

University of Houston – Clear Lake

Information Security

Policies and Procedures

Reviewed and Updated 7-1-06

Document meets compliance with Texas Administrative Code, Title 1 (TAC 202).

TABLE OF CONTENTS

1. Information Security Policy		
	Policy Statement	3
	Background	3
	Scope	3
	Definitions	3
	Responsibilities	4
	Enforcement	5
2. Security Planning and Administration Policies and Procedures		
	Information Security Officer – Responsibilities	6
	Information Security Administrator – Responsibilities	8
	Information Security Auditor – Responsibilities	9
	Security Orientation and Training	10
	Information Classification and Ownership	11
	Information Sensitivity/Criticality Levels	12
	Audit Trail	14
	Risk Assessment	15
	Risk Analysis	16
	Risk Assessment Review	17
	Information Security Responsibilities of the Information Security Committee (ISC)	18
	Security Procedures Manual	19
	Emergency Preparations	20
	Record Retention and Data Confidentiality	21
3. Personnel Policies and Procedures		
	Personnel Practices	22
	Employee Screening	23
	New Employee Orientation	25
	Student Orientation	26
	Rotation and Separation of Duties	27
	Termination of Data Processing Employees	29
	Computer Security Violation Reporting	31
	Use of University Equipment and Resources	33
	Management and Supervision	36
	Security Vulnerability Report	38

PROPERTY OF THE UNIVERSITY OF HOUSTON-CLEAR LAKE

Do not delete this notice. This material shall not be provided, copied or otherwise disseminated, in whole or in part to any party without the express written consent of the University of Houston-Clear Lake.

4. Access Control Policies and Procedures	
Data and Software Access	39
Individual Accountability	40
Audit Trail	41
Password Control	42
System Software	47
Modifications to System Software	48
Sensitive Utilities and Commands	49
Automated Access Control	50
System Surveillance	51
Database Access Controls, Recovery and Maintenance	52
5. Data Communications Policies and Procedures	
Data Communications Software Implementation and Maintenance	54
Network Security	56
Terminal Controls	57
Workstation Requirements	59
Network Documentation	61
Identifying Remote Terminals	62
Dial-up Communications Equipment	63
System Identification Screen	64
Physical Security of Communications Equipment	65
Data Transfer Between Computers	67
Appendix A – UHCL Automated Information Systems Acceptable Use Policy	68
Appendix B – Information Resources Security Policy	70

PROPERTY OF THE UNIVERSITY OF HOUSTON-CLEAR LAKE

Do not delete this notice. This material shall not be provided, copied or otherwise disseminated, in whole or in part to any party without the express written consent of the University of Houston-Clear Lake.

6. INFORMATION SECURITY POLICY STATEMENT

Background

University of Houston-Clear Lake 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 will exist to safeguard these assets. Information will be processed in a secure environment and all employees share the responsibility for the security, integrity, and the 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 the 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

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. Where appropriate, ownership may be shared by managers of different departments.

Custodian

The custodian is responsible for the processing and storage of the information. For 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.

PROPERTY OF THE UNIVERSITY OF HOUSTON-CLEAR LAKE

Do not delete this notice. This material shall not be provided, copied or otherwise disseminated, in whole or in part to any party without the express written consent of the University of Houston-Clear Lake.

Information

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

PROPERTY OF THE UNIVERSITY OF HOUSTON-CLEAR LAKE

Do not delete this notice. This material shall not be provided, copied or otherwise disseminated, in whole or in part to any party without the express written consent of the University of Houston-Clear Lake.

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 or his or her designated representative(s) are responsible for and authorized to:

1. Approve access and formally assign custody of an information resources asset;
2. Determine the asset's value;
3. Specify data control requirements and convey them to users and custodians;
4. 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 state agency.
5. Confirm that controls are in place to ensure the accuracy, authenticity, and integrity of data.
6. Ensure compliance with applicable controls;
7. Assign custody of information resources assets and provide appropriate authority to implement security controls and procedures.
8. Review access lists based on documented security risk management decisions.

Custodian

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

1. Implementing the controls specified by the owner(s);
2. Providing physical and procedural safeguards for the information resources;
3. Assisting owners in evaluating the cost-effectiveness of controls and monitoring; and
4. Implementing the monitoring techniques and procedures for detecting, reporting, and investigating incidents.

PROPERTY OF THE UNIVERSITY OF HOUSTON-CLEAR LAKE

Do not delete this notice. This material shall not be provided, copied or otherwise disseminated, in whole or in part to any party without the express written consent of the University of Houston-Clear Lake.

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 identification and passwords are not disclosed to, or used by others.
5. Become familiar with and abide by the Computing Acceptable Use Policy.

Enforcement

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

PROPERTY OF THE UNIVERSITY OF HOUSTON-CLEAR LAKE

Do not delete this notice. This material shall not be provided, copied or otherwise disseminated, in whole or in part to any party without the express written consent of the University of Houston-Clear Lake.

INFORMATION SECURITY OFFICER – Responsibilities

Position:

Information Security Officer (ISO)

Reports To: Executive Director University Computing and Telecommunications

Primary Functions

Develop and administer system and information ownership and information and data classification guidelines, standards and procedures. Develop, establish and maintain system-wide standards, procedures and guidelines to promote the security and uninterrupted operation of computer-based application systems at University of Houston-Clear Lake. Identify and address exposures to accidental or intentional destruction, disclosure, modification, or interruption of information so as to preclude serious financial and/or information loss to University of Houston-Clear Lake. Be responsible for the protection of the University of Houston Systems' assets and information, which are processed by or stored in University of Houston-Clear Lake's computer information systems.

Specific Duties

1. Manage the information security function in accordance with the policies and guidelines established by the Information Security Committee (ISC).

Report to the Executive Director University Computing and Telecommunications

- 2.
3. Establish and maintain information security standards and procedures compliant with state information security and risk management policies, standards and guidelines. Function as an internal consulting resource on information security issues.
4. Conduct annual information security risk assessment program. Review compliance to the information security policy and associated procedures.
5. Serve as a member of software review committee to evaluate new software and hardware systems.
6. Review new systems designs and major modifications for security implications prior to implementation.
7. Coordinate information security efforts with Internal Audit.
8. Provide periodic reporting on information security issues to the Executive Director of University Computing & Telecommunications.

PROPERTY OF THE UNIVERSITY OF HOUSTON-CLEAR LAKE

Do not delete this notice. This material shall not be provided, copied or otherwise disseminated, in whole or in part to any party without the express written consent of the University of Houston-Clear Lake.

9. Coordinate security orientation and security awareness programs.
10. Assist in coordinating contingency plan tests on a regular basis.
11. Develop and maintain the access control rules within the security software that provided controlled access in accordance with owner defined information access requirements.

PROPERTY OF THE UNIVERSITY OF HOUSTON-CLEAR LAKE

Do not delete this notice. This material shall not be provided, copied or otherwise disseminated, in whole or in part to any party without the express written consent of the University of Houston-Clear Lake.

INFORMATION SECURITY ADMINISTRATOR – Responsibilities

Position: Information Security 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. Supervise 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. Develop and maintain the access control rules within the security software that provides controlled access in accordance with owner defined information access requirements.
7. Maintain valid and current user lists and oversee procedures for password control and for secure distribution of encryption keys (where used).
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 a designated individual to act as an ISA alternate, in case of emergency or absence.
12. Ensure that departments have fulfilled their security responsibilities.
13. Provide liaison with the security function.
14. Consult on planned physical facilities changes, and alterations in work now or operating procedures to evaluate the effect of such changes on security and safety.

PROPERTY OF THE UNIVERSITY OF HOUSTON-CLEAR LAKE

Do not delete this notice. This material shall not be provided, copied or otherwise disseminated, in whole or in part to any party without the express written consent of the University of Houston-Clear Lake.

INFORMATION SECURITY AUDITOR – Responsibilities

Position: Information Security 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 operation, with particular emphasis on major systems.
4. Inform management, the information security function and the information's owners, custodians, and the users of its findings.
5. Participate in the risk analysis process.

PROPERTY OF THE UNIVERSITY OF HOUSTON-CLEAR LAKE

Do not delete this notice. This material shall not be provided, copied or otherwise disseminated, in whole or in part to any party without the express written consent of the University of Houston-Clear Lake.

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

All University of Houston -Clear Lake employees.

Guidelines

An Information Security Training program should be established for all covering topics such as:

Organizational Security Policy - All employees should be aware of the organization's security policy and their responsibility to protect data and other resources from misuse, theft, or destruction.

Security Operating Procedures - Train employees in day-to-day procedures for handling sensitive data/programs, conducting security checks, and maintaining the security and integrity of systems and facilities.

Access Control Procedures - Delineate the types and levels of access to facilities and systems, access control systems in use, and escort policy and procedures.

Security Incident Procedures - Discuss the handling of bomb threats, riots/disturbances, unauthorized personnel in controlled areas, and emergency reporting and responses.

Responsible Party - Information Security Officer (ISO)
Information Security Administrator (ISA)

PROPERTY OF THE UNIVERSITY OF HOUSTON-CLEAR LAKE

Do not delete this notice. This material shall not be provided, copied or otherwise disseminated, in whole or in part to any party without the express written consent of the University of Houston-Clear Lake.

INFORMATION CLASSIFICATION AND OWNERSHIP

Purpose

1. Document all of the University of Houston -Clear Lake information according to its sensitivity and/or criticality.
2. Provide a basis for determining who in the organization should control access to a particular item of information.

Scope

Any and all information produced, used, or maintained by the University of Houston -Clear Lake.

Standard

All information that serves as input to, part of, or output of a computer-based application should have an owner identified for it, and should be clearly identified and secured based on its information sensitivity or criticality.

