Policy Statement

Background

The University of Houston relies heavily on computers to meet its operational, financial, and information requirements. These computer systems, related data files and the information derived from them are important assets of the University. A system of internal controls exist to safeguard these assets. Information is processed in a secure environment and all computer account owners share the responsibility for the security, integrity, and confidentiality of information. It is the responsibility of owners, custodians and users to comply with the Texas Administrative Code, Title 1 (TAC 202), Gramm Leach Bliley Act (GLB Act), Family Educational Rights and Privacy Act (FERPA) and the Health Insurance Portability and Accountability Act (HIPAA). This policy covers both accidental and intentional disclosure of, or damage to, University information.

Scope

This policy statement applies to the security, integrity, and confidentiality, of information obtained, created, or maintained, by university employees. The definition of information, includes paper documents and all computer-related activities involving mainframes, micro and mini computers, and service bureaus.

Definitions

Owner/Program Manager

The owner of a collection of information is the person responsible for the business results of that system, or the business use of the information. In cases where information resources are used by more than one major business function, owners must reach consensus and advise the Information Security Officer as to the designated owner with responsibility for the information resources.

Custodian

The custodian is responsible for the processing and storage of the information. For mainframe, micro and mini applications, the owner or user may retain custodial responsibilities.

User

The user is any person who has been authorized to read, enter, or update information by the owner of the information.

Data

Information that is stored in any form by the university that is used as a basis for official reasoning, discussion, presentation, or calculation.

Information

Source documents, electronic data files, and any data or reports derived from them.

Responsibilities

Owner

Information processed by a computerized system must have an identified owner, and this assignment must be formally documented. The owner may delegate ownership responsibilities to another individual. The owner of information has the authority and responsibility to:

1. Judge the value of the information and classify it.
2. Authorize access and formally assign custody of information.
3. Specify data controls and communicate the control requirements to the custodian and users of the information.
4. Determine the statutory requirements regarding retention and privacy of the information, and communicate this information to the custodian.
5. Specify appropriate controls, based on risk assessment, to protect the state's information resources from unauthorized modification, deletion or disclosure. Controls shall extend to information resources outsourced by the University.
6. Confirm that controls are in place to ensure the accuracy, authenticity and integrity of data.
7. Ensure compliance with applicable controls.
8. Assign custody of information resources assets and provide appropriate authority to implement security controls and procedures.
9. Review access lists based on documented security risk management decisions.
10. Approve, justify, document and be accountable for exceptions to security controls. The information owner shall coordinate exceptions to security controls with the Information Security Officer.
11. The information owner, with the concurrence of the President (or designee) is responsible for classifying business functional information.

Custodian

The custodian is responsible for the implementation and administration of controls as specified by the owner. This includes:

1. Providing physical and technical safeguards.
2. Providing procedural guidelines for the users.
3. Administering access to information.
4. Assist owners in evaluating the cost-effectiveness of controls and monitoring.
5. Implement the monitoring techniques and procedures for detecting, reporting and investigating incidents.

User

A user of information has the responsibility to:

1. Use the information only for the purpose intended by the owner.

2. Comply with all controls established by the owner and custodian.
3. Ensure that classified or sensitive information is not disclosed to anyone without permission of the owner.
4. Ensure that his/her individual passwords are not disclosed to, or used by others.
5. Become familiar with and abide by the **General Computing Policies**.

Enforcement

A violation of standards, procedures or guidelines established pursuant to this policy shall be presented to Management for appropriate action and could result in disciplinary action, including expulsion, dismissal, and/or legal prosecution.

Information Security Officer (ISO) - Responsibilities

Reports To:

Vice Chancellor/Vice President for Information Technology (VC/VPIT).

Primary Functions

Develop and administer system and information ownership; information and data classification guidelines; standards and procedures. Develop, establish and maintain standards, procedures and guidelines to promote the security and uninterrupted operation of computer-based application systems at University of Houston. Identify and address exposures to accidental or intentional destruction, disclosure, modification, or interruption of information that may cause serious financial and/or information loss to University of Houston. Be responsible for the protection of the University of Houston assets and information which are processed by or stored in University of Houston computerized information systems.

Specific Duties

1. Manage the information security function in accordance with the established policies and guidelines.
2. Report to the Vice Chancellor/Vice President for Information Technology.
3. Establish and maintain information security standards and procedures in compliance with state information security and risk management policies, standards and guidelines.
4. Function as an internal consulting resource on information security issues.
5. Conduct the information security risk assessment program. Review compliance with the information security policy and associated procedures.
6. Coordinate information security efforts with the Internal Audit Department.
7. Provide periodic reporting on information security issues to the VC/VPIT.
8. Coordinate security orientation and security awareness programs.
9. Assist in coordinating contingency plan tests on a regular basis.

