

# Departmental Computing Guidelines

## UHD / UHS

### Purpose:

These guidelines are provided to assist UHD departments and users in managing university computing assets and complying with relevant laws, regulations, policies and procedures. It also outlines key issues pertaining to computing that are commonly addressed by UHS auditors during IT and departmental audits.

### Information Security Areas Addressed:

The listed following information security areas are addressed by providing departmental self-assessments in the subsequent sections of these guidelines. These self-assessments are structured to assist UHD departments in taking a critical look at computing practices at the departmental level and determining where systems and information vulnerabilities may exist helping them to correct deficiencies and issues before they become problems. These self-assessments are living documents, and, as technology requirements change, are updated to reflect the most current information available to keep our systems and information secure. Self-assessments are included for:

- Annual Security Practices;
- Equipment Disposal;
- Physical Technology Assets Protection;
- Risk Management and Business Continuity Plans;
- Security and Backups for Applications and Systems;
- Software Licensing;
- Telephone Long Distance; and
- Virus Prevention.

### Relevant Policies and Procedures:

These following UH System Administrative Memorandum, UH – Downtown Policy Statements and procedures and guidelines documents, and Texas Administrative Code references are provided to assist departments in understanding the many areas in which information technology implementation university-wide must comply with standards, rules and laws. Questions regarding specific interpretation and implementation of any UH System or state or federal law should be addressed to the IT Compliance and Project Management Office within the IT Division.

- UH System Administrative Memoranda: SAM 07.A.02; SAM 07.G.01; SAM 03. A.19 and 02.A.25  
([www.uh.edu/policyservices/sam](http://www.uh.edu/policyservices/sam))
- Texas Department of Information Resources Information Security Standards: Texas Administrative Code Title 1, Part 10, Chapter 202, Subchapter C  
([http://texreg.sos.state.tx.us/public/readtac\\$ext.ViewTAC?](http://texreg.sos.state.tx.us/public/readtac$ext.ViewTAC?))

- UHD Network and Information System Password Procedures (<https://www.uhd.edu/computing/help/Documents/passwordprocedure.pdf>)
- UHD PS 07.A.01 - Property Management (<https://www.uhd.edu/administration/employment-services-operations/resources/Documents/PS07A01.pdf>)
- UHD PS 08.A.01 - Review of Information Technology Resources Requests (<https://www.uhd.edu/administration/employment-services-operations/resources/Documents/PS08A01.pdf>)
- UHD PS 08.A.02 - Information Technology Policies, Procedures, Standards, and Plans (<https://www.uhd.edu/administration/employment-services-operations/resources/Documents/PS08A02.pdf>)
- UHD PS 08.A.04 - Computer Access, Security, and Use Policy (<https://www.uhd.edu/administration/employment-services-operations/resources/Documents/PS08A04.pdf>)
- UHD PS 08.A.05 - Academic Computing Services (<https://www.uhd.edu/administration/employment-services-operations/resources/Documents/PS08A05.pdf>)
- UHD PS 02.A.19 - Access to and Maintenance of Staff Personnel Files (<https://www.uhd.edu/administration/employment-services-operations/resources/Documents/PS02A19.pdf>)
- UHD PS 01.A.11 - Ethical and Legal Use of University Property (<https://www.uhd.edu/administration/employment-services-operations/resources/Documents/PS01A11.pdf>)

## 1. ANNUAL SECURITY PRACTICES

### Objective:

To determine if all employees of the department or unit are completing the mandatory review of computing security policies and guidelines at least annually.

### Important Information:

Per TAC 202, computer users are required to review computing security policies and guidelines at least annually. Training required of all users, such as the UHS mandated information security training, addresses UHD employee responsibility to review security practices on an annual basis. In addition to the UHS training, users are provided with copies of the UHD IT policy statements as well as the *Network and Information System Password Procedures* as part of the university account request and renewal process.

### Potential Impact:

Failure to follow mandated annual security practices potentially exposes the university to allowing inappropriate access to protected information and loss or damage of equipment, and puts the university out of compliance with state regulations.