Guidelines

1. Information should be classified according to the most sensitive detail it includes.
2. Information recorded in several formats (e.g. source document, electronic record, report) should have the same classification regardless of format.
3. The data classification and ownership worksheet can serve as the mechanism for documenting this process.
4. Procedures are needed to categorize data. In addition, specific handling, distribution and storage procedures should be defined for each category of data.
5. Procedures should ensure privacy and confidentiality of information that might affect an individual's civil liberties, and ensure compliance with applicable privacy laws.
6. Procedures should identify and safeguard programs and data pertaining to new product and service development and competitive analysis.
7. 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.
8. Systems development projects should have formal checkpoints addressing output labeling and data access control throughout the system design effort.

PROPERTY OF THE UNIVERSITY OF HOUSTON-CLEAR LAKE

Do not delete this notice. This material shall not be provided, copied or otherwise disseminated, in whole or in part to any party without the express written consent of the University of Houston-Clear Lake.

INFORMATION SENSITIVITY/CRITICALITY LEVELS

Purpose

To establish sensitivity and/or criticality levels based on the harm that will occur to the University of Houston-Clear Lake mission if the data at that level should be come corrupted, altered, or disclosed.

Scope

Any and all information produced, used, or maintained by the University of Houston -Clear Lake.

Standard

All information that serves as input to, part of or output of a computer-based application should be clearly identified and secured based on its information sensitivity or criticality.

Guidelines

1. Information should be classified according to the most sensitive detail it includes so that appropriate protective measures may be considered.
2. The sensitivity/criticality level of data or applications is assigned by owner with the level assigned as least as high as the most sensitive/critical data that will be processed.
3. The four-sensitivity/criticality levels together with a definition of each level are presented in Figure 2.0. The definitions are based on the amount of harm or loss that could be experienced from an adverse event that affects the integrity, availability, or confidentiality of data or application.

PROPERTY OF THE UNIVERSITY OF HOUSTON-CLEAR LAKE

Do not delete this notice. This material shall not be provided, copied or otherwise disseminated, in whole or in part to any party without the express written consent of the University of Houston-Clear Lake.

SENSITIVITY / CRITICALITY LEVELS

AUTOMATED INFORMATION EXPLANATION SENSITIVITY / CRITICALITY

Level	Automated information, automated applications, or computer systems, the inaccuracy, alteration, disclosure, or unavailability of which:
3	<p>Would have an IRREPARABLE impact, permanently violating the integrity of University of Houston-Clear Lake missions, functions, image and reputation. The catastrophic result would not be able to be repaired or set right again; or</p> <p>Would result in the loss of MAJOR tangible asset(s) or resource(s).</p>
<u>2</u>	<p>Would have an ADVERSE impact actively opposed to UHCL missions, functions, image, and reputation. The impact would place UHCL at a significant disadvantage; or</p> <p>Would result in the loss of SIGNIFICANT tangible asset(s) or resource(s).</p>
1	<p>Would have a MINIMAL impact on UHCL 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</p> <p>Could result in the loss of SOME tangible asset or resource.</p>
0	<p>Would have a NEGLIGIBLE impact on UHCL missions, functions, image and reputation. The impact, while unfortunate, would be insignificant and almost unworthy of consideration; or</p> <p>Probably would not result in the loss of a tangible asset or resource.</p>

Formatted: Indent: Left: 0",
Numbered+ Level: 1 + Numbering
Style: 1, 2, 3, ... + Start at: 2 +
Alignment: Left + Aligned at: 0.75" +
Tab after: 1.75" + Indent at: 1.75",
Tabs: Not at 1.75"

Figure 2.0

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.

PROPERTY OF THE UNIVERSITY OF HOUSTON-CLEAR LAKE

Do not delete this notice. This material shall not be provided, copied or otherwise disseminated, in whole or in part to any party without the express written consent of the University of Houston-Clear Lake.

AUDIT TRAIL

Purpose

To ensure that all transactions occurring on University of Houston-Clear Lake computer systems are traceable to the origin or source.

Scope

All shareable computer systems under the control of the University of Houston-Clear Lake.

Standard

Audit trails shall be maintained to provide accountability for all accesses to confidential or sensitive information.

Guidelines

1. Audit trails which provide accountability for all accesses to confidential or sensitive information shall be maintained for an appropriate period of time prescribed for the sensitivity/criticality level of data or application accessed.
2. A sufficiently complete history of transactions shall be maintained for each session involving access to confidential or sensitive information to permit audit of the system by tracing the activities through the system.
3. An analysis of transaction histories for the purposes of detecting variances from the norm should be conducted regularly.

PROPERTY OF THE UNIVERSITY OF HOUSTON-CLEAR LAKE

Do not delete this notice. This material shall not be provided, copied or otherwise disseminated, in whole or in part to any party without the express written consent of the University of Houston-Clear Lake.

RISK ASSESSMENT

Definition

The identification of risks to the University of Houston-Clear Lake's information resources through an analysis of information assets, threats, and vulnerabilities.

Objectives

1. To identify risks which require management's attention.
2. To aid in establishing priorities for safeguard evaluation, selection, acquisition and implementation.
3. To provide data for safeguard cost-benefit analysis.

PROPERTY OF THE UNIVERSITY OF HOUSTON-CLEAR LAKE

Do not delete this notice. This material shall not be provided, copied or otherwise disseminated, in whole or in part to any party without the express written consent of the University of Houston-Clear Lake.

INITIAL RISK ANALYSIS

Purpose

To conduct a risk analysis for University of Houston-Clear Lake information resources completed by September 1, 1994.

Scope

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

Standard

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

Identification of assets

Estimation of asset values

Identification of threats

Identification of vulnerabilities

Recommend protective measures

Calculation of risk acceptance after protective measures are implemented

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?

PROPERTY OF THE UNIVERSITY OF HOUSTON-CLEAR LAKE

Do not delete this notice. This material shall not be provided, copied or otherwise disseminated, in whole or in part to any party without the express written consent of the University of Houston-Clear Lake.

ANNUAL RISK ASSESSMENT REVIEW

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 annually all non-compliance situations concerning security policy and practices.
4. Determine the appropriate recourse for each non-compliance situation.

Scope

All University of Houston -Clear Lake 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

On an annual basis, the Information Security Committee (ISC) 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 an annual risk assessment review of the overall information systems environment, current policies, procedures, guidelines and standards and all incidents of non-compliance.
2. The revised risk assessment should be presented to the ISC for acceptance.
3. The revised policies, etc., should be presented to the ISC for formal approval.
4. Incidents of non-compliance should be brought to the attention of the ISC and one of two actions will be taken:
 - a. The ISC should identify those policies, which require mandatory compliance and determine the corrective measures to be taken to ensure compliance.
 - b. The ISC should determine those policies where the cost of compliance outweighs the loss exposure. In either case, the ISC has the option to waive compliance to the policy and accept the risks.

PROPERTY OF THE UNIVERSITY OF HOUSTON-CLEAR LAKE

Do not delete this notice. This material shall not be provided, copied or otherwise disseminated, in whole or in part to any party without the express written consent of the University of Houston-Clear Lake.

INFORMATION SECURITY RESPONSIBILITIES OF THE INFORMATION SECURITY COMMITTEE (ISC)

Objective

The security-related objectives of the Information Security Committee 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 within University of Houston-Clear Lake.

Purpose

The security-related purposes of the ISC are to:

1. Provide the information security function with a mechanism for the review and approval of security implementation and administration policies.
2. Manage the risk acceptance program.
3. 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-Clear Lake.
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.

PROPERTY OF THE UNIVERSITY OF HOUSTON-CLEAR LAKE

Do not delete this notice. This material shall not be provided, copied or otherwise disseminated, in whole or in part to any party without the express written consent of the University of Houston-Clear Lake.

SECURITY PROCEDURES MANUAL

Purpose

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

Scope

All University of Houston -Clear Lake data processing functions.

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:
 - a. Safety: (fire, bomb threat, water damage, police notification)
 - b. Housekeeping: (waste disposal, media storage)
 - c. Data Control: (access policy, job submission authorization requirements, media storage, backup policies and procedures)
 - d. Physical Access Control: (who can go where/how, what type of supervision vendor personnel require)
 - e. Procedures: (operations and shutdown)
 - f. Emergency Procedures: (operations, shutdown, contact personnel, contingency plan initiation)
 - g. Real-time Security Violation Reporting/Exception Reporting
 - h. Maintenance Procedures: (hardware and software)
 - i. Network Security Standards: (e.g., dial-up authentication procedures)
 - j. Forms Control
 - k. Application Processing/Updates/Overriding
 - l. And other policies and procedures deemed appropriate by the Chief Information Officer (CIO) or the Information Security Officer (ISO)

PROPERTY OF THE UNIVERSITY OF HOUSTON-CLEAR LAKE

Do not delete this notice. This material shall not be provided, copied or otherwise disseminated, in whole or in part to any party without the express written consent of the University of Houston-Clear Lake.

EMERGENCY PREPARATIONS

Purpose

To define the emergency preparations to be made by the Chief Information Officer (CIO).

Scope

All IS facilities and employees.

Standard

The Chief Information Officer (CIO) will ensure that preparations are made against possible emergencies, such as bomb threats, minor civil disturbances, snowstorms, tornadoes, hurricanes, floods, earthquakes, fires, explosions, and sabotage.