Information Security Officer - Administrator (ISA)

Primary Functions

Be responsible for providing security and risk management related support services.

Specific Duties

1. Provide assistance to the information security function relative to using the computer's security facilities.
2. Provide supervision to any technical and administrative personnel assigned to the computer security function.
3. Assist in the acquisition of security software and equipment.
4. Assist the information security function (if requested to do so) in developing and maintaining the security and risk management program, including a risk analysis process.
5. Assist in identifying vulnerabilities and the appropriate solutions to eliminate or minimize their potential effects.
6. Assist in developing and maintaining the access control rules within the security software that provides controlled access in accordance with owner defined information access requirements.
7. Serve as a member of software review committee to evaluate new software and hardware systems.
8. Provide periodic reporting on information security issues.
9. Investigate any actual or potential information security violations. Follow up investigations with written reports.
10. Assist management with training employees about information security issues.
11. Train any designated individuals to act as an ISA alternate, in case of emergency or absence.
12. Assist in ensuring that departments have fulfilled their security responsibilities.
13. Review new systems designs and major modifications for security implications prior to implementation.
14. Provide liaison with the Security function.
15. Consult on planned physical facilities changes, and alterations in work flow or operating procedures to evaluate the effect of such changes on security and safety.

Information Security Officer - Auditor

Primary Functions

Be responsible for performing periodically, based on risk assessment, an internal audit of the information security function.

Specific Duties

1. Examine the information security policies and procedures for compliance with state information security and risk management policies, standards and guidelines.
2. Examine the effectiveness of the information security policies and procedures; identify inadequacies within the existing security and risk management program and possible corrective action to be taken.
3. Review and evaluate the effectiveness of controls for automated information systems that are either under development or operational, with particular emphasis on major systems.
4. Inform management, the information security function and the information's owners, custodians, and users of its findings.
5. Participate in the risk analysis process.

Information Security Awareness Training and New Employee Orientation

All UH System employees are required to participate in ongoing Information Security Awareness Training required by the Texas Administrative Code, Title 1 (TAC 202) Family Educational Rights and Privacy Act (FERPA), Gramm Leach Bliley Act (GLB Act), and Health Insurance Portability and Accountability Act (HIPAA).

Purpose

To ensure that an adequate security training program is developed and administered.

Scope

University of Houston employees using corporate computers.

Guidelines

An Ongoing Information Security Awareness Training Course is exists for all University of Houston System employees administered by Human Resources in PeopleSoft covering such areas as:

- State and Federal Laws including:
  - Texas Administrative Code, Title 1, TAC 202
  - Gramm Leach Bliley Act (GLB Act)
  - Family and Educational Rights and Privacy Act (FERPA)
  - Health Insurance Portability and Accountability Act (HIPAA)
- Information security and password tips
- How to identify security and report incidents

A New Employee Orientation Training Program exists for all first-time users of UH System corporate computers:

- Organizational security policy--Corporate computing users are given a copy of the **General Computing Policies**.
- Security operating procedures--Corporate computing users are instructed in the proper use of the corporate systems available.
- Access control procedures--First-time employees using the corporate computing facilities are instructed in the proper use and protection of passwords.
- At the New User Orientation, each person is required to sign a statement that they have read, understand, and agree to comply with the **General Computing Policies**.

Information Ownership

Purpose

Provide a basis for determining who in the organization should control access to a particular item of information.

Scope

Corporate information produced, used or maintained by the University of Houston.

Standard

Information that is in a computer-based application has an owner identified for it, and is clearly identified and secured based on its permissions granted in the profile system.

Guidelines

1. Procedures should ensure privacy and confidentiality of information that might affect an individual's civil liberties, and ensure compliance with applicable privacy laws.
2. Measures must be in place to prevent misappropriation of or unauthorized access to proprietary or confidential programs that are leased or used under non-disclosure or protective agreements.
3. Systems development projects have formal checkpoints addressing output data access control throughout the system design effort.

Initial Risk Analysis

Purpose

To conduct a risk analysis for University of Houston information resources.

Scope

University of Houston information assets, and any process, facility, or equipment associated with the creation, processing, and retention of the information.

Standard

University of Houston should conduct a risk assessment program consisting of the following phases:

- Identification of assets.
- Estimation of asset values.
- Identification of threats.
- Identification of vulnerabilities.
- Calculation of risk.

Guidelines

Factors to consider when conducting a risk analysis include:

- How to manage the risk analysis program.
- What methodology to use.
- What data collection methods to use.
- When risk analysis should be conducted.
- What is to be presented to top management.

