1. BACKGROUND
This Data Storage Guide provides governance for the use of information storage facilities available to the University of Tennessee Chattanooga (UTC) students, faculty, staff, and other constituents. Given the multiple storage options, the potential for leakage of sensitive information is a significant concern. This document outlines best practices for storing information with assurances that work-related data is properly secured, yet available and recoverable in the event of disk failure or file corruption.

2. PURPOSE
This Data Storage Guide presents best practices for storing data in order to assure information confidentiality, integrity and availability.

3. SCOPE
This Guide applies to all UTC faculty, staff, students and other constituents with access to information storage devices.

4. RESPONSIBILITY
UTC is responsible for managing network university storage facilities which includes daily backups, securing access, and monitoring department use. Access and use of network storage facilities establishes an obligation on the part of the individual to use these storage resources responsibly. Network data storage is intended to facilitate secure document collaboration; it is not intended to archive large amounts of non-critical or personal data. Files that are required for long-term storage may be preserved through archival procedures described below.

Students, faculty, staff and other constituents are responsible for reading and understanding this Data Storage Guide and understanding UTC practices for storing information.

5. STORAGE GUIDELINES
In order to ensure the campus network and personal storage is used efficiently UTC must first determine the criticality and sensitivity of information being stored by those systems. This is done through the Security Categorization process. The Security Categorization process is a standard based on determining the security priorities for the UTC’s information systems. UT Policy IT0115 requires the University to classify information systems within the potential impact categories of: low-impact, moderate-impact, or high-impact for three security objectives: confidentiality, integrity, and availability.

5.1 INFORMATION SECURITY OBJECTIVES address industry recognized security concerns for access, modification and accessibility of information resources:

5.1.1 Confidentiality: Preserving authorized restrictions of information access, including means for protecting personal privacy and proprietary information.

5.1.2 Integrity: Guarding against improper modification or destruction and includes ensuring information non-repudiation and authenticity.

5.1.3 Availability: Ensuring timely and reliable access to information.

5.2 CATEGORIZATION OF ELECTRONIC INFORMATION. There are two (2) categories of information: Unclassified and Classified.
5.2.1 **Unclassified-Public:** Any type of information or information system that has no direct impact on the confidentiality, integrity or availability of the information or on the university as a whole is categorized as “Public.” Public information is not applicable to data storage classification or subject to security controls. Examples:
- Information directly posted to a web page
- Newsletters
- Educational/Training material created for public use

5.2.2 **Classified Information:** Should there be a breach in security there are three potential levels of impact that could affect UTC as a whole:

5.2.2.1 **LOW:** The loss of confidentiality, integrity or availability of low-impact classified data is expected to have a **limited adverse effect** on UTC operations, organizational assets, or individuals involved with the university.

5.2.2.2 **MEDIUM:** The loss of confidentiality, integrity, or availability of moderate-impact classified data is expected to have a **serious adverse effect** on UTC operations, organizational assets, or individuals involved with the university. Moderate-impact classified information is restricted and/or confidential and requires special treatment prior to any release. Moderate-impact information must not be made available for public access unless disclosure is permitted with the consent of the information’s custodian or university-recognized management. Some Moderate-impact information may require prior consent from legal counsel if improper disclosure could result in legal liability along with considerable expense and significant real and/or perceived damage to the university. Examples include:
- Legally restricted electronic protected health information (ePHI) (e.g., insurance billing containing patient medical records)
- Health or clinical information (e.g., Health Insurance Portability and Accountability Act [HIPAA] clinical data)
- Research information/data (e.g., research data containing personally identifiable information)
- Student information (e.g., student records that contain personally identifiable information)
- Human resources information (e.g., personal data, disciplinary information, personally identifiable information)
- Financial information/data (e.g., personal financial data),
- Litigation documents (e.g., information concerning pending litigation or settlement information required to be kept confidential)

5.2.2.3 **HIGH:** The loss of confidentiality, integrity, or availability of high-impact classified data is expected to have a **severe or catastrophic adverse effect** on UTC operations, organizational assets, or individuals involved with the university as a whole. High-impact information is restricted by the United States Government—or otherwise restricted by an agreement between the university and the United States Government. Access is permitted only upon receipt of authorization from the proper U. S. and/or university authorities. High-impact classification includes, but is not limited to, all information determined to have an impact on national security. Examples include information that is declared top secret, secret, or confidential by the government or that might affect national security and research information for the government.

