PHYSICAL TECHNOLOGY ASSETS PROTECTION

Objective:

To protect University property, including maintaining proper use, maintenance, and safekeeping.

Important Information:

Physical access to non-public IT resource facilities are granted only to authorized personnel of UHD or other authorized contractors or vendors. All systems considered critical to UHD business operations are located within designated areas equipped with environmental and physical security access control mechanisms.

All departments are responsible for enforcement of property management and appropriate use of computing resources guidelines relating to technology assets. UHD software and hardware standards policy (UHD PS 08.A.02) requires departmental purchases be consistent with UHD's short and long term IT plans. Written justification and approval of the CIO and/or the Information Systems Steering Committee are required for technology implementations outside the scope of traditional IT supported systems.

Standards for centralized computing equipment are maintained by IT. Departments are expected to maintain physical security standards for computing equipment in the offices and facilities they manage. Electronic locking systems are in place for most classrooms, which contain technology equipment; however, some rely on traditional key-based access control.

Departments are encouraged to purchase locking mechanisms for portable devices and machines. All general use computers are equipped with surge protection. IT managed systems designated as critical are protected via UPS' and physically secured via electronic access systems. Department managed facilities, some facilities have electronic access systems.

IT personnel working in a secured or highly sensitive area are required to complete regular and ongoing training and wear appropriate identification.

As required by TAC 202, users are advised that suspected security violations are to be reported to the Division of Information Technology (and the UHD Police Department if criminal activity is suspected) for investigation. UHS Mandated Information Security Training, which is required of all users, addresses this requirement. Security incidents are included in a monthly security incident report submitted to the Department of Information Resources (DIR).

Ongoing training is required and maintained in the following areas:

- UHS Mandated Information Security Training (as required by TAC 202) addresses security incident reporting; protection of physical technology assets
- Computing access procedures training is conducted for every new employee as part of their departmental orientation on or near their first day of work
- Environmental hazards procedures are maintained within the Business Continuity and Disaster Recovery Guide. Testing and training is conducted once per year, is incorporated into the IT Training and User Development program and accessible in multiple formats (face to face or via portable media VHS delivery). The vendor responsible for environmental control systems at UHD is also required to complete system testing on a yearly basis
- Departmental training is conducted by the manager or supervisor

Potential Impact:

Potential impacts can include the loss of University property and/or loss of protected or institutional information if information security is breached. Additionally, may expose the institution to financial loss if equipment is misappropriated or is damaged because it is not physically secure and must be replaced.

Helpful Tools:

- UH System Administrative Memorandum:

  03.E.02 – Property Management

- UH – Downtown Policy Statement:

  Property Management – 07.A.01 – Property Management

  Information Systems – 07.A.03 - Annual Inventory of Capital Property

  Information Systems – 08.A.04 – Information Systems Security and Access Policy

  Information Systems – 08.A.02 – Information Systems Policies, Procedures, Standards, and Plans

- UHD Websites:

  IT User's Handbook

  IT: Help Desk

- Other:

  Texas Administrative Code – Chapter 202 – Subchapter C (TAC 202 C)

Contacts:

Jon Garza
garzaj@uhd.edu
713-221-8950
S701

Paul Tichenor
tichenorp@uhd.edu
713-221-8450
S970

Frequently Observed Weaknesses/Deficiencies:

- Equipment not properly secured.
- Required training not conducted by University/completed by employees.
- Annual inventory not properly conducted by property custodian.
- Inventory not properly conducted when property custodian changes.
- Classrooms containing technology equipment not properly secured.
- Departmental technology equipment not properly secured.

Best Business Practices:

1. Assign a person within your department to be the property custodian responsible for the proper management and control of University property.
2. Conduct an annual inventory for all technical property owned by the organization.
3. Monitor acquisition and disposal procedures and processes to see that University, state and or federal requirements are met.
4. Require the completion of a "Request to Remove Capital Property Form" and signature by the Property Manager prior to removal of property off-campus.
5. Obtain/renew approval when property located off-campus extends past the end of the fiscal year.
6. Take a departmental inventory whenever the property custodian changes, including a departing inventory when staff leave employment and assign an alternate property custodian, if even on a temporary basis.
7. Ensure assigned property custodians are properly trained to comply with all pertinent rules and regulations.

AREA

This questionnaire is designed so that "no" answers indicate that an internal control weakness may exist and the procedure/process may need to be examined in greater detail. **Comments should be provided for "No" answers.** When such weaknesses are identified, a change in the process may be necessary OR a control may need to be put into place to address the weakness. The appropriate UHD contact office (as outlined in the self-assessment text) may be contacted for assistance with identified weaknesses.

Self-Assessment of Internal Controls for Physical Technology Assets Protection	Yes	No	N/A	Comments
Have you assigned a person within your department(s) to be the property custodian that is responsible for the proper management and control of University property? *(SAM 03.E.02, § 2.10; UHD PS 07.A.01, § 2.2).*	☐	☐	☐	
Do you perform an annual inventory of your property? *(SAM 03.E.02, § 4.3.b, 4.4, and 7.1; UHD PS 07.A.03, § 2.3 and UHD PS 07.A.01, § 2.16)*	☐	☐	☐	
Do you monitor acquisition procedures for all technology purchases? *(UHD PS 07.A.01)*	☐	☐	☐	
Do you require a "Request to Remove Capital Property Form" be completed and signed by the Property Manager prior to removal of property off-campus? *(SAM 03.E.02, § 5.1; UHD PS 07.A.01, § 2.12)*	☐	☐	☐	
Is approval obtained/renewed when property located off-campus extends past the end of the fiscal year? *(SAM 03.E.02, § 5.2; UHD PS 07.A.01, § 2.12)*	☐	☐	☐	
Is departmental inventory taken whenever the property custodian *changes? (UHD PS 07.A.01, § 2.2.2)*	☐	☐	☐	

This is a living document and will be updated as revisions are necessary. Periodically, you may want to check for updates and revisions. We welcome any questions and feedback regarding the information contained in this tool including any comments regarding how this may be more useful and effective.