Risk Assessment

Purpose

1. Update the risk assessment based on changes which have occurred since the previous review.
2. Evaluate the continuing applicability of current policies, guidelines, standards and procedures.
3. Review periodically all non-compliance situations concerning security policy and practices.
4. Determine the appropriate recourse for each non-compliance situation.

Scope

All University of Houston information assets, all security related policies and procedures and any non-compliance situation identified by the Information Security Officer or management regarding any existing security policy.

Standard

At appropriate times, the Vice Chancellor/Vice President for Information Technology should review the updated risk assessment, proposed changes to policies and procedures and all non-compliance situations to assess the risk of each situation, and determine the appropriate recourse.

Guidelines

1. The Information Security Officer should conduct a periodic risk assessment review of the overall information systems environment, current policies, procedures, guidelines and standards and all incidents of non-compliance.

2. The risk assessment should be reviewed annually or whenever significant systems changes are implemented.
3. The revised risk assessment should be presented to the VC/VPIT for acceptance.
4. The revised policies, etc., should be presented to the VC/VPIT for formal approval.
5. Incidents of non-compliance should be brought to the attention of the VC/VPIT and one of two actions will be taken:

- The VC/VPIT should identify those policies which require mandatory compliance and determine the corrective measures to be taken to ensure compliance.
- The VC/VPIT should determine those policies where the cost of compliance outweighs the loss exposure. In either case, the VC/VPIT has the option to waive compliance to the policy and accept the risks.

Responsibilities - Vice Chancellor/Vice President for Information Technology (VC/VPIT)

Objective

The security-related objectives of the Vice Chancellor/Vice President for Information Technology are to provide the information security function with a clear direction that is in conformance with the standards, policies and procedures developed for information security at the University of Houston.

Purpose

The security-related purposes of the VC/VPIT are to:

- Provide the information security function with a mechanism for the review and approval of security implementation and administration policies.
- To oversee the risk acceptance program.
- To oversee security incident case handling.

Security-Related Authority and Functions

1. Review status reporting by the Information Security Officer monitoring effectiveness of the existing security program, enforcement of policy and standards, and recommending specific courses of action.
2. Review and approve the current and future plans for information security at University of Houston.
3. Recommend a course of action in cases involving security incidents.
4. Review and approve all non-compliance situations where assumption of risk is involved.
5. Review annual risk assessment program and bring significant issues to the attention of other executives as appropriate.

Central Corporate Computing Procedures

Purpose

To provide standard operating procedures related to information security for University of Houston.

Scope

All UH Information Technologies data processing facilities.

Standard

1. A Security Procedures Manual must be readily accessible to the shift supervisor and all data processing operating personnel.
2. The manual shall contain, at a minimum, procedures for:

- Telephone directory of important numbers.
- Moving data from Bull to VAX.
- System Services.
- Accounts Payable information.
- System password information.
- Production Library maintenance.
- Emergency shutdown procedures.
- Records retention.
- Fire safety.
- Direct deposit tape.
- Printer information.
- Daily production schedule information.
- Micro fiche.
- Personnel information. (shift sched, overtime, etc.)
- Magnetic tape certifying and initializing.
- Facility management.
- Database backup.
- Shift responsibility.
- VAX batch processing.
- Security.
- VAX commands.

- Equipment access.
- Distribution of output.
- TAPSYS information.
- Forms/printers/ribbons information.
- Check count verification.
- VCS console information.

3. And other policies and procedures deemed appropriate by the Vice Chancellor/Vice President for Information Technology (VC/VPIT) or the Information Security Officer (ISO).

Student Orientation

Purpose

To advise students of the information security policies and procedures at University of Houston.

Scope

All first-time student users of information resources at University of Houston.

Standard

All first-time student users of University of Houston's computerized information processing facilities are to receive guidelines on the information security policies and procedures.

Guidelines

1. Every first-time student must sign an account application form, available from Support Services, stating that he/she understands the University of Houston's security guidelines and agrees to comply with them.
2. A student account application form certifying completion of security orientation (including the student's signature) is retained on file in Support Services.

Rotation and Separation of Duties

Purpose

To define required separation and rotation of duties to minimize the risk of fraud.

Scope

University of Houston data processing employees and users of sensitive data.