**Helpful Tools:**

- UH System Administrative Memorandum:  
[07. A.03 – Notification of Automated System Security Guidelines](#)
- UH – Downtown Policy Statement: None cited
- UH System Administrative Memorandum:  
[IT User’s Handbook](#)  
[Annual Review of Security Practices](#)  
[University Account Request](#)  
[Information Technology Forms](#)
- Other(s):  
[Texas Administrative Code – Chapter 202 – Subchapter C \(TAC 202 C\)](#)  
 The *Secure Our Systems* training course is available online via the UHS Online Training website at <http://www.uh.edu/onlinetraining/>. Staff is advised to use this login link; **do not log-in through PASS.**

**Contacts:**

Jon Garza  
[garzaj@uhd.edu](mailto:garzaj@uhd.edu)  
 (713) 221-8950  
 701 South

**Frequently Observed Weaknesses/Deficiencies:**

- Existing staff fail to take annual online training regarding computing security policies and guidelines or newly hired staff fails to take the required mandated training within 30 days of employment.

**Best Business Practices:**

1. Ensure easy and convenient access to required training.
2. Monitor staff completion of required training during specified window(s).

<b>AREA</b>
-------------

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. 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 UH contact office (as outlined in the self-assessment text) may be contacted for assistance with identified weaknesses.

Self-Assessment of Internal Controls for: Annual Security Practices	Yes	No	N/A	Comments
Did all staff review computing security policies and guidelines annually?				

Did all new users receive copies of the UHD IT Policy statements as well as the <i>Network and Information System Password Procedures</i> as part of the university account request process?				
--	--	--	--	--

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.

## 2. EQUIPMENT DISPOSAL

### Objective:

To determine if departments/units coordinate with IT when disposing of any computer equipment and are in compliance with applicable policies, procedures and regulations.

### Important Information:

Texas Administrative Code 202 specifies requirements for proper disposal of computers at state institutions. UHD's IT Division follows formal computer system reclaim and disposal procedures accordingly. Computer systems that are brought back in from the field as part of the Faculty and Staff Desktop Computing and Satellite Lab Refresh Programs or from other deployments are inventoried and inspected. A software application that purges the computers' hard disk to DoD 5220.22-M specifications is then used to prevent future recovery or access to data or applications previously stored on the system. Once this process is completed successfully, the systems are moved to a secured storage area and are ready for reuse or donation.

Although most university computers are maintained by the IT Division, a few departments have computers that are maintained locally. When redeploying or disposing of these systems, departments should coordinate with IT and conduct proper disposal procedures for these systems to ensure that DoD 5220.22-M specifications are met.

### Potential Impact:

Improper equipment disposal can result in unintentional and unauthorized access to protected information; potential legal consequences as well as negative public opinion could be the result if information obtained in this manner is used inappropriately.

### Helpful Tools:

- UH System Administrative Memorandum:  
None cited
- UH – Downtown Policy Statement:  
None cited
- UHD Website:  
[IT User's Handbook](#)  
[IT: Help Desk](#)

Other(s):

[DoD Issuances](#) (official site for access to Department of Defense publications) [US Department of Defense 5220.22-M Clearing and Sanitization Matrix](#)  
[Texas Administrative Code – Chapter 202 – Subchapter C \(TAC 202\\_C\)](#)

**Contacts:**

Jon Garza  
[garzaj@uhd.edu](mailto:garzaj@uhd.edu) (713) 221-8950

**Frequently Observed Weaknesses/Deficiencies:**

- Equipment is disposed of without consulting with IT or applying a checklist from DOD 5220.22-M to ensure all protected, confidential, or sensitive information is permanently removed from the equipment.

**Best Business Practices:**

1. Use of DoD 5220.22-M specifications to purge computer hard disk or other electronic equipment storage media.
2. All computer equipment to be disposed of should be identified and reported to the Office of Information Technology to ensure that the proper disposal of that equipment is done.

**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. 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.

<b>Self-Assessment of Internal Controls for Equipment Disposal</b>	<b>Yes</b>	<b>No</b>	<b>N/A</b>	<b>Comments</b>
Are all computers maintained by IT taken out of service by IT staff to allow hard disk purging via DoD 5220.22M specifications?				
Does department staff responsible for disposing of all technology equipment maintained by the department consult with IT prior to the equipment’s disposal?				
Does department staff responsible for disposing of all technology equipment maintained by the department use DoD 5220.22-M specifications to purge computer hard disk or other electronic equipment storage media?				

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.

