Information Security Policy

Document Number: ITS-0013 **Date Published(sys):** 4/27/2022

General Description

Policy Summary:

The policy and applicable supporting documents are designed with the ultimate goal of protecting the sensitive information of our clients, key stakeholders, and members of our communities and to ensure a normal and uninterrupted operation. TU 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 needs for security and confidentiality.

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:

This Information Security Policy applies to all Trinity University (TU) staff, management, executives, faculty, students, vendors, contractors and any other third parties with access to TU's information technology assets and called from hereinafter TU Constituents.

This policy also applies to all Trinity University and its affiliates Information Technology assets

and services storing, processing, or transmitting TU's information classified as non-public.

Exceptions:

In a few instances, Trinity systems may require to be exempted from the Information Security Program due to possible technical difficulties or third-party contractual obligations. Any such exceptions to the current policy must be documented and approved via Trinity's Exceptions Management Process.

Policy Content

① Roles and Responsibilities

Implementing and adhering to organizational policies and procedures is a collaborative effort, requiring a true commitment from all TU Constituents. Additionally, by being aware of one's roles and responsibilities as it pertains to Trinity University information systems, all relevant parties are helping promote the Confidentiality, Integrity, and Availability (CIA) principles for information security in today's world of growing cybersecurity challenges.

Role	Responsibility
Management Commitment	Responsibilities include providing overall direction, guidance, leadership, and support for the entire information security program, while also assisting other applicable personnel in their day-to-day operations. The CIO is to report to other members of senior management on a regular basis regarding all aspects of the organization's information systems posture.
Internal Employees and Users	Responsibilities include adhering to the organization's information security policies, procedures, practices, and not undertaking any measure to alter such standards on any Trinity University system components. Additionally, end users are to report instances of non-compliance to senior authorities, specifically those by other users. End users, while undertaking day-to-day operations, may also notice issues that could impede the safety and security of Trinity University system components and data, and are to also report such instance immediately to senior authorities.
Vendors, Contractors, Workforce	Responsibilities for such individuals and organizations are much like those stated for end users: adhering to the organization's information security policies, procedures, practices, and not undertaking any measure to alter such

	standards on any such system components.
Security Administrator	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 regarding 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
Information Security Governance Committee	The Security Governance Committee provides leadership in the protection of Trinity University's information assets, data, and technology, as well as managing information risks to be under acceptable levels. The Committee is responsible for overseeing the development of the University's Information Security Program, policies, initiatives, and projects, and ensuring these are aligned with and supportive of the University's strategic goals.
Incident Response Team	Protecting the overall computing infrastructure of Trinity University, the IRT is responsible for responding quickly to identified threats to the data infrastructure, assess the level of risk, and take immediate steps to mitigate risks considered significant and harmful to the integrity of Trinity University information system resources. IRT members notify the appropriate department leads of any incident involving their resources.
Human Resources	Responsible for the overall implementation and management of personnel security controls across Trinity University. As information security programs are developed, the Human Resources Department will ensure coordination of the information security programs developed. They serve as the senior officials responsible for: Developing, promulgating, implementing, and monitoring the organization's personnel security programs; Developing and implementing position

