

Security

The security of Utilities employees and their personal effects, as well as the security of University property and data, is a matter of great importance. Under current state law, each employee can be financially liable for the loss, damage, or theft of University property and data if the loss occurred as a result of negligence on the part of the employee.

In safeguarding University property and data, as well as your own, please observe the following:

- **Data Security**

- All authorized users of Utilities (including but not limited to institution of higher education personnel, temporary employees, and employees of independent contractors), shall protect the security of records containing sensitive data that is stored on university property and desktops or portable computing devices by using physical and technical safeguards through the encryption of electronic records, backups, and locking physical files.

Sensitive data, regardless of form or media in which it may be recorded, includes but is not limited to the following, protected medical/health information, student records, donor/alumni information, research information, employee information, business/vendor data, and other institutional data such as critical infrastructure details.

- Sensitive digital data must not be stored on university or personal computers or other electronic devices such as laptops, hand-held devices, flash drives, or other portable computing devices unless:
 1. It is secured against unauthorized access; and
 2. It will not compromise business or research efforts or privacy interests if lost or destroyed.
- All authorized users accessing sensitive digital data remotely must do so in accordance with our departmental policy, [Administrative Computer Networks, Hardware, and Software](#) sub section Account Management and Privileged Access.
- All employees shall also, based on risk, implement appropriate technical safeguards necessary to protect the security of sensitive digital data during electronic communications or transmissions.
- All employees shall discard electronic media and hard copy files (e.g. disks, tapes, hard drives, facsimile pages, computer printouts, etc.) containing sensitive data as follows:
 1. In a manner that protects the confidentiality of the sensitive data and renders it unrecoverable by overwriting or modifying the electronic media to make it unreadable or indecipherable or physically destroying the electronic media and hard copy files; and
 2. In accordance with our records retention schedule (contact our [Utilities Personnel Rep](#) for more information on our retention schedule).

- All employees shall report promptly unauthorized or inappropriate disclosure of sensitive data to their supervisors, the University's Information Security Officer (via security@utexas.edu or 512-475-9242); and/or the University's Compliance Hotline (via helpline@compliance.utexas.edu or 1-877-888-0002).

For help with implementing security safeguards on your university and personal computer or portable computing devices please visit [BevoWare](#) to download anti-virus and system security software or contact [TRecs](#) at 512-232-3474.

- **Personal Security**

- All unoccupied offices should be kept locked when practical.
- Personal belongings and any equipment the employee is responsible for (such as purses, briefcases, and tools) should be secured whenever the employee leaves the office or work area.
- Any suspicious-looking strangers should be reported to the University Police Department immediately.
- It's recommended that employees carry their identification cards so that they can present it when needed.

- **Other Related Resources***

- [Confidential Information or CAT-I Data](#)
- [University Acceptable Use Policy](#)
- [Information Resources Use and Security Policy](#)
- [Texas Administrative Code 202](#)
- [UT System UTS-165](#)
- [TRecs Security Information and Helpful Links](#)

** This departmental policy serves as a supplement to the above mentioned security policies.*