Information Security Office

Policies

The purpose of policies is to provide guidelines for network users regarding appropriate behavior and use of networking and computing resources at UTD. The policies adopted by UTD have been designed to provide a secure working environment while allowing users the greatest freedom possible in their academic pursuits.

These policies cover a wide range of topics, from acceptable computer use to proper password procedures to acceptable incidental use of computing resources. Each policy is carefully designed to provide a safe and secure environment for all users while allowing the freedom of use that universities have provided traditionally

If you have questions about any policy or would like to clarify a policy issue, or if you would like to suggest a new policy or a change in an existing policy, please contact the Information Security Office.

- Computer Software Copyright
- Digital Millenium Copyright Act
- Encryption Policy
- Information Resources Acceptable Use Policy (Requires Adobe Reader)
- Information Resources Use and Security Policy (Requires Adobe Reader)
- Network Connection Policy (Requires Adobe Reader)
- Security Practice Bulletin #1 (SPB-1) (Requires Adobe Reader)
- SPB-1 Frequently Asked Questions(Requires Adobe Reader)
- Server Management Policy
- State and Federal Laws
- University E-mail Policy (Requires Adobe Reader)
- University Privacy Policy

Guidelines, Manuals, Procedures, Standards & Forms

- Data Classification Standards (Requires Adobe Reader)
- Extended List of Category I Data (Requires Adobe Reader)
- Information Resources Security Operations Manual (Requires Adobe Reader)
- Minimum Security Standards for Systems Associated with Category I, II or III Data (Requires Adobe Reader)
- Security Exception Reporting Process (Requires Adobe Reader)

- Obtaining an External IP Address for a Web Server

- Report an Incident (Requires Adobe Reader)