5.2.2.4 **Classification Special Note:** All information and information systems used and processed through the university fall into one of the categories for the security objective types and potential impact levels. **Information systems meeting the criteria of multiple classification levels must protect the highest level of information on the system or a detailed plan must be provided stating a clear separation of data and the protections for each classification of data on the system.**
<table>
<thead>
<tr>
<th>OBJECTIVE</th>
<th>IMPACT</th>
</tr>
</thead>
</table>
| **Confidentiality** Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. | The unauthorized disclosure of information expected to have a **limited adverse effect** on UTC operations, assets, or individuals. Examples:  
- System Administration Access Systems  
- Directory Services Data  
- Accounts Payable  
- Accounts Receivable  
- Building Access Logs  
- Building Alarm and Lock systems  
- Grades  
- Contingency Plans  
- External Reporting Data  
- Database Records for Computer System Maintenance  
- Intellectual Property  
- Policies and Procedures  
- Voice Over IP  
- Research Information/ Data  
- HR Documentation  
- Financial Transaction Information/ Data  
- Video Monitoring Systems  
- Routine Administrative Information/ Data  
- Industrial Control Systems  
- Emergency Notification or Support Systems  
- Telephone Systems  
- Payroll  
- Student Course Data  
  - Blackboard or Submitted Assignments  
- Student Registration Systems  
- Student Scholarship Information  
- Research Grant Information | The unauthorized disclosure of information expected to have a **serious adverse effect** on UTC operations, assets, or individuals. Examples:  
- Legally Protected Data:  
  - Insurance billing containing Patient Medical Records  
  - Legally protected research information/ data  
    - Data containing personally identifiable information  
  - Legally protected student information  
  - Legally protected human resources information  
  - Legally protected financial information/ data  
  - Litigation documents  
- Personal Information  
  - Social security numbers  
  - Credit card information  
- Other types of information governed by industry or legal compliance  
- Point of Sales Systems  
- Messaging Systems  
- Research Grant Information | The unauthorized disclosure of information expected to have a **severe or catastrophic adverse effect** on UTC operations, assets, or individuals. Examples:  
- Contracts  
- Department of Defense Standards  
- Department of Education Standards  
- Investigative Information |

**Special Note:** All high impact levels are based on standards from governmental regulations and the proper controls are implemented through national standards.

| **Integrity** Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. | The unauthorized modification or destruction of information expected to have a **limited adverse effect** on UTC operations, organizational assets, or individuals. Examples:  
- Directory Services Data  
- Industrial Control Systems  
- Websites  
- Accounts Receivable  
- HR Documentation  
- Messaging Systems  
- Telephone Systems | The unauthorized modification or destruction of information expected to have a **serious adverse effect** on UTC operations, organizational assets, or individuals. Examples:  
- Accounts Payable  
- Investigative Information  
- Grades  
- External Reporting Data  
- Sensitive Contract Information  
- Research Data  
- Financial Transaction Data | The unauthorized modification or destruction of information expected to have a **severe or catastrophic adverse effect** on UTC operations, organizational assets, or individuals. Examples:  
- Contracts  
- Department of Defense Standards  
- Department of Education Standards |
### Availability
Ensuring timely and reliable access to and use of information.

<table>
<thead>
<tr>
<th>The <strong>disruption of access</strong> to or use of information <strong>expected to have a limited adverse effect</strong> on UTC operations, assets, or individuals.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Examples:</td>
</tr>
<tr>
<td>Policies and Procedures</td>
</tr>
<tr>
<td>Directory Services Data</td>
</tr>
<tr>
<td>Accounts Payable</td>
</tr>
<tr>
<td>Accounts Receivable</td>
</tr>
<tr>
<td>Research Data</td>
</tr>
<tr>
<td>Grades</td>
</tr>
<tr>
<td>Financial Transaction Data</td>
</tr>
<tr>
<td>Building Access Logs</td>
</tr>
<tr>
<td>Patient Treatment Records</td>
</tr>
<tr>
<td>HR Documentation</td>
</tr>
<tr>
<td>Directory Services Data</td>
</tr>
<tr>
<td>Voice over IP</td>
</tr>
<tr>
<td>Video Monitoring Systems</td>
</tr>
<tr>
<td>Telephone Systems</td>
</tr>
<tr>
<td>Payroll</td>
</tr>
<tr>
<td>Messaging Systems</td>
</tr>
<tr>
<td>Student Scholarship Information</td>
</tr>
<tr>
<td>System Administration Access Systems</td>
</tr>
<tr>
<td>Research Grant Information</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>The <strong>disruption of access</strong> to or use of information <strong>expected to have a serious adverse effect</strong> on UTC operations, assets, or individuals.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Examples:</td>
</tr>
<tr>
<td>Point of Sale Systems</td>
</tr>
<tr>
<td>Industrial Control Systems</td>
</tr>
<tr>
<td>Student Registration Systems</td>
</tr>
<tr>
<td>Student Course Data</td>
</tr>
<tr>
<td>Blackboard or Submitted Assignments</td>
</tr>
<tr>
<td>External Reporting Data</td>
</tr>
<tr>
<td>Building Alarm and Lock systems</td>
</tr>
<tr>
<td>Messaging Systems</td>
</tr>
<tr>
<td>Telephone Systems</td>
</tr>
<tr>
<td>Building Alarm and Lock systems</td>
</tr>
<tr>
<td>Emergency Notification or Support Systems</td>
</tr>
<tr>
<td>Websites</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>The disruption of access to or use of information <strong>expected to have a severe or catastrophic adverse effect</strong> on UTC operations, assets, or individuals.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Examples:</td>
</tr>
<tr>
<td>Contracts</td>
</tr>
<tr>
<td>Department of Defense standards</td>
</tr>
<tr>
<td>Department of Education standards</td>
</tr>
</tbody>
</table>

