Administrative Computer Networks, Hardware, and Software

All departments and staff are bound by the following computer-related University Policies:

- Off-campus use of computers, HOP 4-1120-PM
- University of Texas Code: Information Resources Use and Security Policy UTS165
- Texas Administrative Code: Information Security Standards Title 1 Part 10 Chapter 202

The Utilities Department is the owner of all Utilities information resources, data and the computer installation. Technology Resources for Employee and Campus Services (TRECS) has custodial responsibility for the Utilities Department computer installation and information resources. TRECS supports the Executive Director of Utilities in complying with the department's, University's and State's related policies for the Utilities Department's computer installation and use of information resources.

Note: The custodial responsibility of TRECS does not extend to facility controls or monitoring functions for equipment, building systems or vendor-supported facilities devices. Computer systems performing these services may or may not be covered by this policy and may or may not be supported by TRECS at the discretion of the Utilities Executive Director or his designee.

Computer User Responsibilities

Each employee is responsible for using Utilities computer resources responsibly within, but not limited to, the following:

Appropriate Use

- Personnel are responsible for managing and securing their access to and use of Utilities information resources and computer installation.
- Personnel must not bypass or disable security controls.
- Personnel shall not attempt to access any data, program, computer or information resource for which they do not have authorization or explicit consent.
- Personnel shall not share their passwords, personal identification numbers, security tokens and other authentication devices.
- Personnel shall protect passwords, personal identification numbers, security tokens and other authentication methods from use by, or disclosure to, another individual or organization.
- Personnel shall not purposely engage in activity that may: harass, threaten or abuse others; degrade the performance of information resources; deprive an authorized user access to a resource; obtain extra resources beyond those allocated; or circumvent computer security measures.
- Personnel shall not download, install or run programs or utilities on the Utilities Department information resources or computers which reveal or exploit weaknesses in information resources or the computer installation.
- Personnel shall not intentionally access, create, store or transmit material which Utilities may deem to be offensive, indecent or obscene.
- Material changes or modification to the Utilities Department information resources, networks, programs or data must be reviewed by the executive director of Utilities or his designee and TRECS.

- Personnel shall not host servers or services on the Utilities Department networks without approval from its Executive Director and TRECS.

Account Management and Privileged Access

- Authorization to the Utilities Department information resources is determined by its Executive Director and his delegates including Associate Directors, Assistant Directors and/or Managers with guidance from TRECS.
- Each individual that has administrative or special access must use the minimum privilege account that is able to perform the work (i.e. user account vs. admin account).
- Administrative & management access will be given to Managers and above at the time of hire.
- When temporary or special access is given or a special account is created, it must:
    - be properly authorized;
    - created with an expiration date;
    - have a departmental manager sponsor; and
    - be removed when the work is complete.
- Each individual that uses special or administrative privileges must refrain from misuse.
- The minimum privilege level for personnel using individually assigned computers is power user.
- The minimum privilege level for personnel using assigned laptops is administrator.
- The minimum privilege level for personnel using common computers is user.
- Increase to privilege levels must be reviewed and approved by the Executive Director of Utilities or his designee and TRECS.

Personal Use

- As a convenience to Utilities employees, incidental use of the Utilities Department information resources is permitted within the following restrictions:
    - Incidental personal use of e-mail, internet access, fax machines, printers, and copiers is restricted to approved users (not extended to family or friends).
    - Incidental use must not result in direct costs to the Utilities Department.
    - Incidental use must not interfere with the normal performance of an employee's work duties.
    - Storage for personal e-mail messages, voice messages, files and documents with the Utilities Department information resources must be nominal.
    - No files or documents may be sent or received that may cause legal action against or embarrassment to the Utilities Department.
    - All messages, files and documents—including personal messages, files and documents—located on the Utilities Department information resources or funded by Utilities may be subject to open records requests and may be accessed in accordance with this policy.
- Use of certain University of Texas information resources intended for personal use or provided as an employee benefit may or may not be subject to this policy.
- Use of Utilities information resources from a home-based computer must adhere to all of the same policies that apply to use of that resource while at work.
- Utilities information resources must not be used for personal or financial gain.