### 3. PHYSICAL TECHNOLOGY ASSETS PROTECTION

#### **Objective:**

To protect university equipment by ensuring its proper use, maintaining the equipment as needed and securing it against misuse.

#### **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 the loss of critical, protected or institutional information if information security is breached. Additionally, it may expose the institution to financial loss or legal issues if equipment is lost, misappropriated, damaged or used for purposes other than University business 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](#)  
[Property Management – 07.A.03 - Annual Inventory of Capital Property](#)  
[Information Systems – 08.A.04 – Computer Access, Security, and Use Policy](#)  
[Information Systems – 08.A.02 – Information Technology Policies, Procedures, Standards, and Plans](#)
- UHD Website:  
[IT User's Handbook](#)  
[IT: Help Desk](#)
- Other(s):  
[Texas Administrative Code – Chapter 202 – Subchapter C \(TAC 202 C\)](#)

**Contacts:**

Jon Garza  
[garzaj@uhd.edu](mailto:garzaj@uhd.edu)  
(713) 221-8950  
701 South

Paul Tichenor  
[tichenorp@uhd.edu](mailto:tichenorp@uhd.edu)  
(713) 221-8450  
970 South

### **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 computing 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 an inventory of all equipment whenever the custodian of the property changes or leaves their position 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. 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.

<b>Self-Assessment of Internal Controls for Physical Technology Assets Protection</b>	<b>Yes</b>	<b>No</b>	<b>N/A</b>	<b>Comments</b>
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? ( <i>SAM 03.E.02, § 2.10; UHD PS 07.A.01, § 2.2</i> ).				
Do you perform an annual inventory of your property? ( <i>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</i> )				
Do you monitor acquisition procedures for all technology purchases? ( <i>UHD PS 07.A.01</i> )				
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? ( <i>SAM</i>				

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.

#### 4. RISK MANAGEMENT AND BUSINESS CONTINUITY

##### Objective:

To determine if the department/unit practices effective IT risk management and has developed and documented a comprehensive business continuity plan as it relates to its dependency on technology resources.

##### Important Information:

Risk management involves identifying, analyzing, and taking steps to reduce or eliminate the university's exposure to loss. Every universities encounter risks, some of which are predictable and controllable, and others which are unpredictable and uncontrollable. UHD IT updates its *Risk Assessment for Major IT Systems* as well as the resulting *Risk Management Plan* annually. The risk assessment process involves:

- the reassessment of risks for major IT systems,
- a critical system validation,
- a business impact analysis for major systems,
- a review of the documented formal data classification scheme for each system,
- the validation of application ownership and custody for each system,
- a current status analysis for the technical environment relevant to each system, and
- an update of the IT business continuity and disaster recovery procedures relevant to restoring each system in the event of disaster or major system failure.

Systems reviewed as part of the risk assessment process at UHD include both academic and administrative systems. The process is coordinated by UHD IT and also includes designated application owners for each of the critical systems. Every other year, key stakeholders and department representatives are also invited to participate in the risk assessment process in order to provide a sufficiently broad perspective on potential risks. These individuals are appointed by university Vice Presidents. Risk Assessment

and Risk Management Plan results are presented to university leadership, and the President signs off on the plan.

In addition to participating in the biennial risk assessment process, departments and units can practice effective risk management by being “risk aware” at all times, and report any potential risks associated with their owned applications and systems to the IT Department once identified or experienced, whichever comes first.

UHD also IT maintains the *UHD IT Business Continuity and Disaster Recovery Manual* (BCDR) for critical systems. This manual details critical IT systems recovery processes, as well as system ownership, and server center information. The procedures are updated regularly throughout the year as new systems are added and as environments and recovery procedures change. A comprehensive review and update of the procedures and manual is conducted annually as part of the update of university’s risk assessment and business impact analysis for critical systems. This process is coordinated by UHD IT. The manual is stored in electronic format, which is backed up nightly, and versions are maintained on and off site. A printed version of the manual is also produced annually and stored on and off site. University departments and units are also required to participate in the maintenance of the university-wide *UHD Business Continuity Plan* (BCP) that address the critical academic and business operations for the university. Departments and units should periodically assess both the BCDR and BCP to ensure that recovery and continuation processes for critical applications, systems, and business functions for which they are responsible are effectively documented and in place.

