2015

University of Houston Downtown

Department of Information Technology

[UHD IT SECURITY HANDBOOK]

This document addresses the policies of the Texas Department of Information Resources Texas Administrative Code 202, Subchapter C 'Security Standards for Institutions of Higher Education' as they pertain to the computing environments at the University of Houston-Downtown.

Table of Contents

I. General Introduction and Overview of the UHD Information Security Handbook

The University of Houston Downtown Information Security Handbook contains computing guidelines and policies for University faculty, staff and students. The primary designee of the University for all IT security related issues is Jon Garza, Information Security and Compliance Officer. Departments that work with faculty, staff and student information whether financial, medical, academic, or any other sensitive information read the security handbook to become familiar with the policies and guidelines listed within. This handbook also addresses Texas State and Federal policies such as FERPA, HIPAA, GLBA, DMCA, and copyright law infringement policies as well as UH System and UHD Policies. This document is available for review and print and is recommended reading for anyone using the University's computing resources.

II. Addressing Security within the University Community

The University of Houston Downtown (UHD) supports the responsible use of its information resources. The information contained in the security handbook is aligned with the requirements outlined in the TAC 202 documentation, Subchapter C, entitled 'Security Standards for Institutions of Higher Education' and UHD's *'Information Technology Policies, Procedures, Standards, and Plans'*.

Information resources include, but are not limited to:

- Computers
- Servers
- Wired and wireless networks
- Computer-attached devices
- Network-attached devices
- Voice systems
- Cable systems
- Computer applications
- Digital signage

General User Access

This section defines the security standards and responsibilities of all users at the University. All individuals using UHD information resources are prohibited from using a computer account for which they are not authorized, or obtaining a password for a computer account not assigned to them. It is the responsibility of all individuals (faculty, staff, students, vendors) using UHD's information resources to protect the privacy of their account(s).

Password Guidelines

Users are responsible for the security of their passwords. Personal account information should not be released to friends, relatives, roommates, etc. Passwords should not be given to/or changed by UHD computer support personnel or co-workers. The only exception to this is when a user may call/or visit the UHD help desk for a reset of a locked/forgotten password. UHD has implemented account level challenge questions for students, faculty and staff that provide the ability for them to reset passwords

online without assistance. If they are not able to recall answers to their challenge questions, students must visit or call the registrar's office or the IT Help Desk directly to reset their passwords. Faculty and staff may visit or call the IT help desk to request that a password be reset. After the initial password is reset by IT personnel, faculty, staff and students are immediately required to change the password after the first time it is used to ensure password confidentiality. All verification of personal information needed to complete a password reset is carried out according to applicable state and federals laws as well as UH System and UHD policies.

System policies require that all new or changed passwords meet the following standards:

- Passwords should not be given over telephones, email, instant messaging, etc.
- All users are required to use complex passwords which must contain a character from at least three (3) out of the following four (4) character sets:
    - Capital letter (A-Z)
    - Lowercase letter (a-z)
    - Digit (0-9)
    - Special characters (such as !, $, #, %)
- Passwords must include a minimum of eight (8) characters and not exceed 16 characters
- All users are required to change their passwords at least once every 90 days and password histories are kept to ensure the passwords are not reused immediately.
- If any misuse of UHD's information resources is found, it is to be reported immediately to the appropriate management personnel. Any employee found to have violated this procedure may be subject to suspension of their UHD network and system access and/or disciplinary actions.

Authentication of Users

In order to use the University's computing environment, users receive a unique network account that allows them to authenticate. Users have an account created for them via the (NARS) Network Account Request System. The (NARS) Network Account Request System can be accessed (internal access only) at http://myaccountadmin.uhd.edu. Only specified administrative users designated by their department have the ability to create new accounts for Faculty/ Staff Users.

