Overview

To assure that appropriate attention is paid to those resources that would cause the most damage if they were compromised, it is necessary to perform a risk analysis of resources available on the University network. This analysis should categorize risks of nil, low, medium and high (or 0, 1, 2, and 3) to important available resources.

UTHSC information is categorized into four main classifications given below.

Classification	Example Resource Information
1. Public	Information declared public by a person with appropriate authority.
2. Internal-Use	General corporate information, phone directories, etc.
3. Confidential	Business, financial, technical, most personnel information, etc.
4. Mission Critical	Student information, private personnel information, research and technical information important to the success of the University, third party confidential information, information protected by contractual agreements (ex. non-disclosure agreements) or by regulatory mandates, health/subject/patient information, customer information, donor lists, other information required for the University to do business, etc.

Public information is, and can freely be given to anyone without damage to UTHSC. If an employee is uncertain of the sensitivity of a particular piece of information, they should contact their manager.

Results of risk analysis will allow identification of critical resources that must be protected. The policies listed in this document are intended to help provide protection to these resources.

Purpose

This policy covers requirements for securing sensitive information classified as confidential, and/or as mission critical data, its protection, its risk assessment, its access, its integrity, and its physical and logical protection.

Scope

This policy applies to all persons authorized to access sensitive information classified as confidential, or mission critical data. This is most likely to include but is not limited to University administrative data, correspondence and other sensitive administrative information, confidential student information, alumni data, research data, teaching and evaluation data, and patient data. Classification of data/information is not automatic and is the prerogative and the responsibility of the owner or the custodian of the data/information. For the purpose of this policy it is assumed that Protected Health Information is mandated by the HIPAA Security Rule and qualifies as mission critical information.

This policy applies to data stored on workstations and desktop machines and portable computers as well as local and central servers.

Definitions

Protected Information (PI): Confidential and/or mission critical information or data.

Policy

- It is against University policy for anyone to access or attempt to access a confidential or a mission critical information resource unless they have a documented need to know.

- Areas used to house resources supporting critical applications must be protected by physical security appropriate to the sensitivity of the data applications. Physical access to sites utilizing mission critical information shall be restricted to authorized personnel. Authorized visitors shall be supervised and their entry and exit shall be logged.

- Assure appropriate physical safeguards and security based on the risk level of information accessed. These safeguards include associated workstation environments to restrict access and view to authorized personnel only.

- For electronic systems containing and/or accessing mission critical resources, electronic access shall generate an audit trail that shall be logged. This includes time stamps, by whom accessed, from what source, for how long, what applications and sections were accessed etc. Modifications of the resource including data additions, deletions and/or other modification should be logged. Audit trails should be captured by applications and by operating systems. Periodic reviews of audit trails shall be done by data owners and by system administrators.

- For electronic systems containing and/or accessing mission critical resources, all users must be assigned unique user identifiers for the purpose of identifying and tracking user identity.

- For electronic systems containing and/or accessing mission critical resources, electronic access shall be terminated after a specified time of inactivity.

- While the use of secure (password) screen savers should be installed and used on all workstations, they are required on all stations that contain or have access to confidential and/or mission critical information.

- Unauthorized access and/or unauthorized attempts to access devices containing confidential or mission critical information must be investigated rigorously by data owners, custodian(s), and/or system administrators. Such incidents shall be documented and reported to the appropriate executive. **(Reference Incident Response Addendum** with its **Root Cause Analysis Guidelines)**

- NO ACCESS to confidential or mission critical information will be allowed from off campus EXCEPT by APPROVED VPN access. This explicitly forbids the use of end user installed modems, wireless access points, or other remote access solutions connected to a network containing mission critical, confidential, or internal use data/information.

- Passwords for access to critical resources must be tested for strength and shall be monitored for change frequency, expiration, excessive incorrect attempts in a row, etc. (Reference **Password Addendum)**

- For computers containing confidential or mission critical information, an approved backup and restore plan and procedures must be documented and routinely implemented. Initial testing of backup restoration shall be performed. Additional backup and restoration tests shall be run periodically followed by revision of the plan, if indicated. (Reference **Backup Addendum**)

- For computers containing sensitive information, all confidential or mission critical data transmission shall be encrypted.

Enforcement

Reference **Enforcement** section of Acceptable Use document.

Additional Information

Any inquiries relating to this Mission Critical Information Addendum should be directed to the Security Director.