Data Storage and Disposal Standard

Objective

In accordance with the Information Security and Acceptable Use Policy, any University Data must be handled in accordance with UTD rules for records retention and minimum security standards during the entire lifecycle of acquisition, storage, and eventual destruction (if applicable).

Electronic vs. Paper Storage

The Information Security Office recommends storing records in electronic format when possible and cost-effective. (For example, the original paper files may be required for some types of documents, or there may be such a volume of stored documents that scanning them is cost-prohibitive.) Electronic storage typically facilitates backups and allows for audit logging; electronic storage is less susceptible to fire, flood, or other factors that are likely to destroy a single paper record.

Paper Records

Paper records containing Confidential or Controlled Data must be stored in an access-controlled drawer, cabinet, or room with adequate protection against theft, fire, and flooding. Paper records must be shredded when no longer needed or required. The Information Security Office recommends a cross-cut shredder that yields a shred size of no larger than ½ inch squares. Locked “shred” bins are also acceptable, provided that keys to access such bins are limited to the shredding vendor and authorized personnel only.

University Information Systems

Electronic records containing Confidential or Controlled Data must be stored in systems that meet the minimum security standards for servers and applications. Records must be removed when no longer needed to reduce security exposure and cost of storage. When an information system or electronic media is no longer needed or required for University use or will be reused for another purpose, the previous data must be destroyed using tools for securely erasing and overwriting data. Such tools are required to meet specific standards for data erasure (such as Department of Defense standard 5220.22-M).

Disposal of hard disk drives must be tracked and logged. Minimum requirements may include:

- Time and date of disposal
- Personnel who performed the disposal
- Description of electronic media or information system that was disposed
- Reasons for disposal of electronic media or information systems

Personally-Owned Equipment

Electronic records stored on personally-owned equipment should be moved to University Information Systems as soon as feasible. When personally-owned computing equipment containing Confidential or Controlled information is retired, all data must be completely removed using tools for securely erasing and overwriting data. Optionally, individuals may bring personally-owned hard drives to the Information Security Office's periodic shredding events.

Records Retention

Data Owners are responsible for understanding the records retention schedule applicable to data under their control, including both retention and destruction schedules. Data should not be kept longer than specified by applicable records retention requirements, unless required by litigation hold or similar preservation requirement. When no longer needed or required, the data should be destroyed according to procedures developed by the Records Retention Office.

Exemptions

In the event that compliance with this data storage and disposal standard cannot be met, please contact infosecurity@utdallas.edu to submit an exemption request which will be approved or denied by the CISO. Denied exemption requests may be appealed to the UTD President for final decision.