Guidelines

1. Programming and operations functions must be performed by different individuals.

2. There should be cross training of operations staff to provide depth and backup, and to reduce individual dependence.
3. Any exception to the following guidelines regarding separation of duties for the following groups of employees should be documented and reviewed on a periodic basis for justification and risk analysis purposes:
   Programmers:

- Programmers should not execute jobs in a production mode.
- Programmers should not control any transfers between programmer development libraries and production libraries.
- Programmers should/may not have update capability within any production application.
  Operators:
- Operators should not have the ability to make changes to production application or system software libraries.
- Operators should not perform balancing activities, except those necessary for run-to-run controls.
- Operators should not have the ability to make changes to job control language (JCL) of scheduled jobs without proper notification and authorization.
- Operators should execute only those jobs/programs scheduled through the established procedures.
- Operators should not execute (outside of standard production processing) data or software-modifying system utilities without proper authorization and dual control.
- Operators should not override internal tape labels without supervisory approval.
  Users:
- Data entry personnel should not prepare source documents for input.
- Someone, other than the input operator, should verify all data input, unless programmatically verified.
- The same person should not perform input and output duties.
- The same person should not post and balance general ledger and other sensitive entries.
- The person who prepared the original transaction should not review rejects or non-reads for reentry.
- Master file and other sensitive transaction changes should be under dual control.

Computer Security Violation Reporting

Purpose

1. To ensure compliance with the Texas Administrative Code, Title 1, (TAC 202), Family Educational Rights and Privacy Act (FERPA), Gramm Leach Bliley Act (GLB ACT), Health Insurance Portability and

Accountability Act (HIPAA) and the policy which requires that all users of UH corporate computers shall have the affirmative obligation to report, directly and without undue delay to the Information Security Officer, any and all information concerning conduct which they know to involve corrupt or other criminal activity or conflict of interest, (1) by another University of Houston employee, which concerns his or her office of employment, or (2) non-University of Houston personnel whose activities involve the University of Houston.

2. To provide prompt notification to the ISO of computer abuse situations which may include:

- Violation of the integrity or confidentiality of student, financial or health information under TAC 202, FERPA, GLB ACT or HIPAA.
- Theft or diversion of the University of Houston funds, computational resources, or other assets contained in or controlled by its computer systems.
- Vandalism or other damage to University of Houston computer systems, computer programs or data.
- Unauthorized modification to (or use of) University of Houston computer systems, programs, or data contained in these systems.

Scope

Applies to all University of Houston employees.

Standard

Every employee who has knowledge of a computer abuse which has or may be occurring on a University of Houston computer processing system must inform an appropriate University of Houston official.

Guidelines

The following information should be gathered for each reported violation. The ISO is responsible for gathering this data, once he/she is initially contacted by the employee reporting the abuse. Information to collect includes:

1. Description of the abuse:

- Unauthorized use of computer time
- Modification/alteration of computer data files or programs
- Detection of non-University of Houston data or programs on a university computer system
- Forgery of negotiable instruments using a computer
- Theft of computer equipment Disclosure of computer systems password to unauthorized individual(s)
- Destruction of computer data files or programs
- Insertion/modification of input documents

2. Person(s) suspected of the abuse

- Name
- Social security number
- Date of birth
- Office title
- Work location
- Length of affiliation with University of Houston
- Office phone number
- Home address

3. Person(s) reporting/detecting abuse
   - Name
   - Office title
   - Office phone number
   - Work location
4. Evidence available to substantiate suspicion of abuse
   - Activity logs
   - Printouts
   - Negotiable instruments
   - Input documents
   - Computer media
   - Audit trails
   - Date(s) of the abuse
   - Location of the abuse situation
   - Any action taken in response to the reported abuse.

Data and Software Access Control

Purpose

To ensure that only authorized individuals are allowed access to data residing on computer systems.

Scope

University of Houston corporate computer systems that access confidential, sensitive, or critical data.

Standard

Software controls must ensure that data are available as needed only to authorized users, that legitimate users of the computer cannot access stored information unless they are authorized to do so, and that unauthorized individuals (whether inside or outside University of Houston) are prevented from accessing any data.

Users of the University of Houston corporate computers should be granted those access privileges to data and software to accomplish their authorized responsibilities.

Guidelines

1. An audit trail of all accesses to sensitive information should be maintained. This record should indicate who changed the information as well as the nature and date of the change.
2. If the available software is inadequate in controlling access to the information within the computer, access to the entire computer system should be restricted to those with permission to access the information.
3. On an annual basis, departments should review their employee's access to University information systems and applications and verify that each has the appropriate level of access to corporate data. Verified reports must be sent to and reviewed by the Information Security Officer.

Individual Accountability

Purpose

To ensure that any file/date modifying activity occurring on a University of Houston corporate computer system is traceable to the individual initiating it.

Scope

All shareable corporate computer systems under the control of the University of Houston.

Standard

A procedure will be in place for all computer systems to ensure that an individual uniquely identify himself/herself before gaining access to any computing resources.