User Access to University Resources

A network account is provisioned for all UHD users and is the account used to gain access to University resources (internet, Banner, etc.) as well as mail. All users are given specific mailbox quotas. Users will receive access to user and departmental file shares upon request. Contractors are given access on a case-by-case basis and at the request of the hiring department. Contractors will not receive a UHD email address unless requested by a specific department. Users requiring specific access to non-standard applications are required to fill out a specialized account form to request access which requires them to obtain upper level departmental management approval for access to these applications.

A user's access to University resources will be terminated upon appropriate notification and documentation from ESO.

Network Access

This section defines the responsibilities of all users at the University with regard to network access. The owner or designated assignee of a computer that is attached to the UHD network is responsible for both the security of that computer system and for any *intentional or unintentional* activities from or to the network connections. Owners or designated assignees are responsible for all network activity originating from their equipment, regardless of who generates it. Any network-intensive application or defective computer that causes network overload shall be reviewed, and if necessary, steps shall be taken to protect other users and the overall UHD network. This includes contacting the offending party (if applicable) and disconnecting the defective computer system from the network until the problem is resolved. If the condition is an imminent hazard to the UHD network or disrupts the activities of others, the defective computer system or the subnet to which it is attached will be disabled without notice. The operator of the defective computer system will not be allowed to connect to the network until they follow explicit instructions from IT networking or help desk staff for securing the machine.

It is the responsibility of every person using UHD's information resources to refrain from engaging in any act that may seriously compromise, damage, or disrupt the UHD network. This includes, but is not limited to, tampering with components of a local area network (LAN) or the backbone, blocking communication lines, interfering with the operational readiness of a computer, creating/operating unsanctioned servers or personal Web servers or File Transfer Protocol (FTP) sites, or accessing/delivering unsanctioned streaming audio, video, or high bandwidth content such as gaming, music sharing or video conferencing.

The content of any files or services made available to others over the network is the sole responsibility of the user with ownership of and/or administrative authority over the computer providing the service. It is this user's responsibility to be aware of all applicable federal (FERPA, HIPAA, GLBA, DMCA) and state laws, as well as UHD policies. The user shall be liable for any violations of these laws and policies.

Network/internet connections used to share copyrighted materials (files, programs, songs, videos/movies, etc.) without permission of the copyright owner(s) is a violation of the DMCA. When informed by the copyright holder of a potential copyright violation, the University is required by Federal Law to remove the copyrighted materials from the system in question. If UHD is unable to remove these materials for any reason, then network access for the system in question will be terminated until the removal of the infringed materials is verified.

Users should refrain from using an IP address not specifically assigned to them and should not attempt to create unauthorized network connections or unauthorized extensions, or re-transmission of any computer or network services.

If any misuse of UHD's network resources is found, it is to be reported immediately to the appropriate management personnel and may be subject to criminal prosecution.

Handling of Sensitive/Confidential Information

Personnel of the University of Houston Downtown that deal with confidential and/or sensitive information concerning students and employees must be cognizant of their responsibilities concerning that information and exercise due caution when dealing with confidential or sensitive information.

Measures should be taken against disclosing information to unauthorized employees, contractors, vendors, parents, etc.

Sensitive/Confidential Information typically falls under the provisions of laws and regulations that impose security requirements designed to prevent unauthorized access to those records. Examples of such laws are the Health Information Portability and Accountability Act, which regulates access to Protected Health Information, and the Gramm-Leach-Bliley Act, which regulates access to non-public financial information about a University customer or employee and Family Educational Rights and Privacy Act (FERPA), a law that protects the privacy of student education records.