5.3 **NETWORK STORAGE** are campus network storage resources backed up by UTC Information Technology division (P:, S:, and O: Drives, SharePoint, SecureShare).

5.3.1 **P: Drive (Work-related Private)** – Store official UTC business (work-related) data that is private and not intended to be shared with co-workers on the P: drive. Store Unclassified (i.e. Public) information or Low-impact and Moderate-impact classified data. **Special Note:** Use and storage of Moderate-impact compliance regulated data (FERPA, SSN, HIPAA PII) must be approved by UTC management, used for business purposes only and stored on the P: drive for the minimum time necessary to complete tasks. When tasks with sensitive data are completed, move appropriate files to the SecureShare archive and delete files with sensitive information from your private (P: ) drive. Never store personal or payment card information (PCI, credit card) on the P: drive.

5.3.2 **Mapped Network Share Drives (Work-related Shares) and SharePoint** – Typical mapped drives are O:, S:, etc. With approval from UTC management, work-related Unclassified-Public data or data classified as Low-impact or Moderate-impact can be stored on a shareable mapped drive. Use and storage of Moderate-impact compliance-regulated data (FERPA, SSN, HIPAA PII) must be approved by UTC management, used for business purposes only, and stored on the shared drive or in SharePoint for the minimum time necessary to complete tasks. When tasks with
Sensitive data are completed, move appropriate files to the SecureShare archive and delete files with sensitive information from the network share. Never store personal or payment card information (PCI, credit card) on a UTC storage device or in SharePoint.

5.3.3 **SecureShare (Sensitive Data Archive)** – Work-related data that is classified as Moderate-impact and subject to regulation must be archived to the SecureShare. Use of the SecureShare archival storage requires Department head approval as required for business purposes only.

5.4 **Vendor-provided Cloud-based Storage and Backup**

5.4.1 **UTC Contract with Cloud Vendor**: (Google Apps for Education, Microsoft 365 for EDU).

5.4.1.1 With prior UTC management approval you may store unclassified Public, personal and Low-impact work-related data on storage provided by Google via Google Apps for Education storage, and by Microsoft via Office365. Do not store compliance-regulated data (FERPA with PII, SSN, HIPAA, etc.) on cloud storage.

5.4.2 **Cloud Vendor with no UTC Contract**: (DropBox, iCloud, personal Google/Microsoft Storage, etc.)

5.4.2.1 You may store unclassified Public work-related information and personal data on storage provided by cloud storage vendors. Do not store Moderate-impact data on cloud storage.

5.5 **Local Storage** (C: drive and portable storage).

5.5.1 **C: Drive**: (Temporary Storage). The computer’s local storage (C: drive, hard disk and portable storage) is not backed-up by UTC’s IT department. The computer local hard disk is intended for temporary use during work-related tasks and not permanent storage. Categorization of data can be unclassified Public, Low-impact, or Moderate-impact information. When working with Low-impact and Moderate-impact information the local system it is to be used for the minimum time necessary to complete tasks, then the appropriate information is transferred to the SecureShare for archiving and deleted from local system. Never store personal or payment card information (PCI, credit card) on a local storage device.

5.5.2 **Portable Storage (USB drives)** - Store only Public and Personal information on portable storage devices. Please note that this storage is not backed up by IT services.

6. **GENERAL FILE MANAGEMENT BEST PRACTICES**

Individuals and departments with access to shared drives should employ the following management practices:

6.1 Control access to your data. When you leave your computer unattended sign out or lock your computer such that it requires login credentials in order to use the computer again.

6.2 Do not store personal information (photos, documents, etc.) on UTC storage resources; use only personal portable devices (for example, a flash drive or portable hard disk).

6.3 Do not store copies of sensitive data on laptops, desktops, smartphones, or portable devices (e.g., USB drives).

6.4 Move any sensitive data no longer being used from local systems and network drives to the SecureShare archive. Routinely delete old, duplicate and unnecessary files (for example once a week or month).

6.5 University-related high-resolution images, video files, and audio files are subject to storage device quotas. The following data is not to be stored on any shared drives:

- Personal, non-work-related information of any kind, for example: personal photos, videos or music.
- Excessive iterations (duplicates) of the same document
- Executable (.exe) files.

