

# 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 departmental audits.

**Issues Addressed:**

1. **Computer Account Best Practices**
2. **Protection of physical technology assets**
3. **Annual Review of Security Practices**
4. **Security and Backups for University-Wide and Department Specific Applications and Systems**
5. **Risk Assessment**
6. **Business Continuity Plans**
7. **Software Licensing**
8. **Virus prevention**
9. **Equipment Disposal Procedures**
10. **Telephone Long Distance**

**Relevant Policies and Procedures:**

SAM 07.A.02; SAM 07.G.01; SAM 03.A.19 and 02.A.25

Texas Department of Information Resources Information Security Standards: Texas Administrative Code Title 1, Part 10, Chapter 202, Subchapter C

([http://info.sos.state.tx.us/pls/pub/readtac\\$ext.ViewTAC?tac\\_view=5&ti=1&pt=10&ch=202&sch=C&rl=Y](http://info.sos.state.tx.us/pls/pub/readtac$ext.ViewTAC?tac_view=5&ti=1&pt=10&ch=202&sch=C&rl=Y))

UHD Network and Information System Password Procedures

([http://www.uhd.edu/computing/services/infosec/password\\_procedure.htm](http://www.uhd.edu/computing/services/infosec/password_procedure.htm))

UHD PS 07.A.01 - Property Management (<http://www.uhd.edu/about/hr/PS07A01.pdf>)

UHD PS 08.A.01 - Review of Information Systems Resources Requests

(<http://www.uhd.edu/about/hr/PS08A01.pdf>)

UHD PS 08.A.02 - Information Systems Policies, Procedures, Standards, and Plans

(<http://www.uhd.edu/about/hr/PS08A02.pdf>)

UHD PS 08.A.04 - Information Systems Security and Access Policy

(<http://www.uhd.edu/about/hr/PS08A04.pdf>)

UHD PS 08.A.05 - Academic Computing Services (<http://www.uhd.edu/about/hr/PS08A05.pdf>)

UHD PS 08.A.07 - Computer Use Policy

(<http://www.uhd.edu/about/hr/PS08A07.pdf>)

UHD 02.A.19 Access to and Maintenance of Staff Personnel Files (<http://www.uhd.edu/about/hr/PS02A19.pdf>)

UHD PS 01.A.11 Ethical and Legal Use of University Property (<http://www.uhd.edu/about/hr/PS01A11.pdf>)

## 1. Computer Account Best Practices

Training that addresses employee responsibility to use *computer best practices* for passwords, accounts, and the safeguarding confidential data is required of all users (e.g. UHS Mandated Information Security Training (as required by TAC 202)).

The Network and Information System Password Procedure addresses password standards and user responsibilities ([http://www.uhd.edu/computing/services/infosec/password\\_procedure.htm](http://www.uhd.edu/computing/services/infosec/password_procedure.htm)) and is provided as part of the UHD computer account authorization process.

UHD PS 08.A.04, Section 2.3 specifies user accountability requirements pertaining to system access, protection of passwords, and accountability for unauthorized or negligent disclosure or use of access means including sharing of passwords. It is also included as part of the university's account request and renewal process.

As part of the UHD account request and renewal process, all users are required to agree to abide by and acknowledge receipt of the UHD Information Technology Policy Statements, which include the Regulations for Using Computing Facilities and Resources as well as the UHD Network and Information System Password Procedure.

Faculty and staff account access is terminated when the person's employment with UHD ends based on the university's exit interview and property/access removal process. Subsequent access to data in a user's computer, voice mail, or application system is provided only by formal request from the leadership of Employment Services and Operations.

Vendor/contractor access to systems requires authorization by the application owner as well as IT management. Prior to access, the vendor/contractor must complete the UHD Account Request Form and agree to its provisions. Vendors and contractors who need access to UHD computer resources must be formally assigned a UHD sponsor, and that person assumes responsibility for directly monitoring the vendor/contractor's activities.

### Relevant UHS Departmental Audit Questions:

**Termination Clearance:** Do you have a process in place to help ensure all university access keys, codes, and cards are recovered and canceled? (SAM 02.A.25, § 3.3; UHD ESO Termination Checklist; Information System Security Access Policy UHD PS 08.A.04)

#### UHD Procedures for IT Related Issues in this context:

Employment Services and Operation's termination checklist must be completed by full time employees when they end their employment with UHD. It includes an IT section, which is used for suspension of account access.