Guidelines

1. The Chief Information Officer (CIO) will be responsible for emergency planning to ensure the continuation of data processing during or after emergency situations.
2. The Chief Information Officer (CIO) will be responsible for keeping both University of Houston-Clear Lake management and IS staff informed during an emergency alert or emergency situation.
3. The Chief Information Officer (CIO) must develop a plan for emergency action within the scope of these guidelines and procedures.
4. The Chief Information Officer (CIO) must:
 - a. Publicize a phone number, which employees may call to receive instructions in case of an emergency or disaster situation.
 - b. Designate and publicize a safe assembly location, where appropriate, within walking distance of the data center, in case of temporary emergencies.
5. The Chief Information Officer (CIO) must, in case of imminent threat:
 - a. Alert University of Houston-Clear Lake management and security personnel. Warn and instruct employees in a manner, which will not cause panic.
 - b. Survey all personnel and inspect premises and equipment to assure emergency readiness.
6. The Chief Information Officer (CIO) is responsible for ensuring that emergency procedures are covered in periodic staff meetings or special training sessions.

PROPERTY OF THE UNIVERSITY OF HOUSTON-CLEAR LAKE

Do not delete this notice. This material shall not be provided, copied or otherwise disseminated, in whole or in part to any party without the express written consent of the University of Houston-Clear Lake.

RECORD RETENTION AND DATA CONFIDENTIALITY

Purpose

To ensure that all sensitive and critical information is given the appropriate level of access control, and that critical information is retained by the organization for the appropriate amount of time to satisfy recovery and regulatory needs.

Scope

All information used in the conduct of the University of Houston-Clear Lake business activities.

Standard

There should be a formal records retention program for manual and computerized information.

Guidelines

1. The retention program should identify what information needs to be retained, for what length of time, and the location and form of the storage.
2. Retention periods should be based on the needs of:
 - a. University
 - b. Taxing Authority
 - c. Regulatory agency requirements
3. There should be a single focal point for the administration and enforcement of the records retention program.

PROPERTY OF THE UNIVERSITY OF HOUSTON-CLEAR LAKE

Do not delete this notice. This material shall not be provided, copied or otherwise disseminated, in whole or in part to any party without the express written consent of the University of Houston-Clear Lake.

PERSONNEL PRACTICES

Objectives

1. To define specific personnel practices, including employee hiring, indoctrination, and termination.
2. To provide guidelines for personnel responsibilities.
3. To define good employee security practices.
4. To establish employee security awareness.
5. To define limitation of employee personal use of organization resources.

Standard

There should be a formal document, circulated annually to all employees outlining user rights and responsibilities as they relate to the use of and access to agency information resources.

PROPERTY OF THE UNIVERSITY OF HOUSTON-CLEAR LAKE

Do not delete this notice. This material shall not be provided, copied or otherwise disseminated, in whole or in part to any party without the express written consent of the University of Houston-Clear Lake.

EMPLOYEE SCREENING

Purpose

To prevent hiring of applicants who do not meet employment eligibility criteria with respect to previous criminal activities or unethical conduct.

Scope

All University of Houston -Clear Lake data processing positions that are subject to background investigation.

Standard

Data Processing managers are to direct all applicants for employment to Human Resources in accordance with this security policy, if the specific job title requires a background investigation.

Guidelines

1. Job titles for which employees background investigations are required include, but are not limited to:
 - a. Data Processing Management Positions
 - b. Systems Programmers
 - c. Data Base Administrators
 - d. Computer Operators
 - e. Technical Support Personnel
 - f. Programmers/Analysts
2. It is the responsibility of the Chief Information Officer (CIO) to see that each person receiving an original appointment or being promoted complies with the requirement for a background investigation. An appointee or promotee who fails to cooperate in following this procedure may be marked not qualified and may be subject to disciplinary action for failing to cooperate in the required investigation process.
3. An applicant's references should be checked for at least the past seven years.
4. Other applicant data, such as date-of-birth, citizenship, home residence, school credentials, and court and financial records, should be verified before a job offer is made.
5. A photograph should be taken as part of the personnel record.
6. There should be signed agreements in effect to cover ownership and royalty arrangements on business-related inventions by employees.

PROPERTY OF THE UNIVERSITY OF HOUSTON-CLEAR LAKE

Do not delete this notice. This material shall not be provided, copied or otherwise disseminated, in whole or in part to any party without the express written consent of the University of Houston-Clear Lake.

7. There should be suitable agreement to cover a non-disclosure/non-use or proprietary software and information trade secrets by individuals during employment and after they leave the organization.

PROPERTY OF THE UNIVERSITY OF HOUSTON-CLEAR LAKE

Do not delete this notice. This material shall not be provided, copied or otherwise disseminated, in whole or in part to any party without the express written consent of the University of Houston-Clear Lake.

NEW EMPLOYEE ORIENTATION

Purpose

To specify procedures for new University of Houston-Clear Lake employees.

Scope

All data processing related jobs within University of Houston-Clear Lake.

Standard

All new employees are to receive security orientation from their supervisors.

Guidelines

1. Every employee must understand University of Houston-Clear Lake interest in information security and the reasons for it. Senior management should be actively involved and participate in motivating employees on this subject.
2. The new employee is to be familiar with and must understand the systems security standards. He/she must be made to realize that violations of several of these standards could be serious enough to lead to termination of his/her employment. He/she must leave the orientation sessions with the comprehension of his/her direct responsibilities in ensuring the security and integrity of the University of Houston-Clear Lake data.
3. Training materials may be based on:
 - a. Systems security standards
 - b. Emergency Recovery Procedures Manual
 - c. Security literature and articles
4. A form (see Appendix A) certifying completion of security orientation (including any subjects covered and the employee's signature) should be inserted in the employee's personnel file.

PROPERTY OF THE UNIVERSITY OF HOUSTON-CLEAR LAKE

Do not delete this notice. This material shall not be provided, copied or otherwise disseminated, in whole or in part to any party without the express written consent of the University of Houston-Clear Lake.

STUDENT ORIENTATION

Purpose

For optional use at the University of Houston -Clear Lake, to advise all students of the information security policies and procedures at University of Houston-Clear Lake.

Scope

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

Standard

All first-time student users of University of Houston-Clear Lake's computerized information processing facilities are to receive information to familiarize themselves with the information security policies and procedures.

Guidelines

1. Every student must understand University of Houston-Clear Lake's interest in information security and the reasons for it.
2. The student is to be familiar with the security standards, and the students must be made aware that violations of several of these standards could be serious. Students must be oriented to their direct responsibilities in ensuring the security and integrity of the University of Houston-Clear Lake's data.
3. A form (Appendix B) certifying completion of security orientation (including the student's signature) should be retained.

PROPERTY OF THE UNIVERSITY OF HOUSTON-CLEAR LAKE

Do not delete this notice. This material shall not be provided, copied or otherwise disseminated, in whole or in part to any party without the express written consent of the University of Houston-Clear Lake.

SEPARATION OF DUTIES

Purpose

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

Scope

All University of Houston -Clear Lake data processing employees and users of sensitive data.

Standard

There should be university and departmental policies and procedures for separation of duties on sensitive job tasks. These policies should be actively enforced.

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:
 - a. Programmers:
 1. Programmers should not execute jobs in a production mode.
 2. Programmers should not control any transfers between programmer development libraries and production libraries.
 3. Programmers should/may not have data update access within any production application.

PROPERTY OF THE UNIVERSITY OF HOUSTON-CLEAR LAKE

Do not delete this notice. This material shall not be provided, copied or otherwise disseminated, in whole or in part to any party without the express written consent of the University of Houston-Clear Lake.

b. Operators:

1. Operators should not have the ability to make changes to production application or system software libraries.
2. Operators should not perform balancing activities, except those necessary for run-to-run controls.
3. Operators should not have the ability to make changes to job control language of scheduled jobs without proper notification and authorization.
4. Operators should execute only those jobs/programs scheduled through the established procedures.
5. Operators should not execute (outside of standard production processing) data or software-modifying system utilities without proper authorization and dual control.
6. Operators should not override internal tape labels without supervisory approval.

Formatted: Indent: Left: 1",
Numbered+ Level: 1 + Numbering
Style:1, 2, 3, ... + Start at: 1 +
Alignment:Left + Alignedat: 0.75" +
Tab after: 1" + Indentat: 1", Tabs:
Not at 1"

Formatted: Indent: Left: 1",
Numbered+ Level: 1 + Numbering
Style:1, 2, 3, ... + Start at: 1 +
Alignment:Left + Alignedat: 0.75" +
Tab after: 1" + Indentat: 1", Tabs:
Not at 1"

Formatted: Indent: Left: 1",
Numbered+ Level: 1 + Numbering
Style:1, 2, 3, ... + Start at: 1 +
Alignment:Left + Alignedat: 0.75" +
Tab after: 1" + Indentat: 1", Tabs:
Not at 1"

Formatted: Indent: Left: 1",
Numbered+ Level: 1 + Numbering
Style:1, 2, 3, ... + Start at: 1 +
Alignment:Left + Alignedat: 0.75" +
Tab after: 1" + Indentat: 1", Tabs:
Not at 1"

Formatted: Indent: Left: 1",
Numbered+ Level: 1 + Numbering
Style:1, 2, 3, ... + Start at: 1 +
Alignment:Left + Alignedat: 0.75" +
Tab after: 1" + Indentat: 1", Tabs:
Not at 1"

Formatted: Indent: Left: 1",
Numbered+ Level: 1 + Numbering
Style:1, 2, 3, ... + Start at: 1 +
Alignment:Left + Alignedat: 0.75" +
Tab after: 1" + Indentat: 1", Tabs:
Not at 1"

c. Users:

1. Data entry personnel should not prepare source documents for input.
2. Someone, other than the input operator, should verify all data input, unless programmatically verified.
3. The same person should not perform input and output duties.
4. The same person should not post and balance general ledger and other sensitive entries.
5. The person who prepared the original transaction should not review rejects or non-reads for reentry.
6. Master file and other sensitive transaction changes should be under dual control.

