, and confidentiality of the University of Texas at Dallas information.

All remote users must comply with the Minimum Security Standards for Systems Associated with Category I, II, or III Data as published by Information Security.

Refer to the *University of Texas at Dallas Encryption Practices for Mobile and Personally Owned Computer Devices* for more information on requirements for protecting portable devices.

[Back to top](#)

19. Security Monitoring

Security monitoring is used for confirming security practices and controls in place are being adhered to and are effective. It is also used in identifying anomalous activity that might be an indication of an operation or security concern. Monitoring consists of activities such as automated notification of security breaches and automated or manual examination of logs, controls, procedures and data. The following monitoring requirements apply to information technology resources at the University of Texas at Dallas:

- Operating system user accounting and application software audit logging processes will be enabled on host and server systems.
- Alarm and alert functions of any firewalls and other network perimeter access control systems must be enabled.
- Audit logging of any firewalls and other network perimeter access control systems must be enabled.
- Information technology resources connected to the university network are subject to automated monitoring and notifications of possible security events of interest by the Information Security Office.
- Any security issues discovered will be reported to the Information Security Office and appropriate executive officials via the Security Incident Report Form (see Section 25).

[Back to top](#)



20. Security Training

Information Security is charged with providing a combination of general computer security awareness programs and training.

- All users of the University of Texas at Dallas information technology resources will be provided with training and supporting materials to allow them to properly protect the information technology resources they use.
- Introductory security awareness training will be performed at employee and student orientation classes.
- Recurring security awareness training for all faculty and staff will be offered annually (training to be arranged by the Compliance Office with input from Information Security).
- All users must acknowledge the Information Resources Acceptable Use Policy.
- Must prepare, maintain, and distribute information that concisely describes the University of Texas at Dallas Information security policies and procedures.
- Must develop and maintain a process to communicate new computer security program information, security bulletin information, and security items of interest to faculty, staff and students.
- Will provide specific security training to information technology professionals serving in positions of special trust (for example, system administrators).

[Back to top](#)

21. System Hardening

Systems are used to transmit information and services throughout the University of Texas at Dallas. Information and services must be transmitted securely and reliably to assure that data integrity, confidentiality, and availability are preserved. To achieve these goals, systems must be installed and maintained in a manner that minimizes service disruptions and prevents unauthorized access or use. The following standards apply:

- A system must not be connected to the University of Texas at Dallas network until it is in a secured state and location.
- All system installations must follow the Minimum Security Standards for Systems Accessing Category I, II, or III Data that provides detailed information required to harden a system. Exceptions may be requested by completing a



Security Exception Request. The following general steps are included in the Minimum Security Standards:

- Application of vendor supplied patches.
- Removal of unnecessary software, system services, and drivers.
- Setting of security parameters, file protections and enabling of audit logging in proportion to the importance, sensitivity, and accountability requirements of the data processed by the system.
- Disabling or changing of passwords associated with default accounts.
- Installation of appropriate intrusion detection and/or file integrity software.
- Departments are responsible for ensuring their systems have been properly specified, configured, installed and properly maintained.
- The responsible department or entity tests security patches before installation, where technically feasible.
- All departments or entities must implement security patches in a timely and appropriate manner.
- The responsible department or entity will periodically examine all systems, in proportion to data sensitivity. System administrators must maintain an inventory of systems, operating system versions in use, critical software and versions that are used, as well as the last time patches were applied. System administrators will also be expected to monitor security mailing lists, and other information sources, for vulnerabilities concerning their operating systems and software.

[Back to top](#)

22. Software Licensing

All software used on the University of Texas at Dallas computers will be used in accordance with the applicable software license:

- Systems administrators have the right to remove software from the University of Texas at Dallas computers for cause. For example, if a user is unable to show proof of license, or if the software is not required for university business purposes and causes problems on the university owned computer.



- All responsible departments or entities will periodically audit all computers to inventory all installed software.
- All University of Texas at Dallas departments are responsible for the accurate accounting of software purchased by the department and must ensure that the installation of the software complies with the license agreement of the software.

[Back to top](#)

23. Enterprise Development and Deployment

The protection of information technology resources (including data confidentiality, integrity, and accessibility) must be considered during development or purchase of new enterprise computer applications.

- Departments or entities are responsible for developing, maintaining and participating in quality assurance/project management practices as appropriate for projects of varying scope, cost and risk (see Quality Assurance Plan).
- During the development of an application the data owner, data custodian and system administrator must be identified.
- All production systems and applications must follow the Information Resources Information Security standards for granting access and must provide methods for appropriately granting privileges of authorized users. User access to applications is granted on a need-to-access basis.
- Whenever possible, new development or modifications to a production system will be made first in a development test environment.

[Back to top](#)

24. Vendor Access

Vendors serve an important function in the support of hardware and software and in some cases possibly even the operations of computer networks, servers, and/or applications.