#### **Potential Impact:**

If departments and units do not plan effectively for business continuity risks, University operations impacting faculty/staff and students may be adversely affected by an interruption of those services due to unforeseen circumstances and poor to no planning. This may result in other negative consequences and/or financial losses for the university.

#### **Helpful Tools:**

- UH System Administrative Memorandum:  
None cited
- UH – Downtown Policy Statement: Information Technology  
[Information Systems – 08.A.02 - Information Technology Policies, Procedures, Standards and Plans](#)
- UHD Website:  
[UHD Website Main Page](#)  
[UHD Emergency Website](#)  
[IT User’s Handbook](#)
- Other(s):

[Texas Administrative Code – Chapter 202 – Subchapter C \(TAC 202 C\)](#)

#### **Contacts:**

Jon Garza  
[garzaj@uhd.edu](mailto:garzaj@uhd.edu)  
(713) 221-8950  
701 South

**Frequently Observed Weaknesses/Deficiencies:**

- Failure to have documented business continuity plans.
- Inadequate or nonfunctional business continuity plans.
- Failure to periodically review and update plans.
- Failure to communicate plans to responsible individuals, as well as to other employees of the unit.
- Only one employee knowledgeable of and/or in possession of business continuity plans and execution of them.
- Failure to appoint a backup person for execution of plans.
- Inappropriate storage location/site for plan (maintaining plans in same area and/or building that may be affected).
- Lack of alternative work space arrangements established in the event current space is unusable.
- Data are stored locally and if the current space is inaccessible, data are unavailable.

**Best Business Practices:**

1. Develop and document comprehensive business continuity plans and review these plans on an ongoing basis.
2. Report, manage and address infrastructure risks on a continuing basis.
3. Identify maximum acceptable outage times for critical business processes and operations.
4. Identify the process for converting operations from your current facility to alternate processing facilities if necessary.
5. Make certain plans incorporate building plans, network/communication diagrams and other documents warranted by the unique function(s) of the department/unit.
6. Make certain plans include any special software that the department/unit may utilize and how that software would be acquired during an emergency.
7. Ensure employees of the department/unit are familiar with business continuity plans and acceptable outage/down times.
8. Relay business continuity plans to staff on a consistent basis dependent on the business need.
9. Ensure a copy of the business continuity plans is stored off-site and/or in an appropriate second location outside of the area/building that may be affected.
10. Encourage employees to promptly report business risks that they may discover.

**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. 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.

<b>Self-Assessment of Internal Controls for Risk Management and Business Continuity</b>	<b>Yes</b>	<b>No</b>	<b>N/A</b>	<b>Comments</b>
Do employees know what to do if they become aware of a potential or realized risk to departmentally-owned applications or systems?				
Do employees know what to do if their computers are not available to use?				
Are sources or primary data stored on a network drive?				
Does the department have plans for the following scenarios? <ul style="list-style-type: none"> <li>- IT resources are down. The department is still functioning.</li> <li>- Building or department is down, but IT resources are available at other locations.</li> <li>- Both are down.</li> <li>- Neither are down, but staffing is unavailable (i.e., influenza epidemic).</li> </ul>				
Has the department identified down time tolerance levels for above scenarios? 0-72 hours, 72-120 hours, and 120 hours or more?				
Has the department identified critical times where IT resources are required (i.e., grades are due for posting, resident match week, payroll, student registration, grant submissions, etc.)?				
Do all department or unit employees know where to locate the UHD BCP and emergency management information on the UHD website?				

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.

## 5. SECURITY AND BACK-UPS FOR APPLICATIONS AND SYSTEMS

### Objective:

Determine if IT Security measures exist in the department/unit to safeguard electronic data and information systems. These measures should include procedures the department/unit has in place for backing up institutional information periodically. Additionally, to determine if employees are performing the backups and adequate protection/storage exists for backups.

### Important Information:

All university-wide Enterprise Systems applications, like the Banner Student Information System or Blackboard, are managed and secured centrally, with UHD IT or UHS IT as custodian. Application/Data owners are verified annually or biennially as part of the university's TAC 202 *Compliance and Risk Assessment Plan* which is coordinated by UHD IT. Individual departments, however, take on management and security responsibilities for department-specific applications and systems.

