ADMINISTRATIVE POLICY STATEMENT

Policy Title: IT Security Program Policy

Functional Area: Information Technology

Brief Description: The IT Security Program serves as the core for the Institute's *IT security* activities and provides general guidance to the computing community on ensuring the privacy of personal information and the availability of *Institution information* and *IT resources*. This Administrative Policy Statement encompasses all IT Security-related requirements as outlined in the following policy sections:

Effective: December 1, 2019

Approved by: President, Melanie Kaye Washington

Responsible Institution Officer: Dean of Business Affairs, Ronald Kendall Washington

Applies to: Institution wide or as specifically defined by each policy section.

Reason for Policy: Establishes the required roles, responsibilities, and functions for the effective management of the Institute's IT Security Program and provides general guidance to the computing community on ensuring the privacy of personal information and the availability of *Institution information* and *IT resources.*

IT SECURITY PROGRAM

Policy Overview: IT Security Program

I. INTRODUCTION

This Administrative Policy Statement is the parent policy for the Institute's Information Technology (IT) security policy suite, which defines and establishes the *IT Security Program* (Program). The Program serves as the core for the Institute's *IT security* activities and provides general guidance to the computing community on ensuring the privacy of personal information and the availability of *Institution information* and *IT resources*.

More specifically, this policy assigns responsibilities for the oversight and day-to-day management of the Program. These fundamental responsibilities are essential to ensuring that the Program provides timely and effective guidance to the Institution computing community in the face of almost continuous change. The effectiveness of this guidance requires that the Program be frequently reviewed and molded to fit the evolving needs of the Institution and its stakeholders. This policy also includes the following IT-security related sections:

II. POLICY STATEMENT

A. The goals of the Institution *IT Security Program* are as follows:

1. All members of the Institution community are aware of and are sufficiently trained to carry out their responsibilities for protecting *Institution information* and *IT resources*.
2. *Institution information* is regarded as a strategic organizational asset and is treated in a manner consistent with that of other strategic assets, such as financial and facility assets.
3. *IT security* is not considered a technical concern, but is addressed as a strategic business issue by integrating *IT security* safeguards into Institution business processes.
4. Institution resources are applied judiciously to *IT security* issues by focusing on those that represent the greatest risk to Institution operations and information.
5. *IT security* incidents are promptly detected and responded to in a manner that limits the impact to the security of *Institution information* and the operations of the Institution.

B. The following principles shall be followed in implementing the Institution *IT Security Program*:

1. Each campus shall adopt all applicable elements of the Program and may make modifications to specific Program elements to meet special campus needs as long as the modifications are as stringent as and meet the intended functionality of the applicable Program elements.
2. *Risk management* methods shall be used to identify and manage risks to *Institution information* and *IT resources*. *Risk management* decisions shall be made by appropriate authorities with jurisdiction over those areas affected by the risks.
3. *Institution information* shall be adequately protected regardless of the information's physical location, the nature of the device or media upon which it is stored, or the persons in possession or control of the information.

C. Roles and Responsibilities for the Institution *IT Security Program*.

1. The Program shall be managed and monitored collaboratively by the Dean of Business Affairs, campus *Information Security Officer*, Jennyfer Henderson, and other Institution representatives as appropriate. Program management responsibilities are as follows:
    a. Dean of Business Affairs
        1. Provide day-to-day management for the Program. Review and report on Program effectiveness to the *President* as appropriate.
        2. Oversee the development and maintenance of Administrative Policy Statements for *IT security* and advise campus *Information Security Officers* on the alignment of campus *IT security* policies with Administrative Policy Statements.
        3. Provide guidance to campus VP of Student Affairs on *risk management* processes to ensure that *IT security* safeguards are applied in a judicious and effective manner. Submit reports to the President on *risk management* decisions as appropriate.
        4. Establish training standards for campus *IT security* awareness and education programs.
        5. When *IT security* incidents affect the campus, lead investigations and coordinate with and/or report to the *President*, and others as appropriate.
    b. Vice-President of Student Affairs