Guidelines

1. Automated identification processes should involve providing the system with both a user identification and a confidential password.
2. All actions, either on-line or batch should be fully auditable to an individual.
3. This policy applies to activities by users and programmers.
4. Procedures are actively enforced to ensure that user I.D.s and passwords are removed from the system whenever that person is transferred to another position or leaves the organization.
5. Sign-on software does not allow one user to be signed on to more than one terminal. Exceptions may be allowed upon written permission of Support Services and the employee's manager.

6. If a decentralized administration approach is used, the ISO has the ongoing responsibility to ensure that these users actively comply with University of Houston policies and procedures regarding user I.D. administration.

Password Control

Purpose

To prevent unauthorized access to University of Houston corporate computer systems.

Scope

For use with all systems which have passwords in the user identification process.

Standard

The Information Security Administrator (ISO) shall establish a sound policy of password control and violation reporting.

Guidelines

1. Passwords are to be assigned to the individual employee or issued on an individual employee basis if computerized records are being accessed as part of their responsibility.
2. Distribution of passwords should be handled with the strictest confidentiality.
3. Passwords shall be changed on a regular basis (at least once every 60 days).
4. Passwords which are obvious, such as nicknames and dates of birth, should not be allowable.
5. Passwords should never be shared with another user. Employees are formally notified as to their role in protecting the security of the user ID. and password. Counter accounts, for view only, are an exception to this rule.
6. Passwords shall have a minimum length of eight characters.
7. When possible, passwords should contain upper and lower case letters, numbers and special characters
8. Passwords stored on a computer should be encrypted in storage.
9. System software should enforce the changing of passwords and the minimum length and format.
10. The non-printing, password-suppression feature should be used on all terminals to prevent the display of a user ID or password at log-on.
11. System software should disable the user identification code if more than three consecutive invalid passwords are given.
12. System software should maintain a history of at least two previous passwords and prevent their reuse.
13. Procedures for forgotten passwords should require that the user be personally identified by Support Services.

System Software

Purpose

To define policies and procedures relating to University of Houston corporate system software.

Scope

All University of Houston corporate system software and utilities.

Standard

System software and utilities are to be treated as application software. All rules applying to acquisition, implementation and access of application software apply to system software (in addition to any special security policies that specifically address system software).

Guidelines

1. System software and package installation or maintenance tapes--Any and all system or package installation or maintenance tapes shall be kept in a secure, locked cabinet.
2. Access to system dumps--Whenever a full system dump occurs, the information should be treated as confidential. On-line access to the dump should be restricted to systems programmers, and hardcopy or dumps should be shredded upon disposal.
3. System software documentation--Any and all system software source code and object code in the form of paper, microfiche or any other medium shall be kept secured.

Modifications to System Software

Purpose

To define procedures for modifying corporate system software.

Scope

All modifications to system software.

Standard

All system software modifications must adhere to University of Houston-defined policies and procedures regarding their development, testing, and implementation.

Guidelines

1. System software modification implementation--The system programmer applying changes to system software must have an approved backout plan, in case there are problems encountered during the implementation of the changes.
2. Separate test environment for system software programs--System software modifications/exits should be made to test versions of the software libraries. The test environment shall have a reasonable set of activities performed within it, in order to validate the integrity of the new environment.

3. Emergency modifications directly to the production system software--All modifications directly to the production system software libraries shall require the approval of the system programmer's direct line manager. After the emergency is past, documentation shall be developed to reflect the changes made to the affected system software.

System Surveillance

Purpose

To ensure that adequate monitoring and follow-up is taking place when unusual system activity is occurring.

Scope

All corporate automated application systems in use at University of Houston.

Standard

Ongoing monitoring of the entire computing environment should be performed by the system manager in order to detect abnormal situations that might indicate a potential security breach.

Guidelines

1. Outage and incident tracking - Historical information regarding the nature, duration and resolution of system problems should be developed. Average incident activity figures should be compared with current data as a means of detecting abnormal conditions.
2. Violations of access controls should be recorded and reviewed by either the owner or the custodian of the information. If appropriate, the violation should be reported to the individual's manager, auditing, or both. Repeated violations or violation attempts must be reported to the individual's manager.
3. Ensure that the operating system provides threat-monitoring information. The system should record data on the following events as often as the user desires:

- Unauthorized attempts to enter the system.
- All authorized or unauthorized attempts to access protected resources
- All attempts to issue restricted commands
- All attempts to modify profiles on restricted data
- The system should have the ability (in real-time) to route messages to the security console, and each incident should be recorded on the security log/audit trail file.

Data Communications Software Implementation and Maintenance

Purpose

To define procedures for implementing and maintaining Data Communications (DC) software that will ensure integrity of data communications.

Scope

All data communications software in use at University of Houston.

Standard

Proper procedures shall be in place to ensure the integrity of the data communications software, and to ensure that no security exposure is posed by the software change control process that governs it.