The roles and responsibilities for department-specific systems vary to some degree by department and application. Most department-specific applications are housed on servers that are centrally managed and secured by UHD IT. However, ownership and accountability for the data and use of these systems is the responsibility of the individual departments and designated application owners.

The university maintains standards for supported software and hardware through the UHD Information Technology Division. Departments are expected to work with the IT Division and through the university planning process to define options to address software needs that cannot be addressed effectively with existing software. Additionally, security and maintenance issues, such as application integration standards, network location and system access best practices, user security awareness, early detection and mitigation of security incidents, must be considered in the development or purchase of new enterprise computer applications. Additional reference regarding applicable procedures can be obtained by referring to (SAM 07.G.01) – *System Development Life Cycle* and UHD PS 08.A.02 – *Information Systems Policies, Procedures, Standards, and Plans*.

Backups for the centrally managed systems occur nightly. In situations where software systems are acquired by or for departments and are set up as department-specific and department-managed applications, the department is expected to work with the IT Division to define roles and responsibilities, as well as security and backup procedures. Automatic backup of users' data (including critical files) are performed on their computers across campus (desktops & laptops) in real-time.

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.



**Potential Impact:**

Potential for protected or institutional information to be inadvertently released if information security is breached. Additionally, the institution may be exposed to cyber threats or financial loss from damaged equipment if equipment is not physically secure. Possible loss of data could greatly reduce the ability of the department/unit to maintain daily operations if information system back-ups are not performed on a regular basis and stored in a secure, off-site location.

**Helpful Tools:**

- UH System Administrative Memorandum:
  - [UH System Records Retention Schedule](#)
  - [7.A.2 – The Ethical and Legal Use of Micro/Personal Use of Computer Software](#)
  - [7.A.3 – Notification of Automated System Security Guidelines](#)
- UH – Downtown Policy Statement: Information Technology
  - [Information Systems – 08.A.02 - Information Technology Policies, Procedures, Standards and Plans](#)
  - [Information Systems – 08.A.04 – Computer Access, Security, and Use](#)
  - [Policy Information Systems – 08.A.05 - Academic Computing Services](#)
- UHD Website:
  - [IT User's Handbook](#)
  - [IT: Help Desk](#)
  - [Computer Account Password](#)
- Other(s):
  - [Texas Administrative Code – Chapter 202 – Subchapter C \(TAC 202 C\)](#)

**Contacts:**

Jon Garza  
[garzaj@uhd.edu](mailto:garzaj@uhd.edu)

(713) 221-8950

701 South

**Frequently Observed Weaknesses/Deficiencies: Security**

- Sharing of passwords.
- Failure to lock desktop computers when stepping away from their use.
- Failures to ensure critical updates are performed.
- Failure to store institutional data on network storage.

- Failure to limit access to sensitive or confidential data to those that “need to know.”
- Lack of adequate training and/or knowledge of IT security.

## **Frequently Observed Weaknesses/Deficiencies: Data Back-Up**

- Lack of back up procedures/policies.
- Failure to back up information on a regular basis.
- Lack of understanding of shared drives.
- Failure to use shared drives to store data.
- Storing back-ups in the same office and/or building as the computer housing the information.

## **Best Business Practices – Workstation Security:**

1. Use only authorized and licensed software.
2. Take measures to secure sensitive areas, computer labs, and the like, and to provide adequate protection against the loss or theft of institution equipment and other assets.
3. Ensure all workstations have active, up-to-date antivirus and antispymware software, service packs and security patches.
4. Ensure externally connected devices such as USB thumb drives, hard drives and the like are secured and stored properly.
5. Do not open e-mails from unknown sources.
6. Ensure all computers are protected with a password log-in.
7. Construct strong, hard to guess passwords.
8. Ensure passwords are changed every 90 days.
9. Protect passwords and computers. Do not share access or passwords to your computer and do not write down or e-mail passwords.

**Best Business Practices – Server Security:**

1. Ensure that the server is following the Server Security Policy.
2. Ensure a *Departmental Server Agreement Form* is completed and submitted to IT if the department/unit maintains a pre-existing server.
3. Ensure all internal servers are physically protected, and in an environmentally controlled area (air conditioning, fire protection, etc.).
4. Review access to servers periodically and ensure only employees with a direct need have access. Make access changes as needed.