IT disables access for all systems centrally managed by UHD IT (e.g. Banner, e-mail, network and desktop computer accounts, long distance security code, Linux, BB Vista, Web Curator access, Fortis, etc.).

- Disabling of UHS managed accounts (e.g. PeopleSoft HR and Finance) is coordinated by ESO and Business Affairs.
- Several departments have applications managed locally which are accessible to employees in that department only, such as Financial Aid (Powerfaids) and the Library (ERS). In these cases, the department may be responsible for disabling access to the systems for their employees.
- Electronic access cards and/or codes used by departments for access to secure areas are managed by UHD Police (for departmental offices) and by Student Services and Enrollment Management (for access to some classrooms). In some cases, such as in the IT department, there is a local departmental coordinator for these cards and codes.

**Maintenance of Personnel Files:** Do you have controls in place to help ensure that personnel files are safeguarded and to help ensure integrity of the files, preserve the confidentiality of the records, and limit access only to authorized personnel? (SAM 02.A.31, §§ 1.1 and 3.6; UHS Mandated Information Security Training (as required by TAC 202);

**UHD Procedures for IT Related Issues in this context:**

Electronic personnel data is maintained in PeopleSoft, Fortis/ESO, and Banner. Some departments may also maintain some local copies of personnel data.

Password based access is required for Enterprise systems such as PeopleSoft, Banner and Fortis/ESO access (including form level security in many cases). Approval for access requires authorization by an employee's unit leadership as well as the application owner.

**Departmental Computing** (SAM 07.A.02; UHD PS 08.A.04; UHD PS 08.A.05) Are computer accounts (e.g. email accounts) assigned to a single individual? (UHD PS 08.A.04, § 2.1; UHD PS 08.A.05, Regulations for Using Academic Computing Facilities and Resources); Are passwords a minimum length of five to eight characters, changed on a regular basis, not obvious/easily guessed (nicknames, date of birth, etc.), not shared with other users, and not written down and easily accessible/visible to other persons? (Good Business Practice) Are computer accounts (e.g. email accounts) assigned to a single individual?

**UHD Procedures for IT Related Issues in this context:**

See UHD's The Network and Information System Password Procedure ([http://www.uhd.edu/computing/services/infosec/password\\_procedure.htm](http://www.uhd.edu/computing/services/infosec/password_procedure.htm)), which is provided to all users as part of the university account request form and is sent to all users periodically via e-mail addresses password standards and user responsibilities. Users are provided copies of these procedures when user accounts are requested.

**2. Protection of physical technology assets**

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.

#### **Relevant UHS Departmental Audit Questions:**

**Property Management:** Have you assigned a person within your department(s) to be the property custodian? (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 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)

#### **UHD Procedures for IT Related Issues in this context:**

Per P.S 07.A.01, all employees and departments are expected to protect university property, including maintaining proper use, maintenance, and safe keeping. Departments are also expected to designate a property custodian, responsible for the proper management and control of university property, including conducting an annual inventory and monitoring acquisition and disposal procedures. <http://www.uhd.edu/about/hr/PS07A01.pdf>

#### **Other Relevant Policies and Procedures:**

- Information System Security Access Policy UHD PS 08.A.04
- Information Systems Policies, Procedures, Standards, and Plans UHD PS 08.A.02

### **3. Annual Review of Security Practices**

Texas Administrative Code Title 1, Part 10, Chapter 202, Subchapter C

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 (as required by TAC 202), address UHD employee responsibility to review security practices on an annual basis. In addition to the UHS mandated training, users are provided with copies of the UHD IT Policy statements as well as the Network and Information System Password Procedure as part of the university account request and renewal process.

### **4. Security and Backups for University-Wide and Department Specific Applications and Systems**

PS 08.A.04 addresses protection of confidential information

PS 08.A.02 addresses policies, procedures, standards, and plans for UHD IT systems.

## **University-Wide Applications and Systems:**

All university-wide Enterprise Systems applications 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.

## **Department Specific Applications and Systems:**

Departmental 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".

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.

Backups for the centrally managed systems occur nightly. Backups are not currently performed for users' desktop PCs. Departments are expected to conduct local back-ups of critical data that is stored on computers that are not in the central server pool and therefore not backed up on an automated basis. UHD is implementing a selective desktop backup system in FY 2008 which will allow departments and end users to define certain desktop data for scheduled, centralized, automated backups.

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.