In order to secure sensitive information it is recommended:

- Privacy screens be used with any computer that displays sensitive or confidential information to avoid inadvertently being seen by others
- Workstations that typically are used for sensitive/confidential information should not be shared by others within/outside of the department
- Workstations should be locked when left unattended
- Workstations should be required to have a password to log in again when the workstation goes into sleep mode
- Confidential or sensitive printed information should not be left in plain view and should be secured when not in use (locked file cabinet, desk, etc.) and locked away after business hours
- Disposal of electronic/paper records are subject to the retention requirements set up by the State of Texas
- Should paper records need to be destroyed then the information should be shredded before discarding

Example of confidential/sensitive information includes but is not limited to:

- Passwords
- Social Security Numbers
- Performance reviews
- Most student information including schedules, grades, and student payroll information
- Confidential memos
- Medical information
- Credit card numbers
- Employee Payroll information
- Budgetary/financial information

Any abuse or disclosure of confidential or sensitive information whether accidental or deliberate, should be reported immediately to the appropriate management personnel.

III. Acceptable use of University Information Resources

The purpose of this section is to outline guidance, rules, and acceptable practices for the use of information resources at the University of Houston-Downtown in support of the *'Computer Access, Security and Use' Policy PS 08.A.04.* All users of the University's computing environment are also responsible for adherence to any State or Federal regulations regarding computer use at the University. This applies to all users of the University's network, web, e-mail, and computing resources, including any and all technical systems and services provided or owned by the University. Access to computing resources at the University is a privilege, not a right and is granted with restrictions, responsibilities and proper documentation for use. UHD reserves the right to limit, restrict, or extend privileges and access to its resources.

Security Awareness and Training

One of the most common security problems that users encounter is unauthorized use of their computer accounts, generally caused by their sharing their account with others (i.e. other UHD staff members, family, and friends). Account and password sharing is prohibited in all circumstances. Users should not log in as anyone other than themselves, and should not allow anyone to log in with their network account. Passwords should never be shared, written down, or disclosed to anyone- not even supervisors nor should they ever be sent through e-mail. If an employee needs access to another employee's electronic files, calendar, etc. the request should be made to their supervisor who will in turn check with ESO if permission can be granted.

If a user has problems with their network account they can contact the UHD Help Desk by calling (713) 221-8031.

Employee Accounts

All new employees at UHD are given specific information on getting and protecting their user accounts during the new employee orientation meeting held on the first day of their employment at the University. In addition, they are required to sign an employee confidentiality document, and provided IT Policy Statements, which outline their duties and responsibilities with all University information. On a yearly basis all employees, and new employees within the first 30 days of employment, are required to take a short informational security course to ensure that they remain up-to-date and cognizant of their security responsibilities and acknowledge that they will comply with the University's security policies and procedures.

If a user has problems with their network account they can contact the UHD Help Desk by calling (713) 221-8031.

Vendor Accounts

All other authorized users, e.g., Employees of independent contractors and vendors, etc., are required as well to sign 'Vendor Account Access Form' before they are given access to the University's resources. Vendor accounts are strictly monitored by the Division of Technology's Technical Services and are

assigned expiration dates and are given limited, secure access. The Vendor Account Form can be downloaded from the UHD website.

Guest Accounts

Official guests of the University can request an account for use at the University but are under the same restrictions as those on a Vendor accounts (e.g., Limited secure access, expiration dates, etc.) and are required to have a University sponsor to gain access to the UHD network. The Guest Network Account Request Form can be downloaded from the UHD website.

Assignment /Use of University Equipment

All UHD equipment is tagged for inventory purposes and assigned either to an individual or department by the Division of Information Technology's Computing/Telecom and Video Operations department.

All personnel requiring the use of individual workstations or assigned laptops are considered the custodians of that equipment and as such are expect to follow University guidelines concerning the securing of that equipment and data on the equipment.

Equipment taken off campus (e.g., Laptops, printers) requires the custodian of that equipment to sign a yearly Request to Remove Capital Property Off-Campus Form stating where the equipment is to be housed.

Routine personal usage of University resources may be permissible if, in the determination of the University, such use does not interfere with the University's mission or preempt normal business/educational activity, does not impede employee productivity, does not interfere with or negatively impact any other person's or entity's rights and work/learning environment, does not conflict with any rule or law, and does not consume more than a trivial amount of resources per the University's *'Computer Access, Security, and Use'* Policy PS08.A.04.*'*

Personal information including the storing of media such as iTunes music files, movies, photos, etc. should not be placed on any university network shared resource and is subject to removal without notice.