**Best Business Practices – Data Back-Ups:**

1. Management should appoint a data administrator or coordinator for overseeing information systems processes to include back up procedures.
2. Strongly recommend/encourage employees to store institutional data on an ITSS managed server.
3. Lock up removable and/or mobile storage media containing sensitive and/or confidential data.
4. Ensure procedures exist for the back-up of information on mobile assets such as laptops, USB and flash drives.
5. Back-ups should be stored in a secure location and should not be stored in the same office and/or building as the computer housing the information.

**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. 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.

<b>Self-Assessment of Internal Controls for Security and Back-Ups for Applications and Systems</b>	<b>Yes</b>	<b>No</b>	<b>N/A</b>	<b>Comments</b>
Are all critical data files backed up and stored in a safe, separate area to help ensure a full recovery of the data, if necessary? ( <i>SAM 07.A.02; UHD PS 08.A.04; UHD PS 08.A.05</i> )				
Are suspected security violations reported to the Information Technology Department to investigate? ( <i>UHD PS 08.A.04, § 2.1; UHD PS 08.A.05</i> )				
Are employees encouraged to use the university’s Desktop Backup System to back-up information?				
With respect to confidential and sensitive data, does your department restrict access based on a “need to know” practice?				
Are all employees encouraged to use the remote desktop option to access university files from off campus rather than transporting university data on portable storage devices?				
If data must be backed up to mobile media (i.e., USB, flash, CD-ROM, DVD, etc.), are confidential data encrypted and secured?				
Are institutional data stored on a network server?				
Are back-up media stored in a different location than source data?				

Do employees have adequate training for and know-ledge of departmental standards for data back-up?				
Are suspected security violations reported to the Division of Information Technology (and the UHD Police Department if criminal activity is suspected) for investigation?				

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.

## 6. SOFTWARE LICENSING

### Objective:

To determine if applications installed on university computers have a valid license and are installed by UHD IT staff or designated departmental technology staff.

### Important Information:

Training required of all users, such as the UHS mandated information security awareness training (as required by TAC 202), address software licensing and the employee's responsibility on the use of licensed software.

Any application installed on university computers must have a valid license. In most cases, UHD IT staff installs the licensed software on university computers; and some cases, designated departmental technology staff installs the licensed software on departmental computers. UHD IT is responsible for verifying licenses it installs on departmental computers. Verification of licensing for any other software installed on departmental computers is the responsibility of the department or unit. Departments are expected to coordinate with UHD IT on any software installation conducted by the department.

UHD PS 08.A.04 informs users that 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 compliance with institutional security policies, procedures, and standards. UHD PS 08.A.04 also highlights the copyright laws concerning computer software and the unauthorized use or duplication of software. UHD PS 01.A.11 also alerts users to the U.S. Copyright laws which prohibit duplication and distribution of software without previous authorization. UHD PS 08.A.05 clearly states that "Copying of copyrighted software is illegal and is prohibited in the Academic Computing facilities or elsewhere on campus." The same PS also states that UHD forbids, under any circumstances, the unauthorized reproduction of software or use of

Illegally obtained software, and that using university equipment to make illegal copies of software is prohibited.

In addition, UHS Administrative Memorandum 07.A.02 informs users that a software license must be purchased for each computer it will be used on, and that university employees shall only use the software in accordance with the license agreement purchased with that software. It also informs staff of the U.S. Copyright Law, and informs readers that the reproduction of software can be subject to civil damages of up to \$100,000 and criminal penalties which include fines and imprisonment.

### **Potential Impact:**

Violation of software licensing and/or copyright laws exposes the university and/or its officers and staff to civil litigation and possible financial losses. Employees who violate copyright laws are personally subject to civil damages up to \$100,000 and criminal penalties, including fines and possible imprisonment.