        1. Jennyfer Henderson will provide day-to-day security advice to the *President*, Dean of Business Affairs, and contractor(s) *Information Security Officers (FAME & Complete Computer Services)* in accordance with Program goals and requirements.
        2. The VP of Student Affairs is the individual designated by the President on campus with oversight authority for all IT operations on campus. This individual has the authority to enforcethe requirements of Institution and campus policies for information security.
        3. Authorize new IT operations, shut down IT operations that are out of compliance with policy, or transfer management of those operations to a department or service provider with the requisite capabilities.
    c. SAC (Security Advisory Committee)
    The SAC provides oversight of and support for the *IT Security Program* and is composed of members of the Advisor Board of the Institution and the President, VP Student Affairs, VP Academic Affairs, and Dean of Business Affairs. SAC members are appointed by the *President* or designee.
        1. Advise, inform, and coordinate with the Dean of Business Affairs as appropriate to promote and support the Program and to ensure that Program requirements reflect and support the functional requirements, external requirements, and the mission of the Institution.
        2. Advise the *President* as appropriate to ensure that Institution-wide *IT security* policies, procedures, and guidelines reflect and support the functional requirements, external requirements, and the mission of the Institution.
        3. In collaboration with the Dean of Business Affairs advise the Institution *President* on *risk management* decisions and Program direction to ensure alignment with Institution objectives.

2. Although campus *Information Security Officers* provide day-to-day management of the Program and general advice on *IT security* issues, the following campus support responsibilities are required:

a. *Organizational Unit* (the Business Affairs department with an independent financed budget) ensuring that all applicable Programand *IT security* policy requirements are implemented in their respective units. The purpose of this unit is to design a reporting system of any security weaknesses, concerns, or breaches to the Dean of Business Affairs. The Dean of Business Affairs will work with the appropriate staff and information security contractors to determine if the risk caused by a security weakness may be accepted.
b. *IT service providers* (e.g., webmasters, network engineers, server administrators, application developers, desktop support staff, or database administrators) shall implement all applicable Program and *IT security* policy requirements within their areas of responsibility. *IT service providers* shall evaluate the effectiveness of *IT security* safeguards in their areas of responsibility and report any security weaknesses, concerns, or breaches to the campus *Information Security Officer*.
c. *VP of Student Affairs will be the Data Trustee* responsible and recognized to have primary authority and decision responsibility over a particular collection of institution data. Data trustees are accountable formanaging, protecting, and ensuring the integrity and usefulness of institution data. Data trustees have the primary responsibility to ensure the institution is following its policies and is in compliance with federal and state laws and regulations. Data trustees typically are associated with the business functions of an organization rather than technology functions. Additional duties include control over a data asset's disposition, whether stored (at rest), in transit, or during creation. Will have modification or distribution privileges and carry a significant responsibility to protect data and prevent unauthorized use. As a data user, will have the responsibility to manage and protect data by understanding and following the IT and information security policies of the institution related to data use.

D. Any exceptions to this policy must be approved by the Dean of Business Affairs or President

IT SECURITY PROGRAM

Section 1: IT Resource User Responsibilities

Brief Description: Establishes *IT security* requirements for all *IT resource users* in protecting *Institution information* and *IT resources*.

Applies to: *IT Resource Users*

SECTION 1 – IT RESOURCE USER RESPONSIBILITIES

I. INTRODUCTION

This section of the IT Security Program Policy establishes the Information Technology (IT) security safeguards that must be taken by every person using an Institution *IT resource* or otherwise accessing *Institution information*. Additional safeguards may be appropriate, depending on the situation and its inherent risk to *Institution information* and *IT resources*.

This policy does not impose restrictions that are contrary to the Institute's established culture of sharing, openness, and trust. However, the Institution is committed to implementing the safeguards necessary to ensure the privacy of personal information, the availability of *Institution information* and *IT resources*, and the integrity of Institution operations.

HTIM has three levels of data classification. These are: *Highly Confidential*, *Confidential*, and *Public*.

II. POLICY STATEMENT

A. It is the responsibility of every *IT resource user* to know the Institute's *IT security* requirements and to conduct her/his activities accordingly. *IT resource users* shall comply with the following requirements:

1. **Protect the Privacy of Others.** Users shall respect the privacy of others when handling *Highly Confidential information* and shall take appropriate precautions to protect that information from unauthorized disclosure or use.