	categorization (including third-party controls), access agreements, and personnel screening, termination, and transfers; and; Ensuring consistent and appropriate sanctions for personnel violating management, operation, or technical information security controls.
Department Managers	Assume primary compliance responsibility for the IT resources under their control. Thoroughly understand the security risks impacting University information under their control. Security risks should be documented and reviewed with the appropriate data steward so that he or she can determine whether greater resources need to be devoted to mitigating these risks. ITS Core Infrastructure Team can assist Department Managers with gaining a better understanding of their security risks. Ensure the implementation of reasonable and appropriate security controls to protect the confidentiality, integrity, and availability of IT resources within their units. Approve exceptions to this policy based on operational or technical needs.
ITS Organization	Maintains overview responsibility for implementation of this policy. Establish policy requirements, including security standards and controls, and monitor and enforce compliance. Develops a comprehensive security program that includes risk assessments, best practices, education, and training. Having IT assume this responsibility does not abrogate the responsibility of individuals and units to comply with policy requirements. Train and educate the Trinity University community on this policy. Monitors technological developments, trends, and changes in laws and regulations and update this policy as appropriate. Conduct annual reviews of minimum technical requirements and update this policy, with appropriate review. Assists units in understanding risk and in identifying and implementing security controls to protect IT resources. Issues critical security notices to units. Develops, implements, and maintains University-level security monitoring and analysis.
Chief Information Security Officer - CISO	Responsible for university-wide efforts related to data and information system security, such as the development of Trinity University data security policies, negotiation, and evaluation of site licenses for security-related software, training, coordination of efforts to improve data security controls, and dissemination of security-related information and incidents, which could affect the availability, and integrity

	of computing resources on campus. Issue the Information Security policies and guidance that establish a framework for an Information Security Management System (ISMS). Identify protection goals, objectives, and metrics consistent with Trinity University strategic plan. Ensure appropriate procedures are in place for Security Testing and monitors, evaluates, and reports on the status of ITS security.

② Policy

Trinity University has defined and maintains, with the Institution areas, a clear definition of the requirements for information security within the university, in a way that the Information Security Program activities are focused on the fulfillment of those requirements. Statutory, regulatory, and contractual requirements are also documented and considered as input to the planning process. Specific requirements about the security of new or changed systems or services will be captured as part of the design stage of each project.

It is a fundamental principle of the Trinity University Information Security Program that the controls implemented are driven by business needs and this will be regularly communicated to all TU Constituents through team meetings and briefing documents. Trinity University requires all TU Constituents adhere to the following policies for purposes of complying with the mandated organizational security requirements set forth and approved by management:

- Information Security Policy
- Information Security Program
- Information Security Risk
- Password Policy
- Acceptable Use Policy
- TUNetwork Security Policy
- Supplier Management Policy
- Asset Management Policy
- Physical Security Policy
- Social Media Policy
- Internet Privacy
- Device Management Policy
- Anti-Virus Policy
- HR Security Policy
- Copyright Policy
- Data Protection Privacy Notice

- Data Destruction and Media Policy
- Electronic Messaging Policy
- Access Control Policy
- Vulnerability & Patch Management Policy
- Firewall Policy

System Administrators should appropriately configure, examine, and confirm their system's settings and all necessary configurations for system components to ensure that the data stored does not exceed the requirements defined in the data retention policy. They will also enforce security by design in all new technology implemented, and during the technology lifecycle.

The University's ITS Chief Information Security Officer is responsible for coordinating and enforcing the Policy. The ITS Chief Information Security Officer 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 Chief Information Security Officer.

Data Protection

Trinity University Data Classification

Public Information

Public data is information that may be disclosed to any person regardless of their affiliation with the University. The Public classification is not limited to data that is of public interest or intended to be distributed to the public; the classification applies to data that do not require any level of protection from disclosure. While it may be necessary to protect original (source) documents from unauthorized modification, Public data may be shared with a broad audience both within and outside the University community and no steps need be taken to prevent its distribution.
Examples:

- press releases,
- directory information (not subject to a Family Educational Rights and Privacy Act (FERPA) block),
- course catalogs,
- application and request forms,
- information solely related to law enforcement activities in accordance with a Texas Public Information Act obligations,
- and other general information that is openly shared.

- The type of information a department would choose to post on its website is a good example of Public data.

1. **Access**
    1. Public Information has been made available or published explicitly for the general public and does not have access restrictions.
2. **Use**
    1. There are no restrictions on use for Public Information except that it may not be used for personal gain.
3. **Storage**
    1. There are no restrictions on storage of Public Information.
4. **Transfer**
    1. There are no restrictions on transfer of Public Information.
5. **Retention & Disposal**

Retention and disposal of Public Information will be determined by the responsible department. Please see the Trinity University Records Retention Policy (BUSO-0020).