Any abuse or theft of University Equipment whether accidental or deliberate, should be reported immediately to appropriate management personnel.

University of Houston Downtown Sponsored Email

This section defines the responsibilities of all users at the University with regard to email.

Email accounts are only created after proper documentation has been supplied to the University. Any person using e-mail should not send excessive e-mail, attachments, or messages locally or over the network. As a general guideline when sending out an email to a large audience, the email messages should be of sufficient general value that it would justify being sent as a memorandum if email were not available. Campus-wide email discussions should use a Listserv (automated mail subscription service) when possible. The IT department can make these available on request for faculty and staff with proper authorization from supervisors of that department.

Each employee is required to complete UH System training, Secure Our Systems, which provides detailed instructions for managing and handling of sensitive data. All electronic mailboxes are not deemed to be private and are subject to review by management personnel after appropriate approval is first obtained by the Employee Service Office (ESO) if necessary or by request from the appropriate departmental supervisors. Any misuse of University Email whether accidental or deliberate, should be reported immediately to appropriate management personnel. The University reserves its right to limit capacity on individual email accounts for archival storage and other University purposes.

Authorized Software

The University has standard software applications that are applied to all University owned workstations. Any software that is installed by a user outside of the approved list may, at the discretion of Information Technology, or the user's department may be removed if the software is detrimental to the University environment.

The list of approved lab software can be found on the UHD website – approved lab software list.

Faculty may request certain software be applied to a computing lab if required for teaching their class. The department of User Support Services has specific guidelines for software installation. If you need software installed in the academic computing labs, electronic classrooms, or presentation classrooms for the purposes of teaching UHD accredited courses a Software Installation Request Form must be submitted to the User Support Services Department.

Physical Access

The University has its main data center situated in the One Main Building (OMB). Access to the data center is under the strict control of the Division of Information Technology's Computing/Telecom and Video Operations department and is strictly limited to Information Technology personnel. In cases where a vendor may need access to the data center, they will be accompanied by personnel from the Operations or Technical Services sections of Information Technology. There is an additional data center for disaster recovery at the Shea building which requires those accessing the area to use the same level of security and access requirements as those at OMB.

All student labs and electronic classrooms are monitored by the Division of Information Technology's Student Technology Services. Any problems with lab equipment can be reported to the UHD Help Desk by calling (713) 221-8031. Access to the electronic classrooms and departmental labs are strictly regulated by the classes taught in those labs. The electronic classrooms and departmental labs are available to students only when the instructor is teaching a class. The general labs are available to students during regularly scheduled published times which are published on the UHD website-lab schedule.

Remote Access

All remote access is limited to faculty and staff users. Students currently are not allowed remote access into UHD with any remote desktop software. The University only allows remote access with the use of security protocols. The use of encrypted protocols like Virtual Private Network (VPN) are required to ensure all transactions are encrypted and secure to and from the UHD network.

If remote access is necessary, the following restrictions apply:

- Remote access sessions must be encrypted using SSH, VPN, or similar technologies
- Remote access is provisioned to the fewest number of IP addresses possible (preferably only one)
- VPN software instructions can be found on the UHD website.

Wireless Computing

Faculty, staff, and students can access UHD's wireless network with their existing network account username and password. Note that any information sent over the wireless network that is not encrypted is unsecure and may allow others to view any and all information sent over the wireless network. Faculty and staff are strongly encouraged to use appropriate technology when accessing confidential employee or student data over wireless.

UHD Alumni may request a computer account for use on the wireless network. To request an account, please contact the Academic Computing Lab (800S). Alumni are required to abide by the *Regulations for Using Academic Computing Facilities and Resources* at the University of Houston-Downtown.

