UNIVERSITY of HOUSTON

YOU ARE THE PRIDE

UNIVERSITY INFORMATION TECHNOLOGY

SECURITY HANDBOOK

Mission Statement:

UIT Security is responsible for developing security best practices, promoting security awareness, coordinating security issues, and conducting investigations. UIT Security works within UIT, UHS component campuses and campus departments to protect UHS information resources, minimize security risks and ensure compliance with security policies and procedures.

What do we do?

The University of Houston relies heavily on computers and the information residing on those computers. A system of security controls exists to safeguard these assets. While it is the responsibility of the information resource owners, custodians, and users to comply with TAC 202, GLB Act, FERPA, PCI, HIPAA, and other federal requirements, UIT Security is available to provide counsel and guidance to assist in the assurance of the confidentiality, integrity and availability of the university's information resources.

Services We Offer:

- Development of IT Security Policies & Procedures
- Guidance on IT Security Best Practices, Design and Architecture
- Security Risk Assessments
- Security Awareness and Training – Faculty, Staff, Students
- Security Incident Monitoring, Response & Reporting
- SSL Certificate Administration
- 2-Factor Authentication Administration for PCI compliance
- Web Site Security Scanning
- Intrusion Detection
- Computer Vulnerability Scanning
- Guidance on Compliance Initiatives - UHS, State, Federal, PCI
- Wireless Security Scans

User Security Tools

Client Tools Available for Download

The following software is available free for faculty, staff and students at the University Information Technology website:
www.uh.edu/infotech/php/software_downloads.php

Anti-Virus Software

Anti-virus software should be installed on all computers. UH provides anti-virus software for Windows and Mac computers.

VPN (Virtual Private Network)

VPN software allows users to connect to internal UH computer resources from off-campus. UH provides VPN software for Windows, Mac and Unix computers. Please note: VPN software is not needed to access web-based campus resources such as email, PASS and WebCT.

Windows SSH Secure Shell for Workstations (SSH2)

SSH Secure Shell for Workstations is usually only needed by those performing system updates and other technical functions.

Secure FTP software

Secure FTP software is usually only needed by those performing website updates and other technical functions. UH provides secure FTP software for Windows and Mac computers.

Identity Finder

Identity Finder software scans computers for personal identifying information. UH provides licenses for faculty and staff to use the software on university-owned machines. Identity Finder Home Edition for Windows and Mac is available to students free of charge. A discounted version is available for faculty and staff at a discounted rate.

Tools and Services Available Directly from UIT Security

For access to any of the following tools or services, please contact **security@uh.edu**.

- Web Site Security Scanning
- 2-Factor Authentication Administration for PCI compliance
- ISS Vulnerability Scanning
- Identity Finder Console Application

Security Policies & Procedures

UH System Security Policies

UIT Security is responsible for enforcing and investigating violations of UH System security policies. UHS policy requires that all University of Houston users comply with System Administrative Memoranda (SAM) policy regarding the use of information resources.

SAM 07.A.02 – The Ethical and Legal Use of Personal Computer Software (www.uh.edu/af/universityservices/policies/sam/7InfoServices/7A2.pdf)

SAM 07.A.04 – Digital Millennium Copyright Act (www.uh.edu/af/universityservices/policies/sam/7InfoServices/7A4.pdf)

Complete UHS IT policies can be found at:

SAM Policies - Information Services (http://www.uh.edu/af/universityservices/policies/sam/7InfoServices.htm)

UH Campus Security Policies

UIT Security is responsible for establishing and enforcing University of Houston information security policies and for investigating security incidents involving University information and information systems. The University of Houston Manual of Administrative Policies & Procedures (MAPP) outlines the responsibilities of all users and departments in regards to University information resources.

All users of University information resources are responsible for appropriate use and protection of those resources.

MAPP 10.03.01 – Acceptable Use of Information Resources (http://www.uh.edu/af/universityservices/policies/mapp/10/100301.pdf)

All users of University information resources are responsible for knowing the data classification level of information they are using, and protecting the information appropriately.

MAPP 10.05.03 – Data Classification and Protection (http://www.uh.edu/af/universityservices/policies/mapp/10/100503.pdf)

All actual or suspected security incidents involving University information resources must be promptly reported to UIT Security.

MAPP 10.05.02 - Information Security Incident Reporting and Investigation (http://www.uh.edu/af/universityservices/policies/mapp/10/100502.pdf)

Colleges and departments are responsible for the use of the information resources under their control. This policy requires each University area to have internal policies and procedures governing the use of their information resources that ensure compliance with all University policies, federal and state laws, and contractual obligations.

