



SECURITY HANDBOOK

FALL 2009



Mission Statement:

IT Security is responsible for developing security best practices, coordinating security issues, conducting investigations and working within IT and other campus departments to minimize security risks and assure compliance with security policies and procedures.

What do we do?

The University of Houston relies heavily on computers and the data 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, Information Technology Security is available to provide counsel and guidance to assist in the assurance of the confidentiality and integrity of information resources.

Services We Offer:

- Development of IT Security Policies & Procedures
- Guidance on IT Security Best Practices, Design and Architecture
- Security Risk Assessments
- Computer Security Awareness 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

Campus Security Tools

Client Tools Available for Download

The software listed below, along with installation instructions and user documentation is available at the UH Information Technology website:

http://www.uh.edu/infotech/php/software_downloads.php

SSL Certificates are also available for purchase through the website.

Additional assistance with user issues can be obtained from the UH IT Support Center via email: support@uh.edu, in person: 116 PGH or via phone: 713-743-1411.

Anti-Virus Software:

Anti-virus software should be installed on all computers. UH provides free anti-virus software to students, faculty and staff. Anti-virus software for both Mac and Windows computers are available.

VPN (Virtual Private Network):

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

SSH Secure Shell for Workstations (SSH2):

SSH Secure Shell for Workstations is usually only needed by those performing system updates and other technical functions. UH provides free SSH Windows client software to students, faculty and staff.

Fugu Secure FTP for Mac OSX:

Secure FTP software is usually only needed by those performing website updates and other technical functions. UH provides Fugu documentation and a link to download.

Identity Finder:

Identity Finder software can scan computer systems for personal identifying information. UH provides licenses for faculty and staff to use the software on university-owned machines. UH provides a link for students to download and register Identity Finder Home Edition for Windows and Mac free of charge from Identity Finder.

Tools and Services Available Directly from IT Security

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

- Web Site Security Scanning
- 2-Factor Authentication Administration for PCI compliance
- ISS Vulnerability Scanning

Security Policies & Procedures

UH System Policies

IT 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 systems.

SAM 07.A.02 - The Ethical and Legal Use of Micro/Personal Computer Software
(<http://www.uhsa.uh.edu/sam/7InfoServices/7A2.pdf>)

SAM 07.A.04 – Digital Millennium Copyright Act
(<http://www.uhsa.uh.edu/sam/7InfoServices/7A4.pdf>)

Complete UHS IT policies can be found at:

SAM Policies - Information Services
(<http://www.uhsa.uh.edu/sam/7InfoServices.htm>)

UH Campus Security Policies

IT 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 systems.

All users of University systems are responsible for those systems and for their protection.

MAPP 10.03.01 – Computer User Responsibilities
(<http://www.uh.edu/mapp/10/100301.pdf>)

All actual or suspected security incidents involving University information systems must be promptly reported to Information Technology Security.

MAPP 10.03.02 - Computer and Network Security
(<http://www.uh.edu/mapp/10/100302.pdf>)

MAPP 10.03.03 - Security Violations Reporting
(<http://www.uh.edu/mapp/10/100303.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 assets 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/mapp/10/100306.pdf>)

Users and departmental IT support personnel should ensure that security controls on each information system is commensurate with the data the system contains or the function(s) the system performs (Information Security Manual, Section 22 - Technical security requirements).

Complete UH IT policies can be found at:

MAPP Policies - Information Technology
(<http://www.uh.edu/mapp/10infotech.htm>)

Information Security Manual
(http://www.uh.edu/infotech/php/template.php?nonsvc_id=268)

Information Protection

All University information and the systems that use or process the information need to be protected. The requirements for each system are directly related to the sensitivity/criticality level of the data it contains and processes. At a minimum, each system should have anti-virus software installed, and a backup plan which can be implemented if needed. Additional protection mechanisms, such as username and passwords, system firewalls or encryption schemes should be implemented as needed, consistent with University policy.

Each college and department is responsible for determining the criticality of the information and information systems under their control, and for implementing mechanisms to ensure their protection. Guidelines for making these determinations can be found in Section 22 – “Technical Security Requirements” and Appendix B of the Information Security Manual. The guidelines detailed in these references outline minimum requirements; each college and department should evaluate their own information protection requirements and implement additional safeguards appropriate for their own operations. Questions regarding the protection of information and the measures taken to accomplish this protection should be directed to Information Technology Security.

Copyright Violations

IT Security investigates reported cases of copyright violations involving University of Houston computers and computer users. Suspected cases of copyright infringement should be reported to IT Security by sending email to dmca@uh.edu.

Additional UHS information on copyright compliance can be found at:

Information on Copyright Compliance -
<http://www.uhsa.uh.edu/common/copyright.html>

Reporting Copyright Infringements -
<http://www.uhsa.uh.edu/common/infringements.html>

Incident Response

Information Technology 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 Information Technology 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 IT 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 and 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 FireFox, 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. Where possible, set passwords on your mobile devices (i.e. Smartphones).
6. Do not save sensitive information to portable drives. Be sure to encrypt sensitive data wherever it is stored.
7. Enable computer firewalls. Mac and Windows computers come with built-in firewalls.
8. Use antivirus software and update the definitions regularly. Free antivirus software is available on the IT website for students, faculty and staff.
9. Back up your data frequently. A free backup service, Tivoli Storage Manager, is provided by IT and is available for faculty and staff computers
10. Educate users about safe browsing habits.
11. Create and enforce policies to prevent the installation of unlicensed/unapproved software.
12. 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

A security incident such as the unauthorized access of a university system or data, unauthorized usage 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, any behavior that violates university policy or is potentially unlawful. To report a computer abuse incident, send email to abuse@uh.edu.

Reporting a Copyright Violation

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