Guest accounts for the UHD network are provided as a courtesy for official visitors to the University. To obtain a Guest Account, ask your campus sponsor to complete the *Guest Network Account Request form* and submit this form to the Information Technology Office located in S-700, Main Building.

Coverage Areas include:

- One Main Building
- North & South Towers (all floors)
- Academic Building (all floors)
- Commerce Building (all floors)
- Shea Building (all floors)
- Willow Street Pump Station
- Student Life Center
- Welcome Center

IV. Other Issues

Malicious Code and Email

All users should refrain from downloading email from people they don't know or opening attachments that look suspicious as they can bring malicious code such as a viruses, Trojans, etc. into the University's environment.

An email may look legitimate but usually has markers that help identify it as suspicious. Words may be misspelled, floating the cursor over the hyperlink may indicate that the URL the link is attached to is not what is expected, the email asks for information that is not common (example: your password) or may indicate a user must do something to verify user information. If any email looks suspicious, a user may forward that email for review to the Division of Information Technology's User Support Services Help Desk at: help@uhd.edu.

V. Security with the University's Computing Environment

All enterprise-wide servers that deliver services across the University network are under the management of the Department of Information Technology at the University. Any department or person that wishes to connect a server to the infrastructure of the University's network environment must notify the IT Department of the University first.

Requirements for UHD Servers

No server may be connected to the UHD Network unless and until it complies with the following minimum technical and security standards:

- All servers that deliver services across the University network must be part of the University's network.
- The server must run an approved and appropriately licensed server operating system supported by Information Technology.
- The server must employ intrusion protection measures appropriate to its operating system, such as virus protection software, an independent intrusion protection appliance, and/or a host based firewall. Anti-virus software is provided by the University and found in e-Services under the Faculty and Staff icon, the section Service and Support and under the bullet entitled Software Download.
- Applications that require email services (e.g., SMTP) must be configured to direct all outbound email through a designated, centrally administered, UHD email gateway. Outbound email not configured in this manner may be blocked.
- Vulnerability patches and updates must be applied regularly, normally within 72 hours of becoming available and vendor certified. If compliance with this standard will conflict with operation or support of any application(s) hosted on the server, the server administrator must contact the IT Security to identify alternative protective measures.

Any departments that plan to buy new servers that will be used to house confidential information of any type must notify the IT Department of the University. In addition, if any department has at the University has a legacy system should contact the Division of Information Technology. Upon notification, the IT Operations and Technical Services group will facilitate an information resources risk assessment to ensure compliance with state and university standards and best practices per UHD's *'Review of Information Technology Resources Request'* policy PS 08.A.01.

Prior to the sale or transfer of any hardware, The Department of Information Technology of the University requires that:

- Notification to the Department is made so that inventory records can be updated as to the status of the hardware including and not limited to how that hardware was disposed of.
- An assessment is made by the data owners to remove data from any associated storage device and how that data will be removed (i.e. transferred to another location or destroyed).
- Confidential or sensitive information on that equipment be destroyed or relocated to type of secured media approved by the IT department.

- 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, resale or donation.

The following services are prohibited and must be disabled whenever the server is connected to the university network unless previously approved by the IT department of the university:

- Anonymous File Transfer Protocol (FTP)
- Domain Name Services (DNS) is allowed only on the University's centrally administered DNS servers
- Dynamic Host Configuration Protocol (DHCP) is allowed only on the University's centrally administered DHCP servers

System administrators must subscribe to notification and/or automated update services appropriate to the server hardware and software they are responsible for. System administrators must subscribe to University provided notification/update services (or equivalent) as those services become available (e.g., Texas State Server Administrators Listserv, SCCM – System Center Configuration Manager).

The server must authenticate all users other than local administrators, using the University's centrally administered login service and identity management credentials (i.e., Network Id and password) if the operating system or application permits. All communication of authentication credentials between the authenticating client and server must be encrypted. Authentication credentials must always be encrypted while in transit from a client or when at rest on the server. The server must enforce UHD's password standards.