Reporting Incidents

- Passwords must be treated as confidential information and must not be divulged to anyone. (TRECS will not request passwords.)If passwords are found, discovered or disclosed, personnel must notify TRECS to secure the password.
- Personnel shall report all security violations to department management.
- Personnel are responsible for reporting any suspected or confirmed violations of this policy to the appropriate management.
- Personnel shall contact TRECS whenever a security incident, such as a virus, worm, hoax, e-mail, compromise, or altered data is suspected or confirmed.
- Personnel must report weaknesses in computer security or incidents of possible misuse or violation to the Utilities Department management and TRECS.

Physical Access

- Computing devices must not be left unattended without securing them.
- Systems not in use for extended periods of time are to be powered off.

Privacy and Monitoring

- There is no guarantee of personal privacy when using information resources.
- There is no guarantee of access to information resources.
- Use of information resource may be monitored.

Electronic Identifiers and Access

- Personnel who are users of Utilities information resources shall be assigned a unique user account.
- Personnel who are users shall be authenticated before the information resources system grants access.

Data Security

- Personnel shall secure data, both electronically and on paper, according to the department's security classification for that data.
- Personnel are responsible for backup of any files stored on the local computer including the desktop.
- Personnel shall store Utilities data in designated locations according to each department's operation practices.
- Personnel are responsible for backup, security and loss of files stored in areas other than those designed by departmental practices.

Software

- Personnel must not use or install non-standard shareware or freeware software without Utilities and TRECS departmental approval.
- Personnel must not make unauthorized copies of copyrighted software or materials.
- The Executive Director of Utilities or his designee must approve all requests for equipment and software not on the Utilities standards list prior to purchase.
- All commercial software used on Utilities computer systems must be supported by software license agreement specifically describing the usage right and restrictions of the product.
- Personnel must abide by all license agreements and must not illegally copy licensed software.

- TRECS reserves the right to remove any unlicensed software from any computer system. All computer software, programs, applications, source code, object code, documentation and data shall be guarded and protected as if it were State property.
- TRECS reserves the right to remove any non-business related software or files from any system.

Virus Protection

- All workstations whether connected to UT-Net or stand alone, must use the TRECS-approved virus protection and configuration.
- The virus protection must not be disabled or bypassed.
- The settings for virus protection software must not be altered in a manner that reduces the effectiveness of the software or the frequency of updates.
- Each virus incident that is not automatically cleaned by the virus protection software constitutes a security incident and must be reported to TRECS.
- Personnel must review e-mail for its potential virus risk before opening and must permanently delete suspicious e-mail.

E-Mail

- Utilities shall provide an e-mail and calendaring mailbox with AEMS (@austin.utexas.edu or @ cpfm.utexas.edu) to personnel routinely using a computer or needing electronic communication for Utilities work.
- Personnel shall use this e-mail and calendaring systems for Utilities business.
- New mailboxes, distribution lists, resource mailboxes, and special mailboxes are reviewed and approved by the Executive Director of Utilities or his designee and TRECS.

Technical Assistance

- Personnel shall submit work requests to the TRECS line (232-FISH) or web page (See Service Request)

Computer Resource Purchasing

Mass equipment upgrades are coordinated through Facilities Information Systems (TRECS). Requests for individual equipment and estimated costs will be forwarded through the Assistant Director, Associate Director, or the Executive Director with an explanation of why the equipment or software is needed. Requestors will obtain estimated costs from the Senior Administrative Associate, Facilities Information Systems (TRECS) and include that estimate on the request. The request should also include the fund source account number and work order number to be used for the purchase. The procedure applies to:

1. Equipment: high value equipment and peripherals such as CPUs, monitors, scanners, external disk drives, printers, and copiers/faxes. This procedure does not apply to low cost peripherals such as keyboards, mouse, cabling, or speakers. Upon the Executive Director’s approval, the requestor will coordinate the equipment purchase through TRECS.

2. Software: Requests for software not on the approved list must be submitted to the Director for approval. A current approved list may be found at the TRECS web site. Upon the Executive Director’s approval, the requestor will coordinate the software purchase through TRECS.

Policy Waivers

In the case of special needs, a departmental policy waiver can be granted. To request a policy waiver, submit a request to the Executive Director of Utilities and the Director of TRECS.