### **Helpful Tools:**

- UH – Downtown Policy Statement:
  - [Administration – 01.A.11 -Ethical and Legal Use of University Property](#)
  - [Information Systems - 08.A.04 – Computer Access, Security, and Use](#)
  - [Policy Information Systems – 08.A.05 - Academic Computing Services](#)
  - [7.A.2 – The Ethical and Legal Use of Micro/Personal Use of Computer Software](#)
- UHD Website:
  - [Desktop Computing Project Reference “Standard Software Applications”](#)
  - [Software Installation Request](#)
- Other(s):
  - [Texas Administrative Code – Chapter 202 – Subchapter C \(TAC 202 C\)](#)

### **Contacts:**

Jon Garza  
[garzaj@uhd.edu](mailto:garzaj@uhd.edu)  
(713) 221-8950  
701 South

Help Desk  
[help@uhd.edu](mailto:help@uhd.edu)  
(713) 221-8031 or x3000  
700 South

### **Frequently Observed Weaknesses/Deficiencies:**

- Applications installed on university owned computers by employees as opposed to UHD IT staff or designated departmental technology staff install those applications without a valid license.
- Unauthorized reproduction of software or use of illegally obtained software, including use of university equipment to make illegal copies of software.

**Best Business Practices:**

1. Only authorized university personnel verify and install licensed software on university computers.
2. The addition or removal of all software, programs or information to/from any operating system, database or university file as authorized by appropriate management and in compliance with institutional policies, procedures and standards.

<b>AREA</b>
-------------

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. 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.

<b>Self-Assessment of Internal Controls for Software Licensing</b>	<b>Yes</b>	<b>No</b>	<b>N/A</b>	<b>Comments</b>
Are employees using software in accordance with the license agreement? <i>(SAM 07.A.02, § 3.2; UHD PS 08.A.04, § 2.2)</i>				
Has IT staff verified and installed all software on the employee’s university computer(s)?				
Has the department coordinated with IT on any software purchase and installation to verify compatibility with university systems and proper licensing/installation?				

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.

## **7. TELEPHONE LONG DISTANCE**

**Objective:**

To determine if the department/unit has appropriately authorized all users of long distance telecommunications and reviews monthly telephone charge reports to insure charges are accurate and appropriate.



## Important Information:

In order to have access to make long distance calls through the university's telephone system, employees are required to have departmental approval for the issuance of long distance codes. Departmental cost center information (for applying long distance charges) must be identified through the *Telecommunications Authorization Form* and authorized by the employee's departmental leadership.

Per PS 01.A.11, section 2.2.4, employees are required to review monthly telephone charge reports and certify that all long distance charges are accurate and made for official university business. Each department is responsible for implementing this policy within their unit and maintaining records accordingly.

## Potential Impact:

Failure to appropriately manage the issuance of long distance codes and review monthly charges could result in a financial loss for the institution and cause a violation of institutional business procedures.

## Helpful Tools:

- UH System Administrative Memorandum:
  - [03. A.19 – Personal Use of UHS Telecommunications Equipment](#)
  - [Services 02.A.25 – Termination Clearance Guidelines](#)
- UH – Downtown Policy Statement:
  - [Administration – 01.A.11 - Ethical and Legal Use of University Property](#)
  - [Financial Affairs – 05.A.21 - Wireless Communications Equipment and Communications Policy](#)
- UHD Website:
  - [Telecommunications Service Authorization Form](#)
- Other(s):
  - [Texas Administrative Code – Chapter 202 – Subchapter C \(TAC 202 C\)](#)

## Contacts:

Jon Garza  
[garzaj@uhd.edu](mailto:garzaj@uhd.edu)  
(713) 221-8950  
701 South

## Frequently Observed Weaknesses/Deficiencies:

- Failure to monitor telecommunication costs for unusual activity/errors, and to preclude personal telephone expenses.
- Failure to periodically communicate to employees that personal telecommunication expenses are unallowable.
- Failure to review monthly long distance telephone usage by staff.
- Failure to perform periodic telecommunications audits of phone lines and equipment.

**Best Business Practices:**

1. Designate an individual(s) with the responsibility and authority to administer the unit’s telecommunication activities/processes. This individual should understand telecommunication procedures and handle and/or be apprised of all telecommunication activities.
2. Review telecommunication costs monthly, ensuring the review is documented and long distance calls are monitored.
3. Research unusual trends in telecommunication activity.
4. Periodically communicate/inform employees that non-business long distance calls are prohibited and that directory assistance is to be avoided.
5. Eliminate unnecessary telecommunication expenses such as lines, equipment, and other telecommunication features.
6. Protect telephones that are accessible to the public from unauthorized long distance calls (including incoming toll-free calls, if applicable).
7. Implement password/code protection on telephones where necessary.
8. Ensure an appropriate approval process exists for cellular phones, pagers, and other telecommunication devices and establish guidelines for determining who may have such items in the unit.