2. **Protect *Highly Confidential* or *Confidential Information* on Workstations and Mobile Devices.** Ordinarily, *Highly Confidential information* shall not be stored on workstations and mobile computing devices (laptops, flash drives, backup disks, etc.) unless specifically justified for business purposes and adequately secured. If *Highly Confidential information* is stored on a workstation or mobile computing device or transmitted to an external network or organization, *IT resource users* shall *encrypt* or adequately protect that information from disclosure. If *Confidential information* is stored on a workstation or mobile computing device or transmitted to an external network or organization, *IT resource users* shall adequately protect that information from disclosure. In addition to *encryption*, adequate protections may include the use of passwords, automatic logoffs, and secure Internet transmissions. IT Resource users are required to secure institution information on personally owned and/or institutionally provided mobile devices in accordance with the mobile device security standards. The protection of Highly Confidential or *Confidential information* shall be in accordance with campus *IT security* requirements and other guidance as available from the appropriate IT service center or help desk.

3. **Protect Highly Confidential Data from Unauthorized Physical Access.** *IT resource users* shall keep all *Highly Confidential* or *Confidential information* out of plain sight unless in use and shall not leave such information displayed when it is not needed.

---

4. **Protect Workstations and Other Computing Devices.** *IT resource users* are responsible for helping to maintain the security of workstations and other computing devices by striving to protect them from unauthorized access and malicious software infections (e.g., viruses, worms, and spyware). Users shall consult the appropriate IT service center or help desk for guidance on protecting their computing devices.

5. **Protect Passwords, Identification Cards, and Other Access Devices.** Passwords, identification cards, and other access devices are used to authenticate the identity of individuals and gain access to Institution resources. Each person is responsible for protecting the access devices assigned to her or him and shall not share passwords or devices with others. If a password or access device is compromised, lost, or stolen, the individual shall report this to the appropriate IT service center or help desk as soon as possible so that the access device is not used by an unauthorized person.

6. **Report Security Violations, Malfunctions, and Weaknesses.** *IT resource users* shall report security related events; known or suspected violations of *IT security* policy; and inappropriate, unethical, and illegal activities involving Institution *IT resources*. Users shall follow the reporting process applicable to their campus. If unsure of the local incident reporting process, users shall call the appropriate IT service center or help desk.

7. **Utilize *Institution Information* and *IT Resources* for Authorized Purposes Only**. *IT resource users* shall access or otherwise utilize *Institution information* and *IT resources* only for those activities they are specifically authorized and in a manner consistent with Institution policies, federal and state laws, and other applicable requirements.

III. RELATED POLICIES, PROCEDURES, FORMS, GUIDELINES, AND OTHER RESOURCES

A. Administrative Policy Statements (APS) and Other Policies

The IT Security Program serves as the core for the Institute's *IT security* activities and provides general guidance to the computing community on ensuring the privacy of personal information and the availability of *Institution information* and *IT resources* and encompasses all related IT Security requirements, including the following policy sections:

IT Resource User Responsibilities
IT Security in Personnel Job Descriptions, Responsibilities and Training
IT Security in Institution Operations, Business Continuity Planning, and Contracting
IT Service Provider Security

The Laws of the Regents, section 14.A.4 states that *employees* shall be responsible for the safekeeping and proper maintenance of institution property in their charge. The administrative policy "Fiscal Code of Ethics" prohibits use of Institution property for personal gain.

The "Use of Electronic Mail" Administrative Policy Statement sets forth the appropriate use of Institution email and expectations for privacy in email communications.

System-wide Mobile Device Security Standards
Standards for Data classification and System security categorization

B. Other Resources (i.e. training, secondary contact information)

Educational information and resources are available on the Office of Information Security website www.htim.edu.

IT SECURITY PROGRAM

Section 2: IT Security in Personnel Job Descriptions, Responsibilities and Training

Brief Description: Establishes requirements for incorporating employee responsibilities for *IT security* into performance management processes, as well as ensuring *employees* are aware of their *IT security* responsibilities and are adequately trained to fulfill those responsibilities.

Applies to: Management

SECTION 2 – IT SECURITY IN PERSONNEL JOB DESCRIPTIONS, RESPONSIBILITIES AND TRAINING

I. INTRODUCTION

Information technology (IT) security responsibilities are, to various degrees, part of all duties within the Institution. For *employees* and job candidates it is important that the applicable *IT security* responsibilities are known, documented, and accepted as part of the terms and conditions of employment.

II. POLICY STATEMENT

A. *IT Security* Guidance and Support

1. Campus *Information Security Officers* shall, in collaboration with the Dean of Business Affairs (CISO), provide information and guidance to supervisors on implementing the requirements of this policy.
2. Campus *Information Security Officers* shall establish and oversee *IT security* awareness and education programs for their respective campuses.