PROPERTY OF THE UNIVERSITY OF HOUSTON-CLEAR LAKE

Do not delete this notice. This material shall not be provided, copied or otherwise disseminated, in whole or in part to any party without the express written consent of the University of Houston-Clear Lake.

TERMINATION OF DATA PROCESSING EMPLOYEES

Purpose

To specify required employee termination procedures.

Scope

All University of Houston -Clear Lake data processing employees.

Standard

All terminating or transferring data processing employees are to be interviewed by the ISA, who should complete the Data Processing Employee Termination Checklist (see Appendix C) if they:

1. Have been employed in a data processing position.
2. Have been involved in work, which has directly or under their supervision involved the use of the University of Houston-Clear Lake computers or data entry programs, data or documentation.

Guidelines

1. The Data Processing Employee Termination Checklist must be completed for all employees performing data processing operations at University of Houston-Clear Lake. This will include personnel using other terminals as well as those directly involved in data processing operations.
2. This form is to be completed by the ISA if the terminating employee is unavailable, unwilling or unable to complete it.
3. All University of Houston -Clear Lake property including computer and communications equipment, keys, identification cards, programs, data and documentation must be returned to the terminating employee's supervisor or the ISA prior to completion of this form. It is the responsibility of the ISA to verify return of the materials.
4. It is the responsibility of the ISA to advise the departing employee that they cannot continue to use University of Houston-Clear Lake data processing facilities, data or equipment.
5. Situations requiring immediate revocation of access and/or processing authorization should be resolved directly with the ISA.
6. It is recommended that in addition to completing the Data Processing Employee Termination Checklist, Human Resources should prepare a property issuance and return record for all employees responsible for University of Houston -Clear Lake property. The

PROPERTY OF THE UNIVERSITY OF HOUSTON-CLEAR LAKE

Do not delete this notice. This material shall not be provided, copied or otherwise disseminated, in whole or in part to any party without the express written consent of the University of Houston-Clear Lake.

record should include issuance and return dates, and authorized issuer's signature for each item specified. Typically, the record will include keys, identification cards, badges, passwords, etc. In special instances, computer and communications equipment may also have been issued to employees for use in off-site locations.

7. It is recommended that department heads develop a formal exit interview process for employees within the scope of this standard. University of Houston -Clear Lake would like to maintain a stable work force with minimum level of staff losses. Facts and opinions stated during an exit interview may be of material value toward that objective.

PROPERTY OF THE UNIVERSITY OF HOUSTON-CLEAR LAKE

Do not delete this notice. This material shall not be provided, copied or otherwise disseminated, in whole or in part to any party without the express written consent of the University of Houston-Clear Lake.

COMPUTER SECURITY VIOLATION REPORTING

Purpose

1. To ensure compliance with the policy which requires that all employees of the University of Houston-Clear Lake shall have the affirmative obligation to report, directly and without undue delay, to the ISA, any and all information concerning conduct which they know or should reasonably know to involve corrupt or other criminal activity or conflict of interest, (1) by another University of Houston-Clear Lake employee, which concerns his or her office of employment, or (2) by persons dealing with University of Houston-Clear Lake. The knowing failure of any employee to report as required above shall constitute cause for disciplinary action.
2. To provide prompt notification to the ISA of computer abuse situation which may include:
 - a. Theft or diversion of the University of Houston-Clear Lake funds, computational resources, or other assets contained in or controlled by its computer systems.
 - b. Vandalism or other damage to computer systems, computer programs or data.
 - c. Unauthorized modification to (or use of) University of Houston-Clear Lake computer systems, programs, networks, networking equipment or data contained in these systems.

Scope

Applies to all University of Houston-Clear Lake employees.

Standard

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

Guidelines

The following information will be gathered for each reported violation. The ISA is responsible for gathering this data, once the employee reporting the abuse initially contacts him. Information to collect includes:

1. Description of the abuse:
 - a. Unauthorized use of computer time
 - b. Modification/alteration of computer data files or programs
 - c. Detection of illegal programs on a university computer system

PROPERTY OF THE UNIVERSITY OF HOUSTON-CLEAR LAKE

Do not delete this notice. This material shall not be provided, copied or otherwise disseminated, in whole or in part to any party without the express written consent of the University of Houston-Clear Lake.

- d. Forgery of negotiable instruments using a computer
 - e. Theft of computer equipment
 - f. Disclosure of computer systems password to unauthorized individual(s)
 - g. Destruction of computer data files or programs
 - h. Insertion/modification of input documents
2. Person(s) suspected of the abuse
- a. Name
 - b. Employee Number
 - c. Date of Birth
 - d. Office Title
 - e. Work Location
 - f. Length of University of Houston -Clear Lake service
 - g. Office Phone Number
 - h. Home Address
3. Person(s) reporting/detecting abuse
- a. Name
 - b. Office Title
 - c. Office Phone Number
 - d. Work Location
4. Evidence available to substantiate suspicion of abuse
- a. Printouts
 - b. Negotiable instruments
 - c. Input documents
 - d. Computer media
5. Date(s) of the abuse
6. Location of the abuse situation

PROPERTY OF THE UNIVERSITY OF HOUSTON-CLEAR LAKE

Do not delete this notice. This material shall not be provided, copied or otherwise disseminated, in whole or in part to any party without the express written consent of the University of Houston-Clear Lake.

USE OF UNIVERSITY EQUIPMENT AND RESOURCES

Purpose

To control the use of university equipment and resources.

Scope

All computer related equipment and resources.

Standard

All computer and word processing equipment leased or owned by the university and all timesharing services billed to the university will be used only to conduct University of Houston-Clear Lake business.

Guidelines

Information Security:

1. Where desktop computers have been provided for the exclusive use of a single employee, that employee is responsible for the security of all information and software associated with that desktop computer. It is recommended that the employee:
 - a. Insure that virus detection software is installed and up-to-date on the workstation.
 - b. Implement software that blanks screens and locks keyboards after a period of inactivity and requires a password for reactivation.
 - c. Backup critical or important files and insure that backups are kept secure.
 - d. Manage the hard disk to insure that all information storage policies and procedures are implemented.
 - e. Archive and delete sensitive or confidential information from the hard drive.
 - f. Prevent account codes and passwords from being stored in plain text as part of a menuing system, batch file or automated logon process. Prevent unauthorized individuals from accessing the workstation.
 - g. Use only legally licensed software.
2. Where desktop computers have been provided for shared use, the department manager or supervisor is responsible for the security of all information and software. The department manager or supervisor should:
 - a. Insure that virus detection software is installed and up-to-date on the workstation.
 - b. Implement software that blanks screens and locks keyboards after a period of inactivity and requires a password for reactivation.
 - c. Backup critical or important files and insure that backups are kept secure.
 - d. Manage the hard disk to insure that all information storage policies and procedures are implemented.

PROPERTY OF THE UNIVERSITY OF HOUSTON-CLEAR LAKE

Do not delete this notice. This material shall not be provided, copied or otherwise disseminated, in whole or in part to any party without the express written consent of the University of Houston-Clear Lake.

- e. Archive and delete sensitive or confidential information from the hard drive.
 - f. Prevent account codes and passwords from being stored in plain text as part of a menuing system, batch file or automated logon process.
 - g. Provide a means to track use of the workstation and establish policies, which detail the responsibilities of each user.
 - h. Prevent unauthorized individuals from accessing the workstation.
 - i. Use only legally licensed software.
3. Where desktop computers have been provided for shared use through access to a local area network, the local area network manager is responsible for the security of all information and software. The local area network manager should:
- a. Insure that virus detection software is installed and up-to-date on the workstation.
 - b. Implement software that blanks screens and locks keyboards after a period of inactivity and requires a password for reactivation.
 - c. Establish procedures that allow users to route critical files for automatic backup with system resources, including off-site storage.
 - d. Follow all backup policies and procedures established by University Computing and Telecommunications
 - e. Manage the file and applications server to insure that all information storage policies and procedures are implemented.
 - f. Insure that sensitive or confidential information is not stored on a shared hard drive.
 - g. Prevent account codes and passwords from being stored in plain text as part of a menuing system, batch file or automated logon process. Identify each user by a unique username and password.
 - h. Validate user access by username, password and workstation location.
 - i. Provide a mechanism, which makes the individual user responsible for his/her own data.
 - j. Use only legally licensed software.
 - k. Prevent the unauthorized copying of software or data.
 - l. Maintain a secure file documenting systems, configuration parameters, installed software and operating environments.

Risk Analysis

At present, the software, system, and information implemented on LANs and desktop computers is not considered critical to the university's operation. However, as some of these secondary systems grow in importance, they must become part of a coordinated risk management program.

However, some personal computers act as terminals to mission critical systems. In these cases, the correct operation of the desktop computer could be critical while the integrity of its data might not. These cases must be weighed in any risk management scenario.

PROPERTY OF THE UNIVERSITY OF HOUSTON-CLEAR LAKE

Do not delete this notice. This material shall not be provided, copied or otherwise disseminated, in whole or in part to any party without the express written consent of the University of Houston-Clear Lake.

Physical Security

The University must provide physical security for each important computing asset. Offices equipped with desktop computers must have functioning locks and a mechanism for tracking who has keys. LAN assets, such as network cabling, hubs, routers, switches, bridges, media adapters, and servers, must be secured in space offering limited access to specific authorized individuals.

Protective Measures

LAN servers should have sufficient uninterruptible power to enable a graceful shutdown. LAN servers and network hardware must be capable of remote management and restart.