<b>AREA</b>
-------------

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. 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 Telephone Long Distance	Yes	No	N/A	Comments
Are all university employees authorized to make long distance calls from university telephones and issued long distance authorization codes? ( <i>SAM 03.A.19 and 02.A.25; UHD PS 01.A.11</i> )				
Is a Telecommunications Authorization Form authorized by a new employee’s manager or departmental leadership before a long distance code is assigned?				
Do you have a process in place to require all authorized long distance users to review their long distance telephone records to help ensure their authorization codes are not being compromised?				

Are telecommunication costs reviewed monthly for accuracy and appropriateness and certified by the employee?				
Are unusual trends in telecommunication activity researched?				
Does the unit document the review of telecommunication costs?				
Does the unit protect telephones that are accessible to the public from improper long distance calls?				
Does the unit perform a periodic audit of telecommunication lines and equipment?				

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.

## 8. VIRUS PREVENTION

### Objective:

To determine if the appropriate actions are taking place and the proper policies and procedures are being followed to allow virus prevention safeguards to be installed and/or updated on a regular basis, ensuring the continuing integrity of and access to information on all UHD computer equipment.

### Important Information:

All computers at UHD have anti-virus software installed on them (campus wide site license). UHD IT manages the anti-virus software updates remotely with an automated system that updates all PCs on daily basis with the latest definition files. Furthermore, all faculty and staff PCs on campus are set to automatically check for and install new operating system (OS) security/patch updates, which is important for preventing viruses, on a daily basis between 12 midnight and 5 a.m. Lab PCs are also scheduled for anti-virus and OS security/patch updates once a week (between 12 midnight and 4 a.m. every Friday). Users are instructed to log off but keep their computer on at night so the automatic updates can process regularly. Any applications left open will automatically close.

Training required of all users, such as the UHS mandated information security awareness training (as required by TAC 202), addresses applying computer security best practices by having anti-virus software installed on their computers.

UHS Administrative Memorandum 07.A.03 (*Notification of Automated System Security Guidelines*) informs employees that any person violating component university automated system security policies, such as inserting a virus, is subject to immediate disciplinary action that may include termination of employment, expulsion, or termination of a contract.

**Potential Impact:**

Computer viruses have the potential to cause great harm to the university, including, but not necessarily limited to, loss of data or compromising of data integrity. Any potential breach of security that allows unauthorized access to protected or institutional information can be harmful and could cause the loss and/or destruction of data which could greatly impact the ability of the department/unit to maintain daily operations.

**Helpful Tools:**

- UH System Administrative Memorandum:  
[7.A.3 – Notification of Automated System Security Guidelines](#)
- UH – Downtown Policy Statement: Information Technology  
[Information Systems - 08.A.04 – Computer Access, Security, and Use Policy](#)  
[Information Systems – 08.A.05 – Academic Computing Services](#)
- UHD Website:  
[IT User's Handbook](#)  
[IT: Help Desk](#)

Other(s):

[Texas Administrative Code – Chapter 202 – Subchapter C \(TAC 202 C\)](#)

**Contacts:**

Jon Garza  
[garzaj@uhd.edu](mailto:garzaj@uhd.edu)  
(713) 221-8950  
701 South

Help Desk  
[help@uhd.edu](mailto:help@uhd.edu)  
(713) 221-8031 or  
x3000 700 South

**Frequently Observed Weaknesses/Deficiencies:**

- Employees turn off their computers when they leave the office at night, thus preventing remote automated anti-virus software updates not installation.
- Employees visit website, open e-mails or use software/memory devices that introduce viruses to university computers.

**Best Business Practices:**

1. Ensure anti-virus software is installed and kept current on all computers.
2. IT management of daily anti-virus updates on all computers.

**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. 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.

<b>Self-Assessment of Internal Controls for Virus Prevention</b>	<b>Yes</b>	<b>No</b>	<b>N/A</b>	<b>Comments</b>
Do all employees in the department log off but keep their computers on at night so the automated updates can process regularly?				
Have all employees completed the mandatory UHS Information Security Awareness Training?				
Is the latest version of an anti-virus software installed and in use on user’s primary computers in the department?				
Is the latest version of an anti-virus software installed and in use on laptop computers in the department?				

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.