MAPP 10.03.06 - College/Division Responsibilities for Information Technology Resources (http://www.uh.edu/af/universityservices/policies/mapp/10/100306.pdf)

Users and departmental IT support personnel should ensure that security controls on each information resource is commensurate with the data the system contains or the function(s) the system performs.

Complete UH IT polices can be found at:

MAPP Policies - Information Technology (http://www.uh.edu/af/universityservices/policies/mapp/10mappit.htm)

Copyright Violations

UIT Security investigates reported cases of copyright violations involving University of Houston computers and computer users. Suspected cases of copyright infringement should be reported to UIT Security by sending email to **dmca@uh.edu**. Additional information on copyright compliance can be found at www.uh.edu/dmca.

Incident Response

UIT Security is required by University policy and Texas state law to investigate all suspected information security breaches that occur at the University of Houston. All members of the University community are required to assist and cooperate in the investigation process. If you suspect that a computer has been compromised, there are things you should do to protect the system and the information it contains and/or processes, and to assist in the investigation.

1. Contact UIT Security as soon as possible to report the incident.
2. Document any unusual system activity or behavior, unknown or unauthorized users and processes, and any other facts and information that could assist with the investigation of the incident.
3. Determine if sensitive or critical information is stored, used or processed on the system; this includes (but is not limited to) student records, employee personal information, such as Social Security numbers, or financial information such as credit card numbers. This information should be documented and reported to UIT Security.
4. Preserve the system in its original compromised state to the best of your ability; however, if sensitive or vital information is on the system, or other critical system resources are at risk, you should take action to prevent further loss or damage.
5. Protect the system from further attack or damage. If the system is currently under attack or control of an attacker or unauthorized user, you should remove the system from the network. This is often most easily accomplished by removing or unplugging the network cable. In some extreme cases, you may need to manually terminate unauthorized users or processes, or power off the system. Document all information regarding any procedures you take.
6. Make the system and all information, notes and observations you have made regarding the incident available as needed and cooperate fully with the investigation.

Security Best Practices

1. Restrict access rights by limiting the use of administrator privileges. This will help prevent the potential installation of malware & other unwanted software by unsuspecting users.

2. Keep systems updated with all of the current security patches. Where possible, turn on automatic updates to apply operating system security updates. When using images to support multiple systems, be sure the image is updated regularly with all applicable patches and virus definitions.

3. Automatic updates offered by Windows and Macs do not always patch third party applications such as Adobe, Flash, Java, etc. Be sure to check regularly for updates to these applications or consider using an automated patching solution.

4. Make sure all data is deleted from computers before they are sent to property management.

5. Passwords should be used on mobile devices to prevent unauthorized access to information if the device is lost or stolen (e.g. BlackBerry, Smartphones, etc).

6. Do not save sensitive information to mobile devices. Be sure to encrypt sensitive data wherever it is stored.

7. Enable computer firewalls. Windows and Mac computers come with built-in firewalls.

8. Use anti-virus & anti-malware software and update the definitions regularly. Free software is available on the UIT website.

9. Back up your data frequently. A free backup service, Tivoli Storage Manager, is provided by UIT and is available for faculty and staff computers.

10. When changing your password, remember to change your password in all locations where you may have your credentials stored to prevent account lockout.

To contact the IT Security Team by phone or email:

Phone: 832-842-4695

E-mail: Security@uh.edu

Reporting a Security Incident

Any security incident, such as the unauthorized access of a university system or data, unauthorized use of a user's account or the accidental distribution of sensitive data (i.e. payment card number or social security number), can be reported in the following three ways:

- Send an email to: **security@uh.edu**
- Visit **http://www.mysafecampus.com** to report an incident anonymously
- Call: **832-842-4695**

Reporting a Computer Abuse Incident

Computer abuse incidents include: the misuse and abuse of computer resources, tampering with other users' data, harassment of other users, unauthorized alteration of computer configuration, deliberate wasteful practices, online behavior that intimidates or offends, or any behavior that violates university policy or is potentially unlawful. To report a computer abuse incident, send an email to **abuse@uh.edu**.

Reporting a Copyright Violation

UIT Security investigates reported cases of copyright violations involving unauthorized copying/distribution of copyrighted/licensed material using University of Houston computers or network. Suspected cases of copyright infringement should be reported to UIT Security by sending an email to **dmca@uh.edu**.

Revised August 2012