PROPERTY OF THE UNIVERSITY OF HOUSTON-CLEAR LAKE

Do not delete this notice. This material shall not be provided, copied or otherwise disseminated, in whole or in part to any party without the express written consent of the University of Houston-Clear Lake.

MANAGEMENT AND SUPERVISION

Purpose

To highlight management/supervisor responsibilities towards information security and personnel security issues.

Scope

University of Houston-Clear Lake data processing employees.

Standard

The success or failure of a security program can be traced to employee attitudes towards security and the organization itself. There is direct correlation between employee dissatisfaction and the incidence of carelessness, fraud, theft or other misconduct. Each department manager needs to be aware of and address issues of work environment, professional growth, performance evaluation, incentives, detection and deterrence.

Guidelines

1. Work Environment – Workspaces and conditions should reflect management's concern for employee well being and productivity. Adequate lighting, noise suppression, ventilation and proper temperature and humidity and effective fire detection and suppression equipment should be provided. Exits should be appropriately marked and easily accessible.
2. Professional Growth - Challenge and growth are major motivating factors for data processing professionals (as well as for other employees). Employees should be encouraged to participate in professional organizations and to continue their education, through both external training and in-house professional development seminars.
3. Performance Evaluations – Frequent information performance evaluations should be used to give employees feedback on job performance and to offer them a chance to express their feelings about the working environment and their own career progress. Evaluations can also uncover potential problem areas before they become serious.
4. Detection and Deterrence – Organizations whose employees believe that they are likely to be caught if they engage in unauthorized activities experience a significantly lower level of theft and fraud. The more severe the reaction of management and coworkers, the lower the number of incidents (coworker sanctions are particularly effective).
5. Grievance Procedures– Fair and equitable grievance procedures and impartial administration are important. Management at all levels should be attentive to grievances and act promptly on those that are justified.

PROPERTY OF THE UNIVERSITY OF HOUSTON-CLEAR LAKE

Do not delete this notice. This material shall not be provided, copied or otherwise disseminated, in whole or in part to any party without the express written consent of the University of Houston-Clear Lake.

6. Awareness of Personal Problems– Major changes in the personal and work habits of subordinates should be noted. Such changes frequently signal an increased potential for fraud, misuse of resources, or disclosure of sensitive data. Changes in attendance patterns, evidence of alcohol and/or drug abuse, an inordinately high standard of living in relation to salary, severe indebtedness, and similar changes may indicate serious personal problems. Managers should investigate the causes of these problems and use all available organizational mechanisms to provide effective and timely assistance.
7. Define sensitive job functions and procedures.

PROPERTY OF THE UNIVERSITY OF HOUSTON-CLEAR LAKE

Do not delete this notice. This material shall not be provided, copied or otherwise disseminated, in whole or in part to any party without the express written consent of the University of Houston-Clear Lake.

SECURITY VULNERABILITY REPORT

Purpose

To provide a ready means for all employees to identify potential security vulnerabilities within University of Houston-Clear Lake computer processing systems.

Scope

All University of Houston -Clear Lake facilities, which contain or have access to computerized information processing facilities.

Standard

The Chief Information Officer (CIO) should prepare a memorandum to all employees expressing University of Houston-Clear Lake concern for the security, integrity, and continued availability of computer systems, and the need for employee participation in the protection of these systems.

Guideline

1. The memorandum should, at a minimum, contain the title and address of the ISA, to whom detected security vulnerabilities should be sent, and a brief description of the basis for identifying potential vulnerabilities and the appropriate information to be forwarded to the ISA (e.g., the sender's name, and phone number, a brief description of the vulnerability detected, and any recommended security improvements). It would be appropriate to include a request for suggestions to improve the operation or efficiency of any University of Houston-Clear Lake systems/programs.

PROPERTY OF THE UNIVERSITY OF HOUSTON-CLEAR LAKE

Do not delete this notice. This material shall not be provided, copied or otherwise disseminated, in whole or in part to any party without the express written consent of the University of Houston-Clear Lake.

DATA AND SOFTWARE ACCESS CONTROL

Purpose

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

Scope

All University of Houston -Clear Lake 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 -Clear Lake) are prevented from accessing any data.

Users of the University of Houston-Clear Lake computers should be granted those access privileges to data and software to accomplish their authorized responsibilities. This access control will be implemented by the ISA, and follow a strict "need to know" procedure for determining the detailed access rules to implement.

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. If access control software is inadequate in preventing programmed attacks on the information, all program compilers or assemblers and all general-purpose utilities capable of reading or updating files should be removed from the system.

PROPERTY OF THE UNIVERSITY OF HOUSTON-CLEAR LAKE

Do not delete this notice. This material shall not be provided, copied or otherwise disseminated, in whole or in part to any party without the express written consent of the University of Houston-Clear Lake.

INDIVIDUAL ACCOUNTABILITY

Purpose

To ensure that any activity occurring on a University of Houston -Clear Lake computer system is traceable to the individual initiating it.

Scope

All shareable computer systems under the control of the University of Houston -Clear Lake.

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 resource.

Guidelines

1. Automated identification processes should involve providing the system with both user identification and a confidential password.
2. All actions, either online or batch should be fully auditable to an individual.
3. This policy applies to activities by users, programmer, and operators.
4. Procedures should be actively enforced to ensure that usernames and passwords are removed from the system whenever that person is transferred to another position or leaves the organization.
5. Sign on software should not allow one user to be signed on to more than one terminal.
6. User identification and authentication can be maintained centrally by her ISA, who also has the option of distributing this function to designated user functions. If a decentralized administration approach is used, the ISA has the ongoing responsibility to ensure that these users actively comply with University of Houston -Clear Lake policies and procedures regarding user identification administration.

PROPERTY OF THE UNIVERSITY OF HOUSTON-CLEAR LAKE

Do not delete this notice. This material shall not be provided, copied or otherwise disseminated, in whole or in part to any party without the express written consent of the University of Houston -Clear Lake.

AUDIT TRAIL

Purpose

To ensure that all transactions occurring on a University of Houston-Clear Lake computer system are traceable to the origin or source.

Scope

All shareable computer systems under the control of the University of Houston-Clear Lake.

Standard

Audit trails shall be maintained to provide accountability for all accesses to confidential or sensitive information.

Guidelines

1. Audit trails, which provide accountability for all accesses to confidential or sensitive information, shall be maintained for an appropriate period of time prescribed for the sensitivity/criticality level of data or application accessed.
2. A sufficiently complete history of transactions shall be maintained for each session involving access to confidential or sensitive information to permit audit of the system by tracing the activities through the system.
3. An analysis of transaction histories for the purposes of detecting variances from the norm should be conducted regularly.

PROPERTY OF THE UNIVERSITY OF HOUSTON-CLEAR LAKE

Do not delete this notice. This material shall not be provided, copied or otherwise disseminated, in whole or in part to any party without the express written consent of the University of Houston-Clear Lake.

PASSWORD CONTROL

Purpose

To prevent unauthorized access to University of Houston -Clear Lake computer systems.

Scope

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

Standard

The Information Security Administrator (ISA) 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 appropriate intervals established in accordance with system risk assessments. (Scheduled by ISO)
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 should be formally notified as to their role in protecting the security of the username and password.
6. Passwords should have a minimum length of six characters.
7. Passwords stored on a computer should be encrypted in storage.
8. System software should enforce the changing of passwords and the minimum length and format.
9. The non-printing, password suppression feature should be used on all terminals to prevent the display of a user id or password at logon.
10. System software should disable the user identification code if more than three consecutive invalid passwords are given.
 - a. Student users: time-out after three (3) tries, disabled after six (6) tries.
 - b. Faculty/Staff users: disable after three (3) tries.

PROPERTY OF THE UNIVERSITY OF HOUSTON-CLEAR LAKE

Do not delete this notice. This material shall not be provided, copied or otherwise disseminated, in whole or in part to any party without the express written consent of the University of Houston-Clear Lake.

11. System software should maintain a history of at least two previous passwords and prevent their reuse.
12. Procedures for forgotten passwords should require that the user personally see the ISA or other control person to ensure password control, and present photo identification for re-issuance.

PROPERTY OF THE UNIVERSITY OF HOUSTON-CLEAR LAKE

Do not delete this notice. This material shall not be provided, copied or otherwise disseminated, in whole or in part to any party without the express written consent of the University of Houston-Clear Lake.

PERSONAL CONTROL PROCEDURES (FACULTY/STAFF)**NT ACCOUNTS / PHONEMAIL ACCESS**

Requesting NT Account, NT Password

To receive a NT account, the person requesting the account should:

1. Fill out a Request Form, available at the UCT Support Center (B2300).
2. Get completely filled out form signed by a manager.
3. Returned signed request form to the UCT Support Center.
4. It will take up to five (5) working days for the account to be enabled. Go to the UCT Support Center with photo identification.
5. At no time should a person allow someone else to use his or her account .
6. At no time should you leave your account logged on when you are away from the equipment you have used to log on.
7. Do not write down your password and leave it near your machine.
8. Make your password something uncommon, not a family members name or something easy to guess.
9. Password must be at least six (6) characters long.
10. A NT account password will not be reset over the telephone.
11. If a NT account is not accessed for six (6) months, the account will be disabled.

PROPERTY OF THE UNIVERSITY OF HOUSTON-CLEAR LAKE

Do not delete this notice. This material shall not be provided, copied or otherwise disseminated, in whole or in part to any party without the express written consent of the University of Houston-Clear Lake.

PHONEMAIL PASSWORD RESETTING

If a person is unable to access the phonemail box that is assigned to their extension, they must follow the following procedures to have it reset.

