Information Security Policy

General Description

**Purpose:**
The University expects all stewards of its Non-Public Information to create, access, share, and utilize the information in a manner that is consistent with the University's need for security and confidentiality. All University faculty, staff, students, vendors, and contractors who have access to University Non-Public Information are required to maintain and manage it in accordance with this policy regarding the storage, disclosure, access, and classification of such information. They are required to ensure that all contractors, vendors, and other parties with whom they work also comply with this policy.

The Information Security Policy (the “Policy”) is Trinity University’s written information security policy mandated by the Federal Trade Commission’s Safeguards Rule, the Gramm – Leach – Bliley Act (“GLBA”), and the Family Educational Rights and Privacy Act (“FERPA”). In particular, this document describes the policy elements pursuant to which the University intends to (i) ensure the security and confidentiality of covered information, (ii) protect against any anticipated threats or hazards to the security of such information, and (iii) respond to information security breaches should they occur.

**Scope:**
The Information Security Policy applies to any Non-Public Information, whether in paper, digital, or other format, that is handled or maintained by or on behalf of the University or its affiliates.

Policy Content

The University’s ITS Security Administrator shall be responsible for coordinating and enforcing the Policy. The ITS Security Administrator may designate other representatives of the University to manage particular elements of the Policy. Any questions regarding the implementation or interpretation of the Policy should be directed to the ITS Security Administrator.

- **Public Information**
  - A. Access
    Public Information has been made available or published explicitly for the general public and does not have access restrictions.
  
  - B. Use
    There are no restrictions on use for Public Information except that it may not be used for personal gain.
  
  - C. Storage
There are no restrictions on storage of Public Information.

D. Transfer
There are no restrictions on transfer of Public Information.

E. Retention & Disposal
Retention and disposal of Public Information will be determined by the responsible department. Please see the Trinity University Records Retention Policy.

● Protected Information

A. Access
Access must be limited to Authorized Users.

B. Use Protected
Information may only be used by Authorized Users to fulfill University job responsibilities for a legitimate purpose and may not be used for personal gain.

C. Storage

1. Device Storage
   a) Trinity Devices
   Protected Information may be stored on Trinity-owned devices, such as computers, tablets, hard drives, and University-issued mobile phones as long as precautions are taken to protect it from unauthorized access, such as:
      - Creating strong passwords or passcodes for each device
      - Locking each device when not actively using it
      - Never leaving a device unattended in a public or unlocked space
      - Never using a public wifi connection while conducting University work, and
      - Remembering to log out of your accounts when not using a system.
   b) Personal Devices
   Personal computing devices such as laptops, hand-held equipment (PDAs) and data storage media pose a significant risk for the exposure of Protected Information and potential access to the University’s administrative systems. For these reasons, and because you will be held personally responsible for security breaches of University information, special care must be exercised when utilizing these devices. Protected Information may be temporarily stored on personal devices if they are owned by Authorized Users and the devices are used to fulfill University job responsibilities. Security precautions must still be taken with personal devices, such as:
- Apply strong passwords or passcodes to every device
- Lock your device with a protected lock screen
- Log off of all sensitive systems when not in use
- Never share your login credentials with others
- Maintain up-to-date software patches and antivirus software
- Never leave your device unattended in a public or unlocked space
- Do not access Protected Information using a public unsecured wifi network

2. Trinity Network Storage
Protected Information may be stored digitally on Trinity-hosted systems, such as the campus network drives, as long as precautions are taken to limit access to Authorized Users.

3. Physical Storage
Protected Information may reside in a physical format (e.g. paper) as long as it is stored on campus in a locked room, desk, cabinet, etc. with access limited to Authorized Users.

4. Cloud Storage
External storage providers (ESP), sometimes referred to as cloud file storage providers (e.g. Google Drive, Dropbox), allow access to files from almost any internet-enabled mobile or desktop computing device. Protected Information may not be stored on or sent through any ESP unless ITS and the Office of Risk Management have explicitly approved the provider for storage of Protected Information.

For a list of authorized external storage providers, please see the ITS Service Catalog. The risk associated with the use of non-approved ESP providers for storing Protected Information is borne solely by the user of such services. In the event of litigation, University data stored on non-approved ESP services must be disclosed by the user to the Security Administrator and will be subject to discovery.

5. Email Storage
Protected Information may be stored in the Tmail (Trinity email) accounts of Authorized Users.

It is important that University employees not forward, send, or receive emails containing Protected Information to or from email accounts other than Tmail. The risk associated with the use of non-approved email providers for storing Protected Information is borne solely by the user of such services. In the event of litigation, University data stored on non-approved email services must be disclosed by the user to the Security Administrator and will be subject to discovery.
The use of non-Trinity email accounts for the storage of Protected Information is prohibited.