B. Management Responsibilities for *IT Security*

1. Management shall ensure that all *employees* within their areas of authority are aware of their *IT security* responsibilities and that these responsibilities are incorporated into *employee* performance managementprocesses and addressed in recruitment and hiring practices.
2. Management shall ensure that *employees* provide a signed, written, or other documented acknowledgment of their *IT security* responsibilities as a condition of gaining access to *Institution information* and *IT resources*.Where feasible, acknowledgements should be provided prior to gaining access or as soon afterward as reasonably possible. Personnel supervising authorities shall track and/or maintain the records of *employee* acknowledgements.
3. Management in consultation with the campus *Information Security Officer*, are encouraged to make recommendations on the designation of positions with significant *IT security* responsibilities as "security-sensitive positions."

C. *Employee* Training

1. Management shall ensure that *employees* are adequately trained to fulfill their *IT security* responsibilities. *Employees* with elevated computing privileges (e.g., server support technicians, user account managers, or web page administrators) may require additional, specialized training for carrying out their *IT security* responsibilities effectively.
2. All Institution *employees* including associates and other individuals, who require the use of Institution *IT resources* to perform their duties, shall receive initial training and periodic refresher training relevant to their *IT security* responsibilities.
3. Management shall coordinate their local *IT security* training initiatives with the campus *Information SecurityOfficer*.

D. Changes in *Employee* Duties or Employment Status

1. Management shall provide timely notification to the appropriate service center or help desk when an *employee*'s duties or employment status changes so that access to *Institution information* and *IT resources* is adjusted accordingly.

III. RELATED POLICIES, PROCEDURES, FORMS, GUIDELINES, AND OTHER RESOURCES

A. Administrative Policy Statements (APS) and Other Policies

The IT Security Program serves as the core for the Institute's *IT security* activities and provides general guidance to the computing community on ensuring the privacy of personal information and the availability of *Institution information* and *IT resources* and encompasses all related IT Security requirements, including the following policy sections:

IT Resource User Responsibilities
IT Security in Personnel Job Descriptions, Responsibilities and Training
IT Security in Institution Operations, Business Continuity Planning, and Contracting
IT Service Provider Security

The "Use of Electronic Mail" Administrative Policy Statement sets forth the appropriate use of Institution email and expectations for privacy in email communications.

B. Procedures

IT Security Training Standards and Core Topics

C. Other Resources (i.e. training, secondary contact information)

Educational information and resources are available on the information security website: www.htim.edu.

IT SECURITY PROGRAM

Section 3: IT Security in Institution Operations, Business Continuity Planning, and Contracting

Brief Description: Requires *IT security* safeguards to be integrated into Institution operations, asset management, contracting, *business continuity* planning, *disaster preparedness*, and enterprise *risk management* processes.

Applies to: *Management/Organization Units*

SECTION 3 – IT SECURITY IN INSTITUTION OPERATIONS, BUSINESS CONTINUITY PLANNING,AND CONTRACTING

I. INTRODUCTION

Institution operations are organized into *Organizational Units* that develop and execute strategic and tactical plans to carry out the Institute's mission and achieve its objectives. In doing so, these units collect, store, and process information that is essential to Institution operations and must be protected from unauthorized use and disclosure. To ensure that *Institution information* is protected in a manner consistent with other strategic assets, *Organizational Units* must implement Information Technology (IT) security safeguards as a part of normal Institution operations.

II. POLICY STATEMENT

A. *IT Security* Guidance and Support

1. Campus *Information Security Officers* shall, in collaboration with the Dean of Business Affairs (CISO), provide information and guidance to *Organizational Units* on implementing the requirements of thispolicy.

B. Information Classification

1. Campus *Information Security Officers* shall provide security standards based on the criticality and sensitivity of *Institution information* for their respective campuses.
2. *Organizational Unit* directors / chairs or their designees shall, following guidance from the campus *Information Security Officer*, ensure that appropriate *IT security* safeguards are in place for the *Institution information* and *IT resources* under their care. The appropriateness of the safeguards shall be determined by the criticality and sensitivity of information involved, campus policies and guidance, and applicable external requirements (e.g., state and federal laws, and industry standards).

