UH Policies are available at - http://www.uh.edu/af/universityservices/policies/mapp/
IT Policies are available at - http://www.uh.edu/af/universityservices/policies/mapp/10mappit.htm
G. University information resources are provided in support of the mission and goals of the university. Examples of inappropriate use include, but are not limited to, activities relating to personal or corporate profit, viewing creating or transmitting obscene material (as commonly defined by applicable federal and Texas law), or for the production of an output that is unrelated to the objectives for which the account was issued. Incidental personal use is acceptable with the following restrictions:

1. Incidental personal use of e-mail, internet access, fax machines, printers, copiers, etc., is restricted to university approved users; it does not extend to family members or other acquaintances.
2. Incidental personal use must not result in direct costs to the university.
3. Incidental personal use must not interfere with the normal performance of an employee’s work duties.
4. No files or documents may be sent or received that may cause legal action against the employee or the university.
5. Storage of personal e-mail messages, voice messages, files, and documents within the university’s information resources must be nominal.
6. All messages, files, and documents – including personal messages, files, and documents – located on university information resources are owned by the university, may be subject to open records requests, and may be accessed by the university in accordance with this policy. University employees (including supervisors) are not authorized to access the e-mails of a current or former employee without their consent unless there is a business justification and prior approval is obtained by contacting the Executive Director of IT Security, who will review the matter in consultation with the Department of Human Resources and the Office of the General Counsel before authorizing access to the e-mails.
7. Use of university facilities, equipment, or other resources for consulting or other non-university business activities is prohibited unless a financial arrangement has been made between the individual and the university, and it has been approved by the department head or director prior to the employee’s use for the external purpose.

H. Users of university information resources have no expectation of privacy while using a university information resource except as otherwise provided by applicable privacy laws. Access to user e-mail messages may only be granted in accordance with Section IV (G) (6) above.
WIRELESS NETWORK

All wireless network access point devices shall be provided by UIT. Any exceptions must be authorized by UIT through the process outlined in Section III. All wireless access points must meet the following requirements:

1. All wireless access point devices must be registered by UIT. UIT regularly performs building-to-building assessments to detect unauthorized wireless access point devices.
2. The wireless router or access point administration interface must be secure. The default password must be changed to be a strong password as described in MAPP 10.05.01 - Information Security Program. Guest access or accounts should be disabled.
3. The SSID must be changed from its default. Naming convention information is located on the UIT web site.
4. The strongest form of encryption should be used. Encryption of at least 128 bit must be enabled on the access point.
5. Wireless administration must be disabled. Access points should only be administered via a wired connection.
6. Confidential and sensitive personal information is prohibited from being transmitted over wireless network devices unless an encryption method such as Virtual Private Network (VPN) is utilized.
1. When the contents of an e-mail message exhibit one or more of the following characteristics, it should be classified as a university/business record:

   a) Has operational value (required by a department to perform its primary function)
      - Administrative actions taken or planned
      - Reports or recommendations
      - Policies, procedures, guidelines, rubrics, or templates
      - Non-transitory communication pertaining to routine operation of policies, programs, services, or projects of the university or of a department

   b) Has legal or evidential value (required to be kept by law), such as a legal hold or investigation (see “Legal Holds” below).

   c) Has fiscal value (related to the financial transactions of the campus), required for financial reporting and audits.

   d) Has historical significance (of long-term value to document past events). These messages may arise from exceptional age and/or some significant historical event.

   e) Has vital value (critical to maintain to ensure operational continuity after disruption or disaster). Vital records or information may fall into any one of the above value categories.

2. University/Business records, including messages and information, must be retained as noted in SAM 03.H.01 – Records Retention, and in accordance with the Texas State Records Management Statutes. See in particular, Section 1.1 on General Administrative Records.
4. User access must employ the use of a password. The degree of complexity of the password is dependent upon the highest level of data that can be accessed by the user. Passwords must be changed regularly. A strong password must contain each of the following:

a. At least 8 characters  
b. At least one alphabetic character (upper or lower case, a-z or A-Z)  
c. At least one number (0-9)  
d. At least one special character (!, @, #, $, %, ^, &, (, ), *)

J. Security Awareness and Training – All users of University information resources will participate in Security Awareness and Training regularly. Awareness and training efforts cover applicable state and federal laws, information security best practices, and identification and reporting of information security incidents.

K. Security Incident Handling & Information Disclosure – All security incidents must be reported and investigated in accordance with MAPP 10.05.02, Information Security Incident Reporting and Investigation. Policies related to information disclosure are found in SAM 01.D.06, Protection of Confidential Information.

You can always email the IT personnel about any IT security related incident or contact the UH IT security directly at security@uh.edu
SUBJECT: Data Classification and Protection
Number: 10.05.03


A. Critical information resource: An information resource housing confidential, sensitive personal or mission critical information. Critical information resources must have the following physical and technical safeguards implemented:

1. Physical access granted only to authorized personnel via access cards, keys or other control mechanisms.
2. Protection from environmental hazards.
3. Regularly completed backups of all files. If the University Information Technology backup system is not used, the backup data must be stored in a separate, secure area.
4. Uninterrupted power supply (UPS).
5. Relevant security patches installed.
6. Anti-virus software installed and appropriately configured.
7. Unnecessary and/or inactive accounts must be disabled or deleted.
8. Vendor-supplied system passwords must be replaced with strong passwords.
9. Audit/security logs enabled on the critical information resource.
10. Prior to the disposal of the critical information resource, a secure destruction method must be used to ensure the resource is sanitized rendering the data unrecoverable.