1. Fill out a Phone Work Request; forms are located at the UCT Support Center (B2300).
2. The request must then be signed by a manager or Business Coordinator.
3. Bring the signed request, along with a picture id before the request will be fulfilled.
4. At no time will a password be changed without a signed request.
5. Other than at the time of termination, a person should never give out their personal password. A password for a department's phonemail should be shared with a department manager, in case the person who normally handles the phonemail is out sick or on vacation.
6. The passwords should be at least four (4) characters long.
7. The password should be an uncommon group of characters that are not easy to guess.

TERMINATION

If an employee resigns the employee should go through terminal clearance, at which time they will be signed out for both their NT account and phonemail. If at all possible, the manager should ask the person who is resigning for their phonemail password so it can be reset quickly.

If an employee is to be let go under non-favorable conditions, before the person is told of their release, their manager should notify UCT and have UCT disable their NT access and their phonemail access.

PROPERTY OF THE UNIVERSITY OF HOUSTON-CLEAR LAKE

Do not delete this notice. This material shall not be provided, copied or otherwise disseminated, in whole or in part to any party without the express written consent of the University of Houston-Clear Lake.

USING SOFTWARE

Software enables us to accomplish many different tasks with computers. Unfortunately, in order to get their work done quickly and conveniently, some people justify making and using unauthorized copies of software. They may not understand the implications of their actions or the restrictions of the United States copyright law.

Unauthorized copying of software is illegal. Copyright law protects software authors and publishers, just as patent law protects inventors.

Unauthorized copying of software by individuals can harm the entire academic community. If unauthorized copying proliferates on a campus, the institution may incur a legal liability. Also, the institution may find it more difficult to negotiate agreements that would make software more widely and less expensively available to members of the academic community.

Unauthorized copying of software can deprive developers of a fair return for their work, increase prices, reduce the level of future support and enhancement and inhibit the development of new software products.

Respect for the intellectual work and property of others has traditionally been essential to the mission of colleges and universities. As members of the academic community, we value the free exchange of ideas. Just as we do not tolerate plagiarism, we do not condone the unauthorized copying of software, including programs, applications, data bases and code.

Therefore, we offer the following statement of principle about intellectual property and legal and ethical use of software. This "code" intended for adaptation and use by individual colleges and universities was developed by the EDUCOM Software Initiative.

SOFTWARE AND INTELLECTUAL RIGHTS

Respect for intellectual labor and creativity is vital to academic discourse and enterprise. This principle applies to works of all authors and publishers in all media. It encompasses respect for the right to acknowledgement, right to privacy and right to determine the form, manner and terms of publication and distribution.

Because electronic information is volatile and easily reproduced, respect for the work and personal expression of others is especially critical in computer environments. Violations of authorial integrity, including plagiarism, invasion of privacy, unauthorized access and trade secret and copyright violations may be grounds for sanctions against members of the academic community.

PROPERTY OF THE UNIVERSITY OF HOUSTON-CLEAR LAKE

Do not delete this notice. This material shall not be provided, copied or otherwise disseminated, in whole or in part to any party without the express written consent of the University of Houston-Clear Lake.

SYSTEM SOFTWARE

Purpose

To define policies and procedures relating to University of Houston-Clear Lake system software.

Scope

All University of Houston -Clear Lake 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. Online 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.

PROPERTY OF THE UNIVERSITY OF HOUSTON-CLEAR LAKE

Do not delete this notice. This material shall not be provided, copied or otherwise disseminated, in whole or in part to any party without the express written consent of the University of Houston-Clear Lake.

MODIFICATIONS TO SYSTEM SOFTWARE

Purpose

To define procedures for modifying system software.

Scope

All modifications to system software.

Standard

All system software modifications must adhere to University of Houston-Clear Lake defined policies and procedures regarding their development, testing, and implementation. Individual users are encouraged to consult with UCT prior to modifying system software.

Guidelines

1. System software modification implementation – The system programmer applying changes to system software must have an established back out plan, in case there are problems encountered during the implementation of the changes.
2. Separate test environment for system software programs – System software modifications 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.

PROPERTY OF THE UNIVERSITY OF HOUSTON-CLEAR LAKE

Do not delete this notice. This material shall not be provided, copied or otherwise disseminated, in whole or in part to any party without the express written consent of the University of Houston-Clear Lake.

SENSITIVE UTILITIES AND COMMANDS

Purpose

To ensure that sensitive programs and commands that can either bypass normal security controls or corrupt production systems have adequate procedures in place to control their use.

Scope

All application and system software in use at University of Houston -Clear Lake.

Standard

The ISA is responsible for identifying all sensitive programs in the system. The term “sensitive” is defined to include such items as programs that can be used to bypass access control software, commands to initiate/terminate the online environment, and data file/database low-level manipulation tools.

Guidelines

1. The use of these tools and commands shall absolutely be restricted to a “must need” basis.
2. The identification of sensitive utilities and commands is an ongoing process. The ISA must update and maintain the list of “sensitive” programs as new items are added to the operating environment.
3. Operating System Control of Maintenance Software – The operating system should permit access/execution of utility software only in the system state or privileged mode. This feature protects against covert modification of software. Special care should be taken in the control of utilities with all accessed and/or uses logged and reviewed on a daily basis.

PROPERTY OF THE UNIVERSITY OF HOUSTON-CLEAR LAKE

Do not delete this notice. This material shall not be provided, copied or otherwise disseminated, in whole or in part to any party without the express written consent of the University of Houston-Clear Lake.

AUTOMATED ACCESS CONTROL

Purpose

To prevent and detect unauthorized access (disclosure, modification, destruction and misuse) of data and software which can occur without requiring any physical access.

Scope

All computer systems at the University of Houston-Clear Lake containing sensitive or confidential information.

Standard

Any computer system, which contains sensitive or confidential information, must have a mechanism for restricting access to unauthorized individuals. This may include the use of access control software, passwords, encryption and restricted use or limited function input/output devices or communications systems.

Guidelines

1. The restriction software should log to a file all violations and unauthorized logon attempts, and generate reports as a means for the ISA to enforce access security.
2. Application access authority (emergency) access privileges – Any temporary update access given to application programmers will require documentation to the ISA, the reason for the access given and the resolution of the problem. The ISA will be responsible for the timely reimplementations of the prior access authority. The ISA should keep records of all these exceptions items.
3. Achieving privileged (supervisor) state – Any additions or changes to the contents of authorized libraries (or their functional equivalent) should be automatically logged by the access control software, and the list generated should be used to ensure that any changes are fully documented. This documentation should include a statement of why the particular changes are occurring. The documentation should be reviewed by the ISA.
4. Access control software use before application specific software – All use of any applications specific tables must be evaluated by the ISA to determine whether or not the same level of security can be provided by the general resources access control facilities in use. If the general resources access control facility can indeed accomplish the same access control, then it shall be used to secure the application, instead of the application specific security tables.

PROPERTY OF THE UNIVERSITY OF HOUSTON-CLEAR LAKE

Do not delete this notice. This material shall not be provided, copied or otherwise disseminated, in whole or in part to any party without the express written consent of the University of Houston-Clear Lake.

SYSTEM SURVEILLANCE

Purpose

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

Scope

All automated application systems in use at University of Houston-Clear Lake.

Standard

Ongoing monitoring of the entire computing environment must occur by an independent person (e.g., the ISA) 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 detected 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:
 - a. Unauthorized attempts to enter the system
 - b. All authorized or unauthorized attempts to access protected resources
 - c. All attempts to issue restricted commands
 - d. 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.

PROPERTY OF THE UNIVERSITY OF HOUSTON-CLEAR LAKE

Do not delete this notice. This material shall not be provided, copied or otherwise disseminated, in whole or in part to any party without the express written consent of the University of Houston-Clear Lake.

DATABASE ACCESS CONTROL, RECOVERY AND MAINTENANCE

Purpose

To ensure that any Data Base Management System (DBMS) in use has the appropriate integrity and access control mechanisms in place.

Scope

All DBMS software in use at the University of Houston-Clear Lake.

Standard

Reviews should occur for each application system utilizing DBMS software to ensure that the application is making appropriate use of logging, access control, and recovery features available within the DBMS.

Guidelines

1. Data Base Access Controls – Data base controls should be provided at the user, data, and process levels. Loggings of all accesses and attempted accesses should be available, and the DBMS should provide concurrent access controls and deadlock resolution.
2. Data Dictionary Controls – Certain data dictionary features enhance security in the database; these features include:
 - a. Level of integration – A highly integrated data dictionary requires greater security measures. Develop procedures to prevent misuse of the additional capabilities integration offers.
 - b. Access control – The data dictionary should have access controls to prevent any unauthorized use or modification.
 - c. Backup – Establish procedures for keeping a current copy of the data dictionary.
 - d. Certification/verifiability – Establish procedures for certification and verification of backup as well as production copies of the data dictionary.
 - e. Program restriction – The data dictionary should have registration capabilities to prevent unauthorized access or use.
3. Data Base Recovery – Provide the capability for rapid and efficient data base recovery, including:
 - a. Backup – Utilities, programs, and procedures should be available to provide backup for the database.

PROPERTY OF THE UNIVERSITY OF HOUSTON-CLEAR LAKE

Do not delete this notice. This material shall not be provided, copied or otherwise disseminated, in whole or in part to any party without the express written consent of the University of Houston-Clear Lake.

- b. Up-to-date copies – Current copies of all essential program codes and the like should be kept available and secure.
 - c. Documentation – Recovery and backup procedure documentation should be kept current.
 - d. Levels of recovery – Provisions for selective recovery and definitions of acceptable degradation of service should be specified.
4. Data Base Maintenance – Adequate facilities and procedures for data base maintenance are essential for data base security. These include:
- a. Vendor interface – Vendor maintenance procedures should be established to ensure that security is not compromised.
 - b. Ease of maintenance – Easy-to-maintain modules and well-defined software maintenance procedures are essential. The lack of proper maintenance can cause security breaches.
 - c. Maintenance responsibility – Clearly define maintenance responsibility and specify procedures for certification and verification.
 - d. Evaluation/certification – Establish requirements for the evaluation and certification of the DBMS, and keep a certified audit copy as backup. Documentation relating to the DBMS should be kept current with the operational version.