C. Continuity of Operations

1. *Organizational Unit* directors / chairs or their designees, with guidance from the campus *Information Security Officer*, shall ensure that *business continuity* and *disaster preparedness* plans include all appropriate *IT security* requirements and are reviewed, tested, and updated as needed to ensure the viability of such plans.

D. *IT Security* Requirements in RFPs, Contracts, and Other Service Arrangements

1. *Organizational Unit* directors / chairs or their designees shall, with guidance from the Procurement Service Center and the *Information Security Officer*, ensure that Request for Proposals (RFP), contracts, or other service arrangements include adequate safeguards so that contractors and other third parties protect *Institution information* at a level that is equal to or greater than that required of Institution *employees.*
2. *Organizational Unit* directors / chairs or their designees, with guidance from the campus Information Security Officers, shall ensure that access to *Institution information* and *IT resources* by contractors and third parties follows established policies and procedures.

E. Risk Evaluation and Handling

1. *Organizational Unit* directors / chairs or their designees shall, with guidance from the campus *Information Security Officer*, evaluate risks related to the protection of *Institution information* and *IT resources* in their care. *Organizational Unit* directors / chairs or their designees shall forward issues of risk to campus authorities with appropriate jurisdiction over those affected by the risks.

III. RELATED POLICIES, PROCEDURES, FORMS, GUIDELINES, AND OTHER RESOURCES

A. Administrative Policy Statements (APS) and Other Policies

The IT Security Program serves as the core for the Institute's *IT security* activities and provides general guidance to the computing community on ensuring the privacy of personal information and the availability of *Institution information* and *IT resources* and encompasses all related IT Security requirements, including the following policy sections:

IT Resource User Responsibilities
IT Security in Personnel Job Descriptions, Responsibilities and Training
IT Security in Institution Operations, Business Continuity Planning, and Contracting
IT Service Provider Security

The Laws of the Regents, section 14.A.4 states that *employees* shall be responsible for the safekeeping and proper maintenance of institution property in their charge.

B. Other Resources (i.e. training, secondary contact information)

Educational information and resources are available on the Office of Information Security website www.htim.edu.

IT SECURITY PROGRAM

Section 4: IT Service Provider Security

Brief Description: Requires that *IT service providers* (e.g., server and workstation support, programmers, webmasters, user account administrators) incorporate *IT security* safeguards into the IT services and products provided to the Institution community.

Applies to: *IT Service Providers*

SECTION 4 – IT SERVICE PROVIDER SECURITY

I. INTRODUCTION

This section of the IT Security Program Policy sets forth the Information Technology (IT) security safeguards that must be taken by every *IT service provider*. These safeguards are necessary to protect *Institution information* from inappropriate access, disclosure and misuse; provide assurances that information resources are available as needed for Institution business; and comply with applicable policies, laws, regulations, rules, grants, and contracts. Campus *Information Security Officers* may require additional safeguards so as to address campus specific risks or compliance requirements.

II. POLICY STATEMENT

A. *IT Security* Oversight and Guidance

Campus *Information Security Officers* in collaboration with the Dean of Business Affairs (CISO) shallprovide guidance and information as needed to *IT service providers* on implementing the requirements of this policy. *IT service providers* shall be aware that purchases of IT goods and services may be subject to a security review by the campus *Information Security Officer* or a designated campus authority.

Organizational Unit directors / chairs shall be aware of their responsibilities, as described by IT Security in Institution Operations, Continuity, and Contracting, to ensure that adequate safeguards are implemented for the *IT resources* under their control.

B. Life Cycle Management

Campus *IT service providers* shall ensure that *IT security* controls are appropriately implemented and managed throughout the life of the *IT resources* under their responsibility. This is to ensure that security is addressed in the design and purchase of new systems, implementation of new or modified systems, maintenance of existing systems, and removal from service of end-of-life systems.

C. *IT Resource* Security Management

Providing an IT service is a complex undertaking that requires continuous monitoring, maintenance, and system management to ensure that *Institution information* is adequately protected as it is processed, stored, and transmitted. Therefore, *IT service providers* shall implement the following controls where appropriate for the *IT resources* under their responsibility:

1. System and application security management. *IT resources* shall be maintained according to industry and vendor best practices to ensure that system and application updates, vulnerability fixes, security patches, and other modifications are applied in a timely fashion. Where applicable these practices shall include vulnerability management, system/application hardening, and security testing.