Protected Information

Protected data is information that, if made available to unauthorized parties, may adversely affect individuals or the business of Trinity University. This classification also includes data that the University is required to keep confidential, either by law (e.g., FERPA) or under a confidentiality agreement with a third party, such as a vendor. This information should be protected against unauthorized disclosure or modification. Confidential data should be used only when necessary for business purposes and should be protected both when it is in use and when it is being stored or transported.

Any unauthorized disclosure or loss of Confidential data must be reported to the ITS Chief Information Security Officer. The ITS Chief Information Security Officer will then notify the CIO, and the Incident Response Team once the incident is confirmed or validated.
Examples:

- Information covered by the Family Educational Rights and Privacy Act (FERPA), which requires protection of records for current and former students. This includes pictures and video of students kept for official purposes.
- Personally identifiable information entrusted to our care that is not otherwise categorized as Restricted Use data, such as information

regarding applicants, alumni, donors, potential donors, or parents of current or former students, and information covered by the European Union's General Data Protection Regulation (GDPR).
- The Trinity University ID Number, when stored with other identifiable information such as name or e-mail address.
- Information covered by the Gramm-Leach-Bliley Act (GLB), which requires protection of certain financial records.
- Individual employment information, including salary, benefits, and performance appraisals for current, former, and prospective employees.
- Legally privileged information.
- Information that is the subject of a confidentiality agreement.
- Human subject research data with identifiers limited to dates, city, Zip Code, such as information that is the subject of a HIPAA Limited Data Set covered by a Data Use Agreement.

1. **Access** - Access must be limited to Authorized Users.
2. **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.
3. **Storage**
    1. **Device Storage**
        1. **Trinity Devices** - Protected Information may be stored on Trinity-owned devices, such as computers, tablets, and hard drives, as long as precautions are taken to protect it from unauthorized access, such as:
            - Remembering to log out of your accounts when not using a system.
            - Never leaving a device unattended in a public or unlocked space.
            - Locking each device when not actively using it.
            - Creating strong passwords or passcodes for each device. Please refer to the *ITS-0015 Password Policy* for more details on password management.
        2. **Personal Devices**
            1. 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. Security precautions must still be taken with personal devices, such as:

1. Apply strong passwords or pass codes to every device
2. Lock your device with a protected lock screen
3. Log off of all sensitive systems when not in use
4. Never share your login credentials with others
5. Maintain up-to-date software patches and antivirus software
6. Never leave your device unattended in a public or unlocked space or visible in a locked vehicle
7. Do not access Protected Information using a public unsecured wifi network

2. **Trinity Network Storage**
    1. Protected Information may be stored digitally on Trinity-hosted systems, such as the campus network drives. Precautions should be taken to limit access to Authorized Users.
3. **Physical Storage**
    1. 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**
    1. 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.

2. 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**
    1. Protected Information may be stored in the Tmail (Trinity email) accounts of Authorized Users.
    2. 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.
    3. The use of non-Trinity email accounts for the storage of Protected Information is prohibited.
4. **Transfer**
    1. 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.
5. **Retention & Disposal**
    Retention and disposal of Protected Information will be determined by the responsible department. Please see the Trinity University Records Retention Policy (BUSO-0020).

Restricted Information

Restricted Use data includes any information that the Business Unit has a contractual, legal, or regulatory obligation to safeguard in the most stringent manner. In some cases, unauthorized disclosure or loss of this data would require the University to notify the affected individual and state or federal authorities. In some cases, modification of the data would require informing the affected individual.

The University's obligations will depend on the data and the relevant contract or laws. The Minimum-Security Standards sets a baseline for all Restricted Use

data. Systems and processes protecting the following types of data need to meet that baseline:

- Personally identifiable health information that is not subject to HIPAA but used in research, such as Human Subjects Data.
- Personally Identifiable Information (PII) covered under Texas General Law, including an individual's name plus the individual's Social Security Number, driver's license number, or a financial account number.
- Unencrypted data used to authenticate or authorize individuals to use electronic resources, such as passwords, keys, and other electronic tokens.
- "Criminal Background Data" that might be collected as part of an application form or a background check.