PROPERTY OF THE UNIVERSITY OF HOUSTON-CLEAR LAKE

Do not delete this notice. This material shall not be provided, copied or otherwise disseminated, in whole or in part to any party without the express written consent of the University of Houston-Clear Lake.

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-Clear Lake.

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 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 throughput), care must be taken that coding does not inadvertently weaken security and control.
6. Modifications should not be made to DC software without prior review and authorization by both the Director of Technical Services and ISA.
7. Communications hardware backup – Where practical, replacements should be available for critical communications hardware/circuitry, such as:
 - a. Modems
 - b. Multiplexers
 - c. Digital switches
 - d. Communications controller terminals

PROPERTY OF THE UNIVERSITY OF HOUSTON-CLEAR LAKE

Do not delete this notice. This material shall not be provided, copied or otherwise disseminated, in whole or in part to any party without the express written consent of the University of Houston-Clear Lake.

- e. Cluster controllers
 - f. Redundant leased (or dial-up) communication circuits
8. All 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.
 9. Automated techniques such as parity and redundancy checks should be used to help detect and correct data transmission errors.

PROPERTY OF THE UNIVERSITY OF HOUSTON-CLEAR LAKE

Do not delete this notice. This material shall not be provided, copied or otherwise disseminated, in whole or in part to any party without the express written consent of the University of Houston-Clear Lake.

NETWORK SECURITY

Purpose

To ensure integrity and availability of the University of Houston -Clear Lake computer data network.

Scope

All computer-connected information processing networks.

Standard

The Chief Information Services Officer (CISO) shall be responsible for the protection of the University of Houston-Clear Lake's information processing data network and the prompt elimination of security vulnerabilities within it.

An inventory of all communication lines shall be prepared and updated on an annual basis. The inventory shall include the facilities connected, a description of the data being handled, line identification and security controls employed.

Guidelines

1. Consideration as to cost reductions through network and equipment changes should be considered in conjunction with this inventory.
2. Hardware and software security measures such as locks and encryption should be used where appropriate.
3. UCT is solely responsible to make and remove any and all connections to the University's telecommunications and networking backbone/equipment.
4. Unsuccessful accesses to call back devices and see through security mechanisms should be monitored. Access control software is strongly recommended where appropriate.
5. Procedures must be in place to ensure that security violations are regularly reported to the ISA and the Chief Information Services Officer (CISO).
6. Network control functions should be restricted to operations personnel, and network control terminals should only be located inside the computer room.

PROPERTY OF THE UNIVERSITY OF HOUSTON-CLEAR LAKE

Do not delete this notice. This material shall not be provided, copied or otherwise disseminated, in whole or in part to any party without the express written consent of the University of Houston-Clear Lake.

TERMINAL CONTROLS

Purpose

To prevent unauthorized access to University of Houston -Clear Lake's data by providing terminal controls.

Scope

All University of Houston -Clear Lake terminals connected by leased line or dial up.

Standard

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

Guidelines

1. Restricted Input Points – Both physical and programmed restrictions should be developed on terminals that process critical transactions or capture critical data.
2. 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.
3. 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. A report should be created for use in identifying and locating terminals according to the ids.
4. The operating system should inspect logon requests to determine which application the terminal user desires. The user should identify an existing application and supply a valid username and password combination. If the logon request is valid, the operating system should make a logical connection between the user and the application.
5. Limitation of logon attempts – Limit system logon 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 ISA (and log of said message in an audit file), and purging of the input queue of messages from the terminal.
6. Process Lockout – Develop controls to restrict critical transactions to specific time periods such as normal working hours and prohibit their generation at any other time. Terminals used to process restricted transactions and critical files can be locked out physically and/or through system software controls.

PROPERTY OF THE UNIVERSITY OF HOUSTON-CLEAR LAKE

Do not delete this notice. This material shall not be provided, copied or otherwise disseminated, in whole or in part to any party without the express written consent of the University of Houston-Clear Lake.

7. Time-Out Feature – Ensure that the operating system provides the timing services required to support a secure operational environment. Both time-of-day clock and CPU (interval) timer facilities should be supported. Task management should use timer services to control and limit CPU use through scheduling algorithms. Inactive processes, or terminals (in an interactive environment) should be terminated after a predetermined period.
8. Dial-Up Control – Positive user authentication procedures should be in place for all dial-up facilities. The communications software should ensure a clean end of connection in all cases, especially in the event of abnormal disconnection.

PROPERTY OF THE UNIVERSITY OF HOUSTON-CLEAR LAKE

Do not delete this notice. This material shall not be provided, copied or otherwise disseminated, in whole or in part to any party without the express written consent of the University of Houston-Clear Lake.

Technical Security Requirements

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

Workstation Security Requirements

Workstations include personal computers (PCs), LANs, and LAN servers typically used in an office or laboratory environment.

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 will do the following:

LEVEL	REQUIREMENTS
3, 2, 1	<ul style="list-style-type: none"> - 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	<ul style="list-style-type: none"> - Ensure that the system configuration is documented - Establish backup requirements - Ensure that virus detection software is installed on each single user workstation

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 will apply.

Management, where multi-user workstations are installed, will implement a process that accomplishes the following:

PROPERTY OF THE UNIVERSITY OF HOUSTON-CLEAR LAKE

Do not delete this notice. This material shall not be provided, copied or otherwise disseminated, in whole or in part to any party without the express written consent of the University of Houston-Clear Lake.

LEVEL	REQUIREMENTS
3, 2	<ul style="list-style-type: none">- Documents system- Ensure that virus detection software is installed on 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- Assign a system administrator- Identify each user by a unique username and password- Provide secure backup storage external to the processing area- Ensure that critical data back-ups are placed in secure storage
1	<ul style="list-style-type: none">- Document system configuration- Ensure that virus detection software is installed on the workstation- Ensure the back-up requirement are established- Establish the development of a contingency plan
0	<ul style="list-style-type: none">- Document system configuration- Ensure that virus detection software is installed on the workstation- Establish back-up requirements

PROPERTY OF THE UNIVERSITY OF HOUSTON-CLEAR LAKE

Do not delete this notice. This material shall not be provided, copied or otherwise disseminated, in whole or in part to any party without the express written consent of the University of Houston-Clear Lake.

NETWORK DOCUMENTATION

Purpose

1. To facilitate equipment and line control.
2. To facilitate communications cost reduction.
3. To facilitate risk assessment and Emergency Recovery Procedures development.
4. To facilitate equipment inventory.

Scope

All University of Houston -Clear Lake communications lines specifically utilized in information processing and data communications.

Dial-up communication lines at the computer (port) end of the system.

Secondary dial-up communication lines at the user end of the system.

Standard

The Chief Information Services Officer (CISO) shall be responsible for the preparation and maintenance of a complete inventory of dedicated information processing and data communications lines.

Guidelines

1. The inventory shall be updated, at a minimum, on a quarterly basis.
2. The network inventory shall be a restricted use report. The report, or sections within it, shall be provided to persons and departments on a strict need-to-know basis.

PROPERTY OF THE UNIVERSITY OF HOUSTON-CLEAR LAKE

Do not delete this notice. This material shall not be provided, copied or otherwise disseminated, in whole or in part to any party without the express written consent of the University of Houston-Clear Lake.

IDENTIFYING REMOTE TERMINALS

Purpose

To ensure that inbound and outbound messages are transmitted to/from authorized remote equipment.

Scope

All devices not physically located at a University of Houston-Clear Lake facility.

Standard

Transmission techniques (protocols) should include device destination/origination identification information for each message transmitted.

Guidelines

1. Avoid use of transmission protocols (e.g., asynchronous) that do not include device-address data as part of the message packet.
2. In any instance when physical remote device validation is not possible or practical, other methods of validation should be in place.

PROPERTY OF THE UNIVERSITY OF HOUSTON-CLEAR LAKE

Do not delete this notice. This material shall not be provided, copied or otherwise disseminated, in whole or in part to any party without the express written consent of the University of Houston-Clear Lake.

DIAL-UP COMMUNICATIONS CONTROL

Purpose

To secure all dial-up remote access to University of Houston-Clear Lake computing facilities.

Scope

All dial-up communication links shall have the appropriate hardware mechanisms and/or manual procedures in place to minimize the possibility of unauthorized external access occurring.

Guidelines

1. Phone numbers for dial-up ports should be considered confidential data, and users of said dial-up links should be informed as to their responsibilities in restricting distribution of the numbers.
2. Use of the dial-back equipment or see-through security should be mandatory for any auto-answer connection to a University of Houston-Clear Lake computer system.
3. Updating the security table within the callback devices should occur immediately when an employee using the dial-up system leaves the organization or changes job responsibilities.

PROPERTY OF THE UNIVERSITY OF HOUSTON-CLEAR LAKE

Do not delete this notice. This material shall not be provided, copied or otherwise disseminated, in whole or in part to any party without the express written consent of the University of Houston-Clear Lake.

SYSTEM IDENTIFICATION SCREEN

Purpose

To ensure that system identification screen is displayed on all terminals.

Scope

All authorized University of Houston-Clear Lake terminal equipment.

Guidelines

1. The system identification screen should be implemented so that a user cannot bypass it.
2. The system identification screen should remain on display for a sufficient amount of time for the message to be read.
3. The system identification screen shall include notices regarding:
 - a. System access
 - b. Legal liabilities; and
 - c. That system use is subject to security testing and monitoring.