The server must capture and archive critical user, network, system, and security event logs to enable review of system data for forensic and recovery purposes. The system administrator must review these logs for signs of malicious activity on a regular basis. Such logs should be retained for a period sufficient to address business requirements, document changes to access permissions, and provide an adequate history of transactions to satisfy audit requirements. Maintaining external copies of these logs is also recommended. Based upon risk assessment, server logs should:

- provide the means for authorized personnel to audit and establish individual accountability for any action that can potentially cause access to, generation of, modification of, or result in the release of confidential information;
- Maintain audit trails to establish accountability for updates to mission critical information, hardware and software, and automated security or access rules; and
- Maintain a sufficiently complete history of transactions to permit an audit of the server by logging and tracing the activities of individuals through the system.
- To the extent possible, the system administrator must configure the server operating system and/or resident applications to display a log-on banner to anyone requesting a connection to the server or application.

The server must not be administered remotely unless the remote access methodology has been specifically approved by IT Security. At a minimum, information transmitted during remote administration sessions must be encrypted. The server should accept remote administration commands from the fewest number of predefined hosts. Vendor accounts used for this purpose must be inactive at all times except when the vendor is actively engaged in providing support services.

Backup and Recovery

Backups are completed according to a risk assessment of the data and services provided. Restoration of software and data from backups should be tested on a regular basis to assure viability in the event of a service disruption. If backup media contains sensitive or restricted/confidential data, the data on the backup media or the media itself must be encrypted. Depending on the level of risk, central IT may designate specific backup procedures.

Server Hardening

Server hardening consists of creating a baseline for the security on servers at UHD. In general:

- The server must not be used for multiple purposes that would put its security or performance at risk.
- Physical access to any server and backup media must be restricted to persons with a legitimate need for such access.
- University servers should never be connected to any other network outside the University's without prior authorization from the appropriate personnel in the Information Technology department.
- Host-based intrusion detection should be installed
- System and application logging should be enhanced
- Requirements to achieve compliance with externally imposed standards must be identified and addressed before access to servers is given
- University security policies shall apply to all information and accounts on externally constrained servers

Incident Management

The Information Technology Help Desk is the centralized location for the University community to report issues concerning technology needs including but not limited to software problems, hardware problems, telephone issues, user accounts and access privileges. Should any incident require additional or escalating support the UHD Help Desk personnel are trained to route the information to the proper resource within the Information Technology staff using MAGIC. The proper recording of user information in the incident details of the MAGIC call is required when opening service requests and offers recorded documentation of the incident through its resolution.

Network Configuration

Prior to connecting the server to the university network the system administrator will:

- Disable all default accounts except those required to provide necessary services

- Change the default passwords for all enabled accounts, consistent with university password standards
- Terminate or disable all unnecessary user and support accounts
- Establish a minimal number of user accounts with administration privileges
- Apportion user accounts and/or groups to achieve proper separation of duties and to avoid the granting of excess privileges to any individual user or group
- Use the local administrator account only to perform server management functions
- Register the server with IT Security and for server protection by the University's network edge protection mechanisms (e.g., perimeter firewall, etc.)

VI. Websites concerning Security on a University, State and Federal Level

- University of Houston Downtown Information Security Website
- Texas Administrative Code Title 1, Part 10, Chapter 202, Subchapter C (Information Security Standards for Higher Education)
- Texas Penal Code, Chapter 33 (Computer Crimes)
- Texas Penal Code, Chapter 33(a) (Telecommunications Crimes)
- Texas Penal Code, Title 8 Chapter 37 sec. 37.10 (Tampering with a Governmental Record)
- U.S. Penal Code, Title 18, Section 1030 (Fraud and related activity in connection with computers)
- U. S. Penal Code, Title 18, Chapter 47 Section 1030 (Fraud and related activity in connection with computers)
- U.S. Penal Code, Title 18, Chapter 47 (Fraud and False Statements)
- Copyright Law of the United States
- Digital Millennium Copyright Act
- Computer Software Rental Amendments Act of 1990
- Texas Open Records Act
- FERPA (Family Educational Rights and Privacy Act)
- HIPPA (Health Insurance Portability and Accountability Act)
- GLBA (Gramm-Leach-Bliley Act)

VII. Definitions in this Handbook

The following words and terms, when used in this handbook, shall have the following meanings, unless the context clearly indicates otherwise.