Guidelines

1. When selecting DC software, an evaluation and selection of security related options or features must be performed as part of standard procedures.
2. If a DC software package has security weaknesses, additional security measures will be implemented to correct the security weakness.
3. Communications software backup - Up-to-date backup of copies of all communications software will be maintained for use in the event of destruction or failure of the primary system. Storage should be on a secure off-site location.
4. Source executable versions of the DC software must be protected by software mechanisms against unauthorized read and update access.
5. Where DC software modifications are made to enhance capabilities (e.g., improving throughout), care must be taken that coding does not inadvertently weaken security and control.
6. Communications hardware backup - Where practical, replacements should be available for critical communications hardware/circuitry, such as:

- Modems
- Multiplexors
- Digital switches
- Communications controllers
- Terminals
- Cluster controllers
- Redundant leased (or dial-up) communication circuits

7. Abnormal DC hardware, circuit, and software anomalies should be investigated to determine their cause. A permanent incident log should be maintained to detect trends that may reveal potential access penetration attempts.

8. Automated techniques such as parity and redundancy checks should be used to help detect and correct data transmission errors.

Terminal Controls

Purpose

To prevent unauthorized access to University of Houston data by providing terminal controls.

Scope

University of Houston terminals.

Standard

Proper physical and software control mechanisms shall be in place to control access to and use of devices connected to University of Houston computer systems.

Guidelines

1. Hardware Terminal Locking - In areas that are not physically secured, terminals should be equipped with locking devices to prevent their use during unattended periods. The locks should be installed in addition to programmed restrictions, such as automatic disconnect after a given period of inactivity.
2. Operating System Identification of Terminals - All terminal activity should be controlled by the operating system, which should be able to identify terminals, whether they are hardwired or connected through communications lines. The operating system should inspect log-on requests to determine which application the terminal user desires. The user should identify an existing application and supply a valid user ID and password combination. If the log-on request is valid, the operating system should make a logical connection between the user and the application.
3. Limitation of log-on Attempts - Limit system log-on attempts from remote terminal devices. More than three unsuccessful attempts should result in termination of the session, generation of a real-time security violation message to the operator and/or the ISO (and log of said message in an audit file), and purging of the input queue of messages from the terminal.
4. Time-Out Feature - Ensure that the operating system provides the timing services required to support a secure operational environment. Inactive processes, or terminals (in an interactive environment) should be terminated after a predetermined period.
5. Dial-Up Control - The communications software should ensure a clean end of connection in all cases, especially in the event of abnormal disconnection.

Technical Security Requirements

The technical security requirements are directly related to the sensitivity/criticality level of the data processed.

Workstation Security Requirements

Workstations include corporate personal computers (PCs), LANs, and LAN servers. When a workstation is used as a host, host security requirements apply.

Single User Workstation

A single user workstation is one which, though many people have access, may be used by one person at a time. Where single user workstations are installed, management should do the following:

Critical Level *	Requirements
3, 2, 1	Implement a risk management program commensurate with sensitivity and/or criticality of the information/application being processed. Ensure that virus detection software is installed on each single user workstation.
0	Ensure that the system configuration is documented. Establish backup requirements. Ensure that virus detection software is installed on each single user workstation.
* See **Appendix B** for critical level definitions.	

Multi-User Workstation

A multi-user workstation is one that can be accessed simultaneously by other workstations. In some cases a multi-user workstation may be configured to operate as a host, and the requirements for hosts will apply to that workstation, Otherwise, the requirements below should apply. Management, where multi-user corporate workstations are installed, should implement a process that accomplishes the following:

Critical Level *	Requirements
3, 2	Documents system configuration. Ensure that virus detection software is installed in the workstation. Ensure the backup requirements are established. Implement a risk management program commensurate with sensitivity

	and/or criticality of the information/application being processed. Assigns a system administrator. Identifies each user by a unique user ID and password. Provides secure backup storage external to the processing area. Ensures that critical data backups are placed in secure storage.
1	Documents system configuration. Ensure that virus detection software is installed in the workstation. Ensure the backup requirements are established. Establishes the development of a contingency plan.
0	Documents system configuration. Ensure that virus detection software is installed in the workstation. Establish backup requirements.
* See **Appendix B** for critical level definitions.	

System Identification Screen

Purpose

To ensure that system identification screen/logon banner is displayed on all systems.

Scope

Authorized University of Houston corporate equipment.

Guidelines

1. The system identification screen/logon banner should be implemented so that it cannot be bypassed by a user.
2. The system identification screen/logon banner should remain on display for a sufficient amount of time for the message to be read.
3. The system identification screen/logon banner shall include the following warning statements:

- Unauthorized Use is Prohibited;
- Usage May be Subject to Security Testing and Monitoring; and
- Misuse is subject to criminal prosecution.
- Users have no expectation of privacy except as otherwise provided by applicable privacy laws.