More stringent requirements exist for some types of Restricted Use data. Individuals working with the following types of data must follow the University policies governing those types of data and consult with Information Security to ensure they meet all the requirements of their data type:

- Protected Health Information (PHI) subject to the Health Insurance Portability and Accountability Act (HIPAA).
- Financial account numbers covered by the Payment Card Industry Data Security Standard (PCI-DSS), which controls how credit card information is accepted, used, and stored.
- Controlled Unclassified Information required to be compliant with NIST 800.171
- Data controlled by U.S. Export Control Law such as the International Traffic in Arms Regulations (ITAR) or Export Administration Regulations (EAR). ITAR and EAR have additional requirements.
- U.S. Government Classified Data
- Restricted Use data should be used only when no alternative exists and must be carefully protected. Any unauthorized disclosure or loss of Confidential data must be reported to the ITS Information Security Officer, the CIO, or the Incident Response Team.

1. **Access**
    1. Restricted Information concerning individual students or employees may be accessed or released only if such an action has been authorized by the Data Owner.
2. **Use**
    1. 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.

3. **Storage**
    1. **Device Storage**
        1. Trinity Devices
            1. 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 Personal Devices
            2. Restricted Information may not be stored on personally owned devices, including desktops, laptops, phones, or other mobile devices.
    2. **TUNetwork Storage**
        1. The TUNetwork is the preferred location for local storage of digitized Restricted Information.
        2. 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.
        3. A Trinity-provided VPN or VDI connection may be used to access Restricted data from the TUNetwork while off campus. Do not access Protected Information while connected to a public unsecured wifi network.
    3. **Physical Storage**
        1. 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**
        1. 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**
        1. In general, users should avoid long-term storage of restricted Information on Tmail. Users must be aware that although utilizing email encryption, the security of the information may be compromised by hacked passwords,

forwarding of the email to other parties, etc. Users sending sensitive Information through Tmail are strongly encouraged to employ additional security precautions such as two-factor authentication or email encryption

2. 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.

4. **Transfer**
    1. Transfer of Restricted Information should be limited to only instances when it is absolutely necessary.
    2. 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.
    3. The use of non-Trinity email accounts for the transfer of Restricted Information is prohibited.
    4. 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.
5. **Retention & Disposal**
    1. Retention and disposal requirements for Restricted Information are often mandated by law. The University must remain in compliance with all mandated timeframes and security measures in regard to the long-term maintenance of Restricted Information. Please see the Trinity University Records Retention Policy (BUSO-0020).

Types of Data

Data may be in electronic media or in hardcopy format. The following is a list of where data may reside:

- Electronic Media - Electronic media are the bits and bytes contained in hard drives, Random Access Memory (RAM), Read-Only Memory (ROM), disks, memory devices, phones, mobile computing devices, networking equipment and various other media.
- Hardcopy Format - Hardcopy media are physical representations of information. Paper printouts, printers, facsimile ribbons, drums, and platens are all examples of hardcopy media.
    - Paper receipts or other supporting hardcopy documents and receipts
    - Credit card printouts from processing machines
    - Invoices
    - Purchase orders
    - Offline hardcopy batch printouts
    - Other hardcopy formats as identified by organizations

Obtaining Data

Data must be obtained in a secure manner so as not to compromise the information traversing public networks and internal company-wide networks. Appropriate security-hardening and configuration standards are to be utilized throughout the entire network, which include but are not limited to the following system components: any network component (routers, switches, firewalls, load balancers, etc.), server or application(s) included in or connected to the data environment.