2. Malicious activity protection. *IT resources* that transmit or receive information on a Institution-managed network shall be adequately protected from malicious activities, such as viruses, worms, and denial of service attacks.

3. Data backup and recovery. *Institution information* shall be backed up and retained as appropriate for business needs, **retention** schedules, and legal requirements as provided by law or related institution policy. Data backups shall be tested where appropriate to ensure the effective recovery of information.

4. Media handling and storage. Electronic storage media (e.g., CD-ROMs, memory sticks, disk drives, tapes, cartridges, etc.) shall be appropriately protected from loss and unauthorized access. All media containing Highly Confidential and *Confidential information* shall be stored in a secure location and adequately protected with a safeguard that restricts access to authorized personnel only. In addition, Highly Confidential information stored on portable electronic media shall be encrypted or otherwise adequately protected based on security standards and guidance from the campus Information Security Officers.

5. Disposal of electronic equipment and media. Computing and network equipment and storage media shall be purged of all *Institution information* so that information is not recoverable, or destroyed before disposal or release from Institution control to a third party. In the rare event the information is not purged prior to release or the device destroyed prior to disposal, the *IT service provider* shall acquire confirmation from the contracted third party that the information is properly purged. For equipment and media that is to be redeployed within the Institution, the *IT service provider* shall purge all information not authorized for access by the receiving person(s) prior to redeployment.

D. **Access Management**

Although *students*, faculty, and staff require access to *Institution information* resources for academic and business purposes, this access must be limited to what is needed for his/her work. Use of resources beyond that which is authorized results in unnecessary risks to *Institution information* with no corresponding academic or business value.

1. User access management. *IT service providers* shall manage user access to the *IT resources* under their responsibility, so that such access is appropriately authorized, documented, and limited to that which is needed to perform authorized tasks. Because a user's responsibilities and relationships with the Institution change over time, *IT service providers* shall ensure that user access privileges are regularly reviewed and adjusted to comply with currently authorized activities.

2. *IT resource* access controls. *IT service providers* shall ensure that *IT resources* under their responsibility (developed, purchased or otherwise used to handle *Institution information*) have adequate features and controls to support the proper management of user access as described in section II.D.1.

3. Network security controls. *IT service providers* shall ensure that electronic access to and use of the campus data networks under their responsibility is adequately controlled to protect data network equipment and other networked *IT resources*.

E. **Physical and Environmental Security**

Institution data centers and *IT resources* shall be sufficiently protected from physical and environmental threats to prevent the loss, damage, or compromise of assets, and interruption to business activities.

1. Data centers. Data center owners, managers, or their designees shall, following guidance from the campus *Information Security Officer*, ensure that data center facilities under their responsibility have adequate physical security safeguards. These safeguards may include: physical barriers (e.g., walls, gates, locked doors), access controls (e.g., identification cards, visitor escorts and logs, facility/equipment repair records), environmental controls and protections (e.g., uninterruptible power supplies, generators, temperature and humidity systems, fire suppression units).

2. *IT resources*. *IT service providers* shall ensure that all *IT resources* under their responsibility have adequate physical security safeguards. While the value of these *IT resources* may not rise to that found in a data center, the physical protections normally afforded to *IT resources* within a data center should be employed where reasonable and appropriate.

F. **Incident Detection and Reporting**

IT service providers shall monitor for and report security breaches or other significant security events involving the *IT resources* under their control, following guidance from the campus *Information Security Officer*.

III. RELATED POLICIES, PROCEDURES, FORMS, GUIDELINES, AND OTHER RESOURCES

A. Administrative Policy Statements (APS) and Other Policies

The IT Security Program serves as the core for the Institute's *IT security* activities and provides general guidance to the computing community on ensuring the privacy of personal information and the availability of *Institution information* and *IT resources* and encompasses all related IT Security requirements, including the following policy sections:

IT Resource User Responsibilities
IT Security in Personnel Job Descriptions, Responsibilities and Training
IT Security in Institution Operations, Business Continuity Planning, and Contracting
IT Service Provider Security

The Laws of the Regents, section 14.A.4 states that employees shall be responsible for the safekeeping and proper maintenance of institution property in their charge.

B. Other Resources (i.e. training, secondary contact information)

Educational information and resources are available on the Office of Information Security website www.htim.edu.