Wireless Access Policy

Purpose

To insure that wireless network access is secure.

Scope

All University of Houston wireless network devices.

Guidelines

1. The wireless router or access point administration interface must be secure. The default password must be changed to be compliant with the UH Strong Password standard. Guest access or accounts should be disabled.
2. The SSID should be changed to conform to the location of the access point. Use the official building abbreviation followed by an underscore, then the room number of the access point. For example PGH_207 would be Phillip G. Hoffman room 207.
3. At least 128 bit encryption must be enabled on the access point. If possible, utilize WPA encryption instead of WEP.
4. Wireless administration should be disabled. Access points should only be administered via a wired connection.
5. All UH wireless access point devices must be registered and authorized with IT. IT regularly performs building-to-building assessments to detect unauthorized wireless access point devices.
6. Confidential and sensitive personal information is prohibited from being transmitted over UH wireless network devices unless an encryption method such as Virtual Private Network (VPN) is utilized.

Best Practices for Performance

- Utilize non-overlapping channels. For example, if two access points are near each other, fix one to broadcast on channel 6 and one to broadcast on channel 11.
- Plan for access points to have no more than 25 users each.
- Force 30-minute or 60-minute re-authentication for all users.
- Continuously monitor the network performance for changes in performance, and report any anomalies immediately to the UH help desk.

General Computing Policies

Introduction

The University of Houston computing facilities exist to provide computing services to the university community in support of instructional, research, and University business activities. These guidelines are intended to improve the computing services offered and provide these services in a cost-effective

manner. University computing facilities are a public resource and may not be used for personal or corporate profit.

Computing facilities at the University of Houston are increasingly decentralized. These guidelines apply to all University computing facilities. Local facilities may establish additional guidelines to meet their special needs. The guidelines of each facility are enforced by a facility manager. For example, the Director of Central Computing Services, or the director's designate, is the facility manager for the computing facilities under Central Computing Services' control. Each microcomputer cluster also has a facility manager.

Within the limits of available resources, each computing facility at the University of Houston has a responsibility to provide service to users in an efficient and equitable manner. To that end, facility managers should establish a set of guidelines governing access to the facilities. Any user who believes that these access guidelines are not being followed, or that they fail to recognize the needs of a group of users, should address their concerns to the facility manager. If the user and the facility manager cannot reach an agreement concerning user access, either the user or the facility manager may ask the Vice President for Information Technology to assist in resolving the problem.

The University computing facilities service a large number of students, faculty, and staff. All users have the responsibility to use the University computing systems in an effective, efficient, ethical, and lawful manner. The ethical and legal standards that are to be maintained are derived directly from standards of common sense and common decency that apply to the use of any public resource.

The following conditions apply to all users of the computing facilities. Violations of any of the conditions are considered unethical and may also be unlawful.

Conditions of Use

As a condition of use of any of the computing facilities, the user agrees:

1. To respect and follow state and federal laws related to integrity, confidentiality and safeguarding educational information of former and current students, financial and protected health information against unauthorized access and destruction. For example,

- **Texas Administrative Code, Title 1, (TAC 202)** requires the University and its employees to protect the integrity and confidentiality of information and to take measures to protect information resources against unauthorized access and destruction.
- **Gramm-Leach-Bliley (GLB) Act** requires the University and its employees to safeguard personal financial information that it collects and/or maintains in electronic and paper forms.
- **Family Educational Rights and Privacy Act (FERPA)** requires the University and its employees to protect educational information of both former and current students.
- **Health Insurance Portability and Accountability Act (HIPAA)** requires the University and its employees to ensure the confidentiality and integrity of protected health information that it receives, creates, collects, transmits and/or maintains and to protect such health information from reasonably anticipated threats, uses and disclosures.