University – Refer specifically to The University of Houston Downtown, an institution of higher education as defined by the Texas Education Code- Section §61.003.

Access – The physical or logical capability to interact with, or otherwise make use of information resources.

Business Continuity Planning (BCP) – The process of identifying mission critical data systems, critical personnel, and business functions, analyzing the risks and probabilities of service disruptions and developing procedures to restore those systems and functions.

Confidential Information – Information that must be protected from unauthorized disclosure or public release based on state or federal law (e.g. the Texas Public Information Act, and other constitutional, statutory, judicial, and legal agreement requirements).

Control – A safeguard or protective action, device, policy, procedure, technique, or other measure prescribed to meet security requirements (i.e., confidentiality, integrity, and availability) that may be specified for a set of information resources. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices.

Community – The group of people at the University that includes but is not limited to, all information resources management personnel, owners, system administrators, and users (faculty, staff and students) of the University's information resources.

Custodian of an Information Resource – A person responsible for implementing the information owner-defined controls and access to an information resource. Custodians may include state employees, vendors, and any third party acting as an agent of, or otherwise on behalf of the state entity.

Digital Millennium Copyright Act (DMCA) – The DMCA seeks to update the U.S. copyright law for the digital age in preparation for the ratification of the World Intellectual Property Organization (WIPO) treaties.

DMZ – A network area created between the public Internet and internal private network(s). This neutral zone is usually delineated by some combination of routers, firewalls, and other hosts. A DMZ usually includes devices that are accessible to Internet traffic.

Electronic Communication – A process used to convey a message or exchange information via electronic media. It includes the use of electronic mail (email), Internet access, Instant Messaging (IM), Short Message Service (SMS), facsimile transmission, and other paperless means of communication.

Encryption (encrypt, encipher, or encode) – The conversion of plaintext information into a code or cipher text using a variable, called a "key" and processing those items through a fixed algorithm to create the encrypted text that conceals the data's original meaning.

Family Education Rights and Privacy Act (FERPA) – A federal law protecting the privacy of student education records.

Firewall – A software or hardware device or system that filters communications between networks that have different security domains based on a defined set of rules. A firewall may be configured to deny, permit, encrypt, decrypt, or serve as an intermediary (proxy) for network traffic.

Gramm-Leach Bliley Act (GLBA) – Includes provisions to protect consumers' personal financial information.

Health Insurance Portability and Accountability Act of 1996 (HIPPA) – Protects the privacy of individually identifiable health information held by covered entities and the individual's rights with respect to that information.

Information Owner – A person with statutory or operational authority for specified information (e.g., supporting a specific business function) and responsibility for establishing the controls for its generation, collection, processing, access, dissemination, and disposal. The Information Owner may also be responsible for other information resources including personnel, equipment, and information technology that support the Information Owner's business function.

Information Resources – Is defined in §2054.003(7), Government Code and/or other applicable state or federal legislation.

Information Security Program – The elements, structure, objectives, and resources that establish an information resources security function within an institution of higher education, or state agency.

Information Technology (IT) – The entity at the University of Houston Downtown that is responsible for the maintenance, update, and enforcement of the security policies at the University.

Intrusion Detection System (IDS) – Hardware or a software application that can be installed on network devices or host operating systems to monitor network traffic and host log entries for signs of known and likely methods of intruder activity and attacks. Suspicious activities trigger administrator alarms and other configurable responses.