PROPERTY OF THE UNIVERSITY OF HOUSTON-CLEAR LAKE

Do not delete this notice. This material shall not be provided, copied or otherwise disseminated, in whole or in part to any party without the express written consent of the University of Houston-Clear Lake.

PHYSICAL SECURITY OF COMMUNICATIONS EQUIPMENT

Purpose

1. To prevent interruption of communications caused by physical damage to communications equipment.
2. To prevent interruptions of communications and breaches of integrity caused by malicious interferences with communications equipment.

Scope

All communications equipment including terminals, modems, multiplexers, telephone cables, telecommunications switching devices, servers, and network hardware.

Standard

Adequate physical security must be provided for all visible communications equipment.

Guidelines

1. Provide adequate physical security for all communications equipment (i.e., telephone cable rooms, cable runs) where physical wiretapping is possible. Measures to be taken include:
 - a. Enclosure of all communications apparatus (e.g., phone closets) in areas that can be locked and physically secured.
 - b. Installation of cipher locks or magnetic key card devices on doors leading to wiring rooms or closets.
 - c. Installation of magnetic contact alarms and motion detectors in areas that are not subject to 24-hour human surveillance.
2. Provide all modems, multiplexers, and patch panels with adequate physical security, including:
 - a. Limitation of access to authorized personnel only
 - b. Placement of modems, multiplexers, and other equipment in areas such as the network control center where they can be under 24-hour surveillance.

In remote equipment areas, closed circuit television coverage and/or installation of electronic intrusion detection systems.

PROPERTY OF THE UNIVERSITY OF HOUSTON-CLEAR LAKE

Do not delete this notice. This material shall not be provided, copied or otherwise disseminated, in whole or in part to any party without the express written consent of the University of Houston-Clear Lake.

3. Fiber Optic Cable – Consider using fiber optic cable, where appropriate, to prevent physical wiretapping. Because fiber optics uses light as the transmission medium, any break in the integrity of the cable (such as that created by a wiretap) will destroy the cable's conductivity, reducing the possible attachment of a tap without causing a noticeable disruption in communications.
4. Shielded Cable – Consider using shielded cable (coaxial cable) where appropriate, to minimize electromagnetic radiation and design the configuration so that any attempt to tap will result in destruction of the circuit and/or activation of alarm sensors.

PROPERTY OF THE UNIVERSITY OF HOUSTON-CLEAR LAKE

Do not delete this notice. This material shall not be provided, copied or otherwise disseminated, in whole or in part to any party without the express written consent of the University of Houston-Clear Lake.

DATA TRANSFER BETWEEN COMPUTERS

Purpose

To ensure that the proper security mechanisms and procedures are in place to control the transfer of information between computer systems.

Scope

All computer systems at the University of Houston-Clear Lake that contain or process critical or sensitive information.

Standard

Any transfer of data files from one computer center to another must include mutual validation of the identity of the transmitting and receiving computers prior to allowing the transfer to occur. This validation process must adhere to the University of Houston-Clear Lake policy regarding individual authentication.

Guidelines

1. Use of user identification and passwords to authenticate is a viable mechanism, as are certain hardware security keys and other see-through security mechanisms.
2. Data encryption for remote transmission can also enhance data transfer security.
3. Positive control of all data transfers between files and logical devices should be maintained through the operating system. Performing error and parity checking on each fetch and transfer cycle prevents the injection of malicious or inadvertent errors into the system during data transfer.
4. Avoid the use of transmission protocols that do not have parity checking and error recovery facilities.

PROPERTY OF THE UNIVERSITY OF HOUSTON-CLEAR LAKE

Do not delete this notice. This material shall not be provided, copied or otherwise disseminated, in whole or in part to any party without the express written consent of the University of Houston-Clear Lake.

APPENDIX A

**UHCL AUTOMATED INFORMATION SYSTEMS
ACCEPTABLE USE POLICY**

PROPERTY OF THE UNIVERSITY OF HOUSTON-CLEAR LAKE

Do not delete this notice. This material shall not be provided, copied or otherwise disseminated, in whole or in part to any party without the express written consent of the University of Houston-Clear Lake.

UHCL AUTOMATED INFORMATION SYSTEMS ACCEPTABLE USE POLICY

The University's automated information systems, data processing equipment, information assets, and network systems are a valuable and unique resource dedicated to promoting educational excellence. To allow the University to provide quality, equitable, and cost effective information and communication resources to the educational community, system users must regard it as a shared resource and cooperate as a diverse community for common purposes. It is therefore imperative that users conduct themselves in a responsible, ethical, and polite manner while using these automated information systems. In accordance with the Texas Department of Information Resources and UHCL's Information Resources Security Policies, all users are expected to abide by the following guidelines as an Automated Information Systems Agreement of Understanding:

1. Use of UHCL's automated information systems is for authorized users engaged in educational or research pursuits. Unauthorized use is prohibited and subject to Federal, state, civil, and criminal laws.
2. Use of UHCL's automated information systems for any commercial purpose, including product advertisement, or political lobbying is prohibited. (TAC 201.13b; Vernon's Annotated Texas Codes 556.004)
3. Users are expected to honor all software license agreements and abide by copyright laws. The University does not knowingly permit its equipment to be used in the violation of such conditions. Failure to honor these agreements and laws could have legal ramifications.
4. Users have their own logon accounts to UHCL's shared automated information systems to provide personal accountability for activities. Computer accounts, passwords and other types of authorization codes should not be shared with others.
5. Users shall not leave a terminal or microprocessor unsecured or unattended when it is logged on to a host computer or network.
6. Users of UHCL's shared automated information systems shall not disrupt other user's use of the system. This includes distribution of computer viruses or other obstructive programs.
7. Users shall abide by the security procedures for UHCL automated information systems and have the responsibility to report security problems to the University Computer Support Center at extension 2828 or in B2300.
8. Students are responsible for backing up stored work on their own disks.

PROPERTY OF THE UNIVERSITY OF HOUSTON-CLEAR LAKE

Do not delete this notice. This material shall not be provided, copied or otherwise disseminated, in whole or in part to any party without the express written consent of the University of Houston-Clear Lake.

APPENDIX B

Information Resources Security Policy

PROPERTY OF THE UNIVERSITY OF HOUSTON-CLEAR LAKE

Do not delete this notice. This material shall not be provided, copied or otherwise disseminated, in whole or in part to any party without the express written consent of the University of Houston-Clear Lake.

Information Resources Security Policy

GENERAL POLICY STATEMENT:

Scope: This policy applies to all personnel in the University of Houston-Clear Lake (UHCL) who use UHCL supplied or funded information resources.

SPECIFIC POLICY STATEMENTS:

1. Access to and use of, computing resources is restricted to appropriately identified, authenticated and authorized users. State law requires that state-owned information resources be used only for official state purposes.
2. All identification, passwords, telephone numbers, and other "access means" to information resources are confidential and proprietary to the state. Holders of such access means are accountable for unauthorized or negligent disclosure or use of access means under their control. No individual may access data or other information resources that are not authorized for access by that individual. Authorization is on a "need-to-know" basis. Personnel are not to share assigned passwords with anyone.
3. All computer programs, software and electronic information that are part of information resources are property of the UHCL and must not be copied or disclosed unless explicitly authorized by appropriate management in writing. This includes software developed for or by UHCL and UHCL purchased software and its related documentation.
4. All computer-generated reports are the property of UHCL. Personnel may not use these reports except for internal university business, or as required by their job.
5. No hardware or any type of telecommunications device may be connected to any part of a state network, computers, terminals, or lines unless explicitly authorized in writing by appropriate management and in conformance with security policies, procedures, and standards.
6. No software, program, or information can be added to, or removed from, any operating system, database, or file unless explicitly authorized by appropriate management and in conformance with institutional security policies, procedures, and standards. Additionally, software that can bypass, in any manner, approved security software or controls may not be written or installed.
7. Personnel shall not disclose any information designated or otherwise marked as confidential or sensitive information unless it is properly required in their job, or except as authorized in writing pursuant to security policies. Such information includes technical and business information, information systems and software development, and products and software licenses disclosed on a confidential basis to the institution.

PROPERTY OF THE UNIVERSITY OF HOUSTON-CLEAR LAKE

Do not delete this notice. This material shall not be provided, copied or otherwise disseminated, in whole or in part to any party without the express written consent of the University of Houston-Clear Lake.

8. Upon termination of employment or at the end of a contractual relationship with the state, or as otherwise requested by appropriate management, personnel must surrender all property and information of the agency that is in their possession and must not subsequently disclose any confidential or sensitive information.
9. Personnel, upon termination or position changes, must reverify their requirements for access to the agency's information resources. Having not received reverification within 30 days of notice of transfer, IDs belonging to the transferred individual will be revoked.

VIOLATIONS OF THIS POLICY

It is the responsibility of all personnel to report any suspected or confirmed violations of this policy to appropriate management. Reports may be oral or written. Failure to do so may result in disciplinary action.

Any person violating this policy is subject to immediate disciplinary action, which may include termination of a contract. In addition, there may be cases in which a person may be subjected to civil and criminal legal sanctions when a violation occurs. Both Texas and Federal law provide punishments for unauthorized access and other computer/communications related crimes. Federal law may apply when the crime is committed on a computer or communications device that communicates to another device outside of the state.

PROPERTY OF THE UNIVERSITY OF HOUSTON-CLEAR LAKE

Do not delete this notice. This material shall not be provided, copied or otherwise disseminated, in whole or in part to any party without the express written consent of the University of Houston-Clear Lake.