## **Relevant UHS Departmental Audit Questions:**

**Departmental Computing** (SAM 07.A.02; UHD PS 08.A.04; UHD PS 08.A.05) 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? (Good Business Practice). (UHD PS 08.A.04, § 2.1; UHD PS 08.A.05, Regulations for Using Academic Computing Facilities and Resources). Are suspected security violations reported to the Information Technology Department to investigate? **(Good Business Practice)**

### **UHD Procedures for IT Related Issues:**

Backups for the centrally managed systems occur nightly. Back-ups are not currently performed for users' desktop PCs. Departments are expected to conduct local back-ups of critical data that is stored on computers that are not in the central server pool and therefore not backed up on an automated basis. UHD is implementing a selective desktop backup system in FY 2008 which will allow departments and end users to define certain desktop data for scheduled, centralized, automated backups.

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.

## 5. Risk Assessment

PS 08.A.02:Information Systems Policies, Procedures, Standards, and Plans UHD; Texas Administrative Code Title 1, Part 10, Chapter 202, Subchapter C

UHD reviews and updates its Risk Assessment for Major IT Systems as well as the resulting Risk Management Plan annually. The risk assessment process involves 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, 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 its business continuity and disaster recovery procedures relevant to restoring each system in the event of disaster or major system failure. These activities have also laid the foundation for UHD to begin a formal update of its overall university-wide Business Continuity Plan, with major activities taking place between October, 2007 and May, 2008.

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 the Vice Presidents.

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

## 6. Business Continuity Plans

Texas Administrative Code Title 1, Part 10, Chapter 202, Subchapter C; PS 08.A.02 addresses policies, procedures, standards, and plans for UHD IT systems.

UHD IT maintains the UHD Business Continuity and Disaster Recovery Manual 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.

UHD is currently gearing up to conduct a university wide Business Continuity Planning exercise to update university and departmental plans and procedures for conducting business in the event of a disaster and/or if its major systems become unavailable for a significant period of time. This project is expected to be active from November 2007 – April 2008. Representatives from key academic and service units, as well as university leadership will be directly involved in the project. The plan that is produced will define responsibilities and activities for university departments to follow in the event of disaster or serious system outages. Subsequent to this project, the UHD policy PS 08.A.02, which specifically addresses Business Continuity Planning, will undergo a formal review and update.

## 7. Software Licensing

SAM 07.A.02; UHD PS 08.A.04; UHD PS 01.A.11

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 verify and install the licensed software on university computers; and in few cases, designated departmental technology staff may verify and install the licensed software on departmental computers.

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 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 (The Ethical and Legal Use of Micro/Personal Computer Software) 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 them of the US Copyright Law, and that the reproduction of software can be subject to civil damages of up to \$100,000 and criminal penalties which include fines and imprisonment.

### Relevant UHS Departmental Audit Questions:

**Departmental Computing** (SAM 07.A.02; UHD PS 08.A.04; UHD PS 08.A.05). Are users using software in accordance with the license agreement? (SAM 07.A.02, § 3.2; UHD PS 08.A.04, § 2.2)

#### UHD Procedures for IT Related Issues:

UHD IT requires that any application installed on university computers must have a valid license. In most cases, UHD IT staff verify and install the licensed software on university computers; and in few cases, designated departmental technology staff may verify and install 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. Departments are expected to coordinate with UHD IT on any software installation conducted by the department.

## 8. Virus prevention

### SAM 07.A.03

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 OS security/patch updates (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.

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.

## Relevant UHS Departmental Audit Questions:

**Departmental Computing** (SAM 07.A.02; UHD PS 08.A.04; UHD PS 08.A.05). Is the latest version of an anti-virus software installed and in use on the computers in the department? (Good Business Practice)

### UHD Procedures for IT Related Issues:

All computers at UHD have anti-virus software installed on them (based on a 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 OS security/patch updates (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.

## 9. Equipment Disposal Procedures

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.

## 10. Telephone Long Distance

### Relevant UHS Departmental Audit Questions:

**Long Distance/Cell Phone Charges** (SAM 03.A.19 and 02.A.25; UHD PS 01.A.11): Are all university employees authorized to make long distance calls from university telephones and issued long distance authorization codes? (Good Business Practice); Do you have a process in place to require all authorized long distance users to review the long distance telephone records to help ensure their authorization codes are not being compromised? (Good Business Practice)

### UHD Procedures for IT Related Issues:

In order to have access to make long distance calls through the university's telephone system, employees are required to have departmental approval. Departmental cost center information (for applying long distance charges) must also 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.