D. Transfer
Protected Information may be transferred between Authorized Users, as long as precautions are taken to limit access to Authorized Users. The use of non-Trinity email accounts for the transfer of Protected Information is prohibited.

E. Retention & Disposal
Retention and disposal of Protected Information will be determined by the responsible department. Please see the Trinity University Records Retention Policy.

● Restricted Information

A. Access
Restricted Information concerning individual students or employees may be accessed or released only if such an action has been authorized by the Data Owner.

B. Use
Restricted Information may only be used to fulfill University job responsibilities and may not be used for personal gain. Use of this information must be defensible and tightly controlled.

C. Storage

1. Device Storage
   a) Trinity Devices
   Restricted Information may not be stored on University mobile devices (e.g. phones, tablets, thumb drives, external hard drives). Restricted Information normally should not be stored on any Trinity-owned desktop or laptop. If necessary, Restricted Information may be stored on Trinity-owned desktops and laptops if the information is encrypted with approved encryption software.
   b) Personal Devices
   Restricted Information may not be stored on personally owned devices, including desktops, laptops, phones, or other mobile devices.

2. TUNetwork Storage
   a) The TUNetwork is the preferred location for local storage of digitized Restricted Information.
   b) Servers on which Restricted Information is stored must be centrally managed by Trinity University Information Technology Services. Physical and server administration access to these servers must be limited to Authorized Users with legitimate need.
   c) A Trinity-provided [VPN or VDI connection] may be used to access Restricted
3. Physical Storage
If the Restricted Information is in a physical format, it must be stored in a secured (e.g. locked) cabinet or office and not be able to be accessed by unauthorized persons.

4. Cloud Storage
Restricted Information should not be stored using any cloud file storage provider, e.g. Dropbox, that is not authorized by Trinity University. Users storing Restricted Information on Google Drive are strongly encouraged to employ additional security precautions such as two-factor authentication.

5. Email Storage
In general, users should avoid long-term storage of Restricted Information on Tmail. Users must be aware that although Tmail is encrypted, the security of the information may be compromised by lost or hacked passwords, forwarding of the email to other parties, etc. Users sending Restricted Information through Tmail are strongly encouraged to employ additional security precautions such as two-factor authentication. The use of non-Trinity email accounts for the storage of Restricted Information is prohibited.

Other parties should be discouraged from emailing Restricted Information to Trinity. If it is necessary for Restricted Information to be emailed to Trinity, consult the ITS Security Administrator for appropriately secured methods.

D. Transfer
Transfer of Restricted Information should be limited to only instances when it is absolutely necessary.

For transfers and sharing within the Trinity Community, the preferred method is to use a folder on a Trinity network drive with access restricted to only Authorized Users. If this method is not feasible, the Restricted Information may be sent from one Tmail account to another Tmail account. In this case, the users must be aware that although the emails are encrypted, the security of the information may be compromised by lost or hacked passwords, forwarding of the email to other parties, etc. Users sending Restricted Information through Tmail are strongly encouraged to employ additional security precautions such as two-factor authentication.

The use of non-Trinity email accounts for the transfer of Restricted Information is prohibited.

Restricted Information must be encrypted during transfer with any approved external party. If the information is being transferred via web interface, web traffic must be transmitted
over Secure Sockets Layer (SSL) using only strong security protocols, such as Transport Layer Security (TLS). Remote file transfers should be performed using SFTP or HTTPS file transfer protocols. For questions or concerns about secure information transfer, contact the ITS Security Administrator.

E. Retention & Disposal
Retention and disposal requirements for Restricted Information is often mandated by law. The University must remain in compliance with all mandated timeframes and security measures in regards to the long-term maintenance of Restricted Information. Please see the Trinity University Records Retention Policy.

External Requests for Information

Anyone receiving a request from an external entity (e.g. law enforcement, legal counsel, court order, government agency) for Protected or Restricted Information, must immediately consult the Office of Risk Management. Only upon approval from Risk Management may the information be released.

Requests received from parents for Protected or Restricted student information must be handled in accordance with the Parental Access to Information policy.

Contract Approval

Any contract with vendors or individuals for services dealing with University information must be approved by the Office of Risk Management. Any contracts involving information technology must be approved through the ITS Project Management Office.