2. To respect the privacy of other users; for example, users shall not intentionally seek or reveal information on, obtain copies of, or modify files, tapes, or passwords belonging to other users, or misrepresent others, unless explicitly authorized to do so by those users.
3. To respect the legal protection provided by copyright and license to programs and data; for example, users shall not make copies of a licensed computer program to avoid paying additional license fees or to share with other users.
4. To respect the intended usage for which access to computing resources was granted; for example, users shall use computing resources authorized for their use by the individuals responsible for these resources only for the purpose specified by that individual. Examples of inappropriate use may include the use of computing resources for purely recreational purposes, the production of output that is unrelated to the objectives of the project, and, in general, the use of computers simply to use computing resources.
5. To respect the integrity of computing systems; for example, users shall not intentionally develop or use programs that harass other users or infiltrate a computer or computing system and/or damage or alter the software components of a computer or computing system. Any defects discovered in system accounting or system security should be reported to the appropriate system administrator so that steps can be taken to investigate and solve the problem.
6. To respect the financial structure of a computing system; for example, users shall not intentionally develop or use any unauthorized mechanisms to alter or avoid charges levied by the University for computing services.
7. To respect the shared nature of the computing resources; for example, users shall not engage in deliberately wasteful practices such as printing large amounts of unnecessary listings, performing endless unnecessary computations, simultaneously queuing numerous batch jobs, or unnecessarily holding public workstations, magnetic tape drives, or dial-up telephone lines for long periods of time when other users are waiting for these devices.
8. To respect the rights of other users; for example, users shall not engage in private or public behavior that creates an intimidating, hostile, or offensive environment for other users.

In addition to the above, each facility may have additional guidelines for the use of particular types of accounts (e.g., student instructional accounts), and it is the user's responsibility to read and adhere to these additional guidelines.

Users of computing resources should be aware that although many computing facilities provide and preserve the security of files, account numbers, and passwords, security can be breached through actions or causes beyond the reasonable control of the facility. Users are urged, therefore, to safeguard their data, to take full advantage of file security mechanisms, and to change account passwords frequently.

E-Mail Distribution of Information

Users of University e-mail systems should be aware that e-mail is not a secure form of communication by default. Sensitive information including social security numbers, payment card numbers and other forms of confidential information should not be distributed via email. Users are strictly prohibited from sending an individual's name and restricted personal information which includes an individual's social security number or data protected under state or federal law (e.g. financial, medical or student data) via email unless the data is encrypted.

Violations of Conditions of Use

Violations of these conditions -- e.g., unauthorized use of another user's account; tampering with other users' files, tapes, or passwords; harassment of other users; unauthorized alteration of computer charges; unauthorized copying or distribution of copyrighted or licensed software or data; deliberately wasteful practices; online behavior that intimidates or offends -- are certainly unethical and may be violations of University policy or may be criminal offenses. Users should report to the facility manager or to the individual in charge of their computing resource, information they may have concerning instances in which the above conditions have been or are being violated.

When possible violations of these conditions of use are reported or discovered, facility managers reserve the right to commence an investigation of possible abuse. In this connection, the facility managers, with due regard for the rights of privacy and other rights of users, may be given the authority to examine files, passwords, accounting information, printouts, tapes, or other material that may aid the investigation. Examination of user files must be authorized by the Vice President for Information Technology, or a designate. Users, when requested, are expected to cooperate in such investigations. Failure to do so may be grounds for cancellation of access privileges. While an investigation is in progress, in order to prevent further possible unauthorized activity, the facility manager may suspend the authorization of computing services to the individual or account in question.

When possible unauthorized use of computing resources is encountered, the facility manager shall notify the user. The user is expected to take remedial action or to indicate that such use should be permitted. Should unauthorized use continue after notification of the user or should differences of opinion persist, these shall be brought to the attention of the Vice President for Information Technology for recommendations on further action. Upon the recommendation of the Vice President for Information Technology, facility mangers may impose limitations on continued use of computing resources. In accordance with established University practices, confirmation of unauthorized use of the computing facilities may also result in disciplinary review which could lead to expulsion from the University, termination of employment, and/or legal action.

Data Classification Levels

Sensitivity/Criticality Level

Automated information sensitivity/ criticality level	EXPLANATION Automated information, automated applications, or computer systems, the inaccuracy, alteration, disclosure, or unavailability of which:

3	Would have an IRREPARABLE impact, permanently violating the integrity of UH missions, functions, image, and reputation. The catastrophic result would not be able to be repaired or set right again; or Would result in the loss of MAJOR tangible asset(s) or resource(s).
2	Would have an ADVERSE impact actively opposed to UH missions, functions, image, and reputation. The impact would place UH at a significant disadvantage; or Would result in the loss of SIGNIFICANT tangible asset(s) or resource(s).
1	Would have a MINIMAL impact on UH missions, functions, image, and reputation. A breach of this sensitivity/criticality level would result in the least possible significant unfavorable condition with a negative outcome; or Could result in the loss of SOME tangible asset or resource.
0	Would have a NEGLIGIBLE effect on UH missions, functions, image, and reputation. The impact, while unfortunate, would be insignificant and almost unworthy of consideration; or Probably would not result in the loss of a tangible asset or resource.
Level 0 applications are not sensitive. Organizations may therefore follow their own plans for level 0 applications as identified in each of the requirements. However, all level 0 organizational plans will have the concurrence of the organization's management.	