- Vendors must comply with the Information Resources Use and Security Policy (UTS-165), when information technology resources are involved, and any University of Texas at Dallas department engaging a vendor must provide the vendor with a copy of this policy and any other procedures they must follow, including, but not limited to:



**THE UNIVERSITY OF TEXAS AT DALLAS
INFORMATION SECURITY**

- Safety
 - Privacy
 - Security
 - Auditing
 - Software licensing
 - Acceptable Use
- Vendors will adhere to Federal and State laws to which the University of Texas at Dallas must adhere.
 - Vendor agreements and contracts must specifically reference The Information Resources Use and Security Policy (UTS-165), The University of Texas at Dallas Acceptable Use Policy, and the Information Resources Security Operations Manual when information resources are involved.
 - Vendor agreements and contracts must address the following issues when information technology resources are involved:
 - The University of Texas at Dallas information the vendor may access.
 - The vendor's responsibility to protect the University of Texas at Dallas information.
 - The vendor's responsibility regarding the deletion, destruction, disposal or return of the University of Texas at Dallas information at the end of the contract.
 - The vendor's responsibility to use the University of Texas at Dallas information only for the purpose of the business agreement.
 - The University of Texas at Dallas, or respective department, right to audit and otherwise verify the security of university information and other resources in the possession of or being managed by the vendor and the university's right to investigate any security breaches involving these resources.
 - The University of Texas at Dallas, or respective department, right to require background checks for vendors working with security sensitive university information.
 - The University of Texas at Dallas will provide an information technology resources point of contact for the vendor. The point of contact will work with the vendor to make certain the vendor is in compliance with these policies.



**THE UNIVERSITY OF TEXAS AT DALLAS
INFORMATION SECURITY**

- Each vendor must provide the University of Texas at Dallas with a list of all employees working on the contract when information technology resources are involved. The list must be updated and provided to the University of Texas at Dallas within one business day of staff changes.
- The owner of the information has the right to approve or disapprove, for cause, any vendor employee having access to the University of Texas at Dallas sensitive or confidential information.
- Vendors must report all security incidents involving university resources to the University of Texas at Dallas Information Security Office.
- Each vendor must follow all applicable University of Texas at Dallas change management procedures approved by the appropriate department or entity.
- For contracts involving onsite work, regular work hours and duties will be defined in the contract. The appropriate department or entity must approve in writing work outside defined parameters.
- All vendor accounts and maintenance equipment connecting the University of Texas at Dallas network to the Internet or outside organizations will remain inactive except when in use for authorized maintenance.
- Vendor accounts providing access to the University of Texas at Dallas information technology resources must be uniquely identifiable and passwords must comply with the University of Texas at Dallas password requirements as detailed in this manual.
- Vendors must maintain a log of major work activities that is available to the University of Texas at Dallas management upon request. Logs may include such events as personnel changes, password changes, project milestones, deliverables, and arrival and departure times, as necessary for a given contract.
- Upon departure of a vendor employee from a University of Texas at Dallas contract for any reason, the vendor will ensure that the employee's access to all the University of Texas at Dallas sensitive and confidential information is removed within 24 hours in a manner agreed upon by the University of Texas at Dallas.
- Vendors are required to comply with all State of Texas and the University of Texas at Dallas auditing requirements, including the auditing of the work the vendor has done for the university.



- All software used by the vendor in providing service to the University of Texas at Dallas must be properly inventoried and licensed. Software provided by the University of Texas at Dallas installed on vendor equipment must be removed at the end of the contract.
- To protect the University of Texas at Dallas intellectual property information, technology vendor contracts must be in accordance with the Board of Regents' Rules and Regulations concerning intellectual property.

[Back to top](#)

25. Disciplinary Actions

Misuse or destruction of information technology resources can vary in severity and appropriate disciplinary actions should be taken in proportion to the severity of the incident. It is the role of Information Security professionals to consult with executive management on disciplinary actions as the result of an incident, to monitor resources, to identify potential incidents and to bring such incidents to the attention of appropriate University of Texas at Dallas officials. The following guidelines apply:

- Suspected incidents involving student, faculty, or staff misuse of information technology resources should be brought to the attention of the Information Security Office.
- If it is determined that a misuse violation may have occurred by a student, faculty, or staff member, this should be brought to the attention of the Information Security Office. The Information Security Office will consult with Human Resource Management or Student Judicial Services, as needed, and in the case of criminal violations, the University Police Department.
- Violations by non-affiliates will be referred to the appropriate authorities. The Office of General Counsel may be contacted to provide direction in terms of identifying the appropriate authority.
- Issues of departmental non-compliance may be reported to the respective executive management, the Office of Internal Audit, or the Office of the President.

[Back to top](#)