Security Administrator Responsibilities

• Provides consultation services to computing and business operations and recommends methods to mitigate security risks.
• Coordinates with the Office of Risk Management on contract approval regarding data distribution and storage of Protected and Restricted information.
• Coordinates the development and implementation of a training and awareness program to educate University employees, contractors, and vendors with regard to the University's security requirements.
• Investigates breaches of security controls and implements additional compensating controls when necessary.
• Reviews and approves all external network connections.
• Manages security incidents and files mandatory reports.
• Is knowledgeable about current laws and regulations that could affect the security controls and classification requirements of the University’s information.

Performance Evaluation

Consequences of Policy Violation:

Enforcement
Any violation of this policy or inappropriate or illegal use of University information is cause for a disciplinary procedure. Violations will be adjudicated, as appropriate, in accordance with University policies. Sanctions due to violations of this policy may result in, but are not limited to, the following:

• Loss of information technology privileges;
• Relevant University judicial sanctions;
• Employees may be subject to disciplinary action up to and including suspension or termination of employment;
• Prosecution under applicable civil or criminal laws by state or federal authorities.

Reporting Violations
Violations or suspected violations of this Policy must be immediately reported to the ITS Security Administrator. The Security Administrator, in collaboration with other appropriate staff, shall determine if a reported incident is or is not a potential violation of the Information Security Policy. If the incident is deemed to be a potential Policy violation, the Security Administrator will refer the issue to the appropriate institutional authority.

Reporting Unauthorized Access
If Protected or Restricted Information stored on a device (e.g. laptop, tablet, external hard drive, thumb drive, CD) or in a physical format (e.g. print out, folder) is lost or stolen, immediately report the incident to the ITS Security Administrator.
If Protected or Restricted Information is found, secure the information and immediately inform the ITS Security Administrator.

Requirements

Approvals:
Chief Information Officer
Terms and Definitions:

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authorized User</td>
<td>Person who is formally and properly empowered to perform specified duties in regards to accessing and using University information. Authorized Users may include University faculty, staff, students, departments, and third party contractors.</td>
</tr>
<tr>
<td>Data Owner</td>
<td>Department or person(s) responsible for security oversight of particular Protected or Restricted Information. Risk Management or the ITS Security Officer may be consulted to determine the Data Owner.</td>
</tr>
<tr>
<td>SSL (Secure Sockets Layer)</td>
<td>the standard security technology for establishing an encrypted link between a web server and a browser. This link ensures that all data passed between the web server and browsers remain private and integral.</td>
</tr>
<tr>
<td>Transport Layer Security (TLS)</td>
<td>and its predecessor, Secure Sockets Layer (SSL) - both frequently referred to as &quot;SSL&quot;, are cryptographic protocols that provide communications security over a computer network.</td>
</tr>
<tr>
<td>Public Information</td>
<td>Information that the University has made available or published for the explicit use of the general public with no restrictions on access, use, or disclosure under University policy or contract, or local, national, or international statute, regulation, or law.</td>
</tr>
<tr>
<td>Non-Public Information</td>
<td>Non-Public Information includes both Protected and Restricted Information.</td>
</tr>
</tbody>
</table>

**Protected Information** - Protected information includes all private data, records, documents, or files that contain information that is not to be shared publicly but also not restricted legally and might be provided upon reasonable request as long as the Data Owner is consulted about its responsible use and approves its release.

**Restricted Information** - Sensitive information that must be safeguarded at the highest priority levels in order to protect the privacy of individuals and the security and integrity of University systems. This information must be limited to authorized University faculty, staff, students, or others with a legitimate need. This information may not be transferred without mandatory security precautions or made vulnerable to unauthorized access, use, or disclosure. Restricted information is categorized as such due to legal protection or privilege, University policy, contract obligation, or important privacy considerations. Restricted Information includes but is not limited to “Sensitive Personal Information” as defined by [Texas S.B. 122 § 48.002.2](https://www.statutes.texas.gov/Legislation/PDF_pages1/2005/2005ch122.pdf) (Identity Theft Enforcement & Protection Act).
Attachments

Securing Information - Data Type Examples
Related Documents

<table>
<thead>
<tr>
<th>Document Type</th>
<th>Document Name</th>
<th>Document Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy</td>
<td>Records Retention</td>
<td>BUSO-0020</td>
</tr>
</tbody>
</table>

Revision Management

<table>
<thead>
<tr>
<th>Revision #:</th>
<th>Date:</th>
<th>Recorded By:</th>
</tr>
</thead>
<tbody>
<tr>
<td>v1.0</td>
<td>8/14/2019 3:48 PM</td>
<td>Courtney Cunningham</td>
</tr>
</tbody>
</table>