Intrusion Prevention System (IPS) – Hardware or a software application that can be installed on a network or host operating system to monitor network and/or system activities for malicious or unwanted behavior and can automatically block or prevent those activities. (Firewalls, routers, IDS devices, and anti-virus gateways all may have IPS capabilities). IPS can make access control decisions based on application content.

Mission Critical Information – Information that is defined by the institution of higher education, or state agency to be essential to the institution of higher education, or state agency function(s).

Platform – The foundation technology of a computer system. The hardware and systems software that together provide support for an application program. (Ref: Practices for Protecting Information Resources Assets.)

Risk Assessment – The process of identifying, evaluating, and documenting the level of impact that may result from the operation of an information system on an organization's mission, functions, image, reputation, assets, or individuals. Risk assessment incorporates threat and vulnerability analyses and considers mitigations provided by planned or in-place security controls.

Risk Management – Decisions to accept risk exposures or to reduce vulnerabilities and to align information resources risk exposure with the organization's risk tolerance.

Router – A device or, in some cases, software in a computer, that determines the next network point to which a packet should be forwarded toward its destination. The router is connected to at least two networks and decides which way to send each information packet based on its current understanding of the state of the networks to which it is connected. A router is located at any intersection where one network meets another.

Sanitize – A Process to remove information from media such that data recovery is not possible: includes removing all confidential labels, markings, and activity logs.

Security Incident – An event which results in accidental or deliberate unauthorized access, loss, disclosure, modification, disruption, or destruction of information resources.

Sensitive Personal Information – A category of personal identity information as defined by §521.002(a)(2), Business and Commerce Code

Storage Device – Any fixed or removable device, which contains data and maintains the data after power is removed from the device such as a DVD/CD-ROM, external or internal hard drive, Universal Serial Bus (USB) flash drive, memory card, or media player.

Test – A simulated or, otherwise documented event for which results and records are kept.

Threat – Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

User of an Information Resource – An individual or automated application authorized to access an information resource in accordance with the information owner-defined controls and access rules.

Vulnerability Assessment – A documented evaluation containing information which includes the susceptibility of a particular system to a specific attack.

Wireless Access (WA) – Using one or more of the following technologies to access the information resources systems of a state agency or institution of higher education:

Wireless Local Area Networks (WLAN) – Based on the IEEE 802.11 family of standards.

Wireless Personal Area Networks (WPAN) – Based on the Bluetooth and/or Infrared (IR) technologies.

Wireless Handheld Devices (WHD) – Includes text-messaging devices, Personal Digital Assistant (PDAs), and smart phones. NIST SP 800-48 provides an overview of Wireless Network Security 802.11 technologies and provides guidelines to reduce the risks associated Bluetooth and Handheld Devices.

VIII. IT Contacts

Name	Title	Contact Information
Hossein Shahrokhi	Associate Vice President, Information Technology	shahrokhih@uhd.edu
Said Fattouh	Director, User Support Services (USS)	fattouhs@uhd.edu
Kong Yin	Director, Enterprise Systems (ES)	yink@uhd.edu
Grace A. Davila	Director, Technical Services (TS)	davilag@uhd.edu
Miguel Ruiz	Director, Computing, Telecommunication and Video Operations	ruizm@uhd.eud
John Lane	Director, Technology Learning Services (TLS)	lanej@uhd.edu
Jackie Smith	Director, IT Business Services	smithja@uhd.edu
Jon Garza	Information Security and Compliance Officer	garzaj@uhd.edu
Jennifer Huenemeier	Senior IT Project Manager and Compliance Analyst	huenemeierj@uhd.edu

IX. End Notes

TAC 202.70 – Responsibilities of the Institutional Head

TAC 202.71 – Responsibilities of the Information Security Officer

TAC 202.72 –Staff Responsibilities

TAC 202.73 –Security Reporting

TAC 202.74 –Institution Information Security Program

TAC 202.75 – Managing Security Risks

TAC 202.76 – Security Control Standards Catalog