6.6 Do not access content containing sensitive information via unsecured mobile devices.

6.7 Do not share the following information through email:

- Social Security numbers
- Passwords
- Credit card numbers
- Bank account numbers
- Driver's license numbers
- Names, addresses, and phone numbers in conjunction with other personal data
- Health, financial, and student educational record information

### 7. COMPLIANCE

Failure to comply with the necessary guidelines may result in the use of Disk Quotas. Disk Quotas will restrict the amount of space any one department can use. Quotas are implemented to allow fair sharing of resources. IT will take the necessary action to protect the stability and performance of its services for all individuals.

<table>
<thead>
<tr>
<th>INFORMATION TYPE</th>
<th>NETWORK STORAGE (UTC IT Provides Backup)</th>
<th>CLOUD STORAGE (Vendor Provides Backup)</th>
<th>LOCAL STORAGE (You Provide Backup)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>P:</td>
<td>S:</td>
<td>O:</td>
</tr>
<tr>
<td>Unclassified-Public: Not subject to Security Controls. See Note (1)</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Personal files (photos, etc.)</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
</tr>
<tr>
<td>LOW-impact See Note (2)</td>
<td>✔️ (2)</td>
<td>✔️ (2)</td>
<td>✔️ (2)</td>
</tr>
<tr>
<td>Work-related Private data not shared with co-workers</td>
<td>✔️ (2)</td>
<td>❌</td>
<td>❌</td>
</tr>
<tr>
<td>MODERATE-impact See Notes (3, 4, 5 &amp; 6)</td>
<td>✔️ (3)</td>
<td>✔️ (3)</td>
<td>✔️ (3)</td>
</tr>
<tr>
<td>FERPA PII data</td>
<td>✔️ (4)</td>
<td>✔️ (4)</td>
<td>✔️ (4)</td>
</tr>
<tr>
<td>Archive of Restricted Data</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
</tr>
<tr>
<td>PCI data</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
</tr>
<tr>
<td>HIGH-impact See Note (7)</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
</tr>
</tbody>
</table>
1. **Unclassified-Public information** is not applicable to security controls and it is acceptable for general public access. Public information can be accessed at will by any entity, has no legal guidelines, and presents no perceived risk to the university. Public documents are explicitly classified as such by the information custodian. Examples include information directly posted to a web page; cafeteria menus; newsletters; newsgroup transfers; educational or training material created for public use; public listservs. Personal data should be stored on personal devices or personal cloud storage.

2. **LOW-impact information** may not be made available for general public access. However, disclosure is permitted with the consent of the information’s custodian or university-recognized management. For information classified as Low-impact, a security breach is expected to have a *limited adverse effect* on UTC operations, assets, or individuals involved with the university as a whole. Low-impact data does not contain sensitive data (FERPA with PII, SSN, HIPAA, etc.). Low-impact information can be shared with other departments that have been given rights to access Department XYZ data. All work-related, private Low-impact data should be moved to the P: drive as soon as possible so that it can be backed-up by UTC IT.

3. **MODERATE-impact information** is restricted or confidential information and requires special treatment prior to any release. Moderate-impact classified information must not be made available for general public or other access without proper prior consent from UTC-recognized management and. Improper disclosure could result in legal liability along with considerable expense and significant real and/or perceived damage to the university. For information classified as Moderate-impact, a security breach is expected to have a *serious adverse effect* on UTC operations, assets, or individuals involved with the university as a whole. Use Moderate-impact information as required for business purposes only and for the minimum time necessary to complete tasks. Confidential data is then transferred to Archive and deleted from local system.

4. Use of FERPA-related information is required for business purposes only and for the minimum time necessary to complete tasks. FERPA-related data is then transferred to SecureShare archive and deleted from local system.

5. Use of SSN is required for business purposes only and for the minimum time necessary to complete tasks. Information with SSN is then transferred to SecureShare archive and deleted from local system.

6. Use of HIPAA-related information is required for business purposes only and for the minimum time necessary to complete tasks. HIPAA data is then deleted from local system.

7. **HIGH-impact information** is restricted by the United States Government—or otherwise restricted by an agreement between UTC and the United States Government. Access is permitted only upon receipt of authorization from the proper U.S. and/or university authorities. For information classified as High-impact, a security breach is expected to have a severe or catastrophic adverse effect on UTC operations, assets, or individuals involved with the university as a whole. High-impact information classification includes, but is not limited to, all information determined to have an impact on national security. Examples include information that is declared top secret, secret, or confidential by the government or that might affect national security and research information for the government.

---

**APPROVALS**

---

![Signature]

Tom Hoover
Associate Vice-Chancellor & CIO

![Signature]

Michael Dinkins, CISSP
Senior Information Security Officer

Date

8/12/14

Date

8/11/2014