Due diligence must be exercised to ensure that other organizations associated with Trinity University environment also have appropriate security measures, standards, and safeguards in place. This includes but is not limited to the following:

- Data centers and managed service providers
- External vendors wanting to process credit cards are not permitted to use the Trinity University network for processing these and must provide their own wi-fi data hotspot.
- Client websites with ecommerce platforms

Protecting Data

The transmission and subsequent storage of data will be protected at all times. Protecting data includes, but is not limited to any of the following:

- Use of HTTPS for secure transmission
- Use of encryption for storage (disk, file, column encryption)
- Hashing

- Truncating

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 General Counsel. Only upon approval from the University General Counsel 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 reviewed by the Office of Risk Management. Any contracts involving information technology must be approved through the ITS Business Affairs Unit.

Audit Logs Security

Audit logs must be always protected for purposes of ensuring their overall integrity. More specifically, if breaches or other security issues arise, audit logs are often used for helping reconstruct and providing necessary evidence of activities.

Trinity University is to ensure that all applicable users adhere to the following policies for purposes of complying with the mandated organizational security requirements set forth and approved by management:

- Only individuals with a job-related need can view audit trail files.
- Current audit trail files are to be always protected from unauthorized modifications via access control mechanisms, physical segregation and/or network segregation.
- Audit trail files are to be promptly backed up to a centralized log server or media that is difficult to alter.
- Logs for external-facing technologies are to be written onto a secure, centralized, internal log server or media.
- Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts.
- Appropriately configure, examine, and confirm system settings and all necessary configurations for system components to ensure the use of file-integrity monitoring or change-detection software on logs.

Audit Trails and Loggings

- Trinity University verifies that audit trails are enabled and active for system components, and that access to system components is linked to individual users.
- Examination the following audit log settings as listed below will be accomplished:
    - Verify actions taken by any individual with root or administrative privileges are logged.
    - Verify access to all audit trails are logged, including failed attempts as well.
    - Verify invalid logical access attempts are logged.
    - Verify use of changes to identification and authentication mechanisms are logged.
    - Verify all elevations of privileges are logged.
    - Verify all changes, additions, or deletions to any account with root or administrative privileges are logged.
    - Verify initialization, stopping, or pausing of audit logs are logged.
    - Verify creation and deletion of system level objects are logged.
- Record the following events in the logs as listed below:
    - Verify user identification is included in log entries.
    - Verify the type of event is included in log entries.
    - Verify date and time stamp is included in log entries.
    - Verify success or failure indication is included in log entries.
    - Verify the origination of events is included in log entries.
    - Verify the identity or name of affected data, system component, or resources is included in log entries.

Incident Response

Data breaches, cyber security threats, and many other malicious exploits are challenging organizations, ultimately requiring comprehensive security measures for helping ensure the confidentiality, integrity, and availability of one's entire information systems landscape. Unfortunately, security breaches do happen - even with the best controls in place - thus the ability to respond swiftly and effectively is a must for mitigating any further damages. Structured protocol is extremely important for incident response initiatives as it achieves the following:

- Responding immediately with information security best practices.
- Isolating the affected systems as quickly as possible, helping minimize the threat to other critical system resources.
- Helping minimize system downtime, while restoring critical infrastructure to full operational capabilities as quickly as possible.
- Providing a "lessons learned" approach for every incident, regardless of size, scale, complexity, and severity.

Comprehensive incident response measures require participation and involvement from everyone within Trinity University, from senior management all the way down to end-user of systems - along with being aware of the following core components of incident response:

- Incident reporting
- Containment
- Notifications
- Investigation
- Final report/recommendations

Important to follow:

- There should be a breach notification for all HIPAA data breaches.
- The Incident Response plan includes, at a minimum, roles, responsibilities, and communication strategies in the event of a compromise.
- The Incident Response plan includes specific incident response, business recovery and continuity procedures and data backup processes.
- The Incident Response plan includes coverage and response mechanisms for all critical system components and all other IT resources deemed critical by Trinity University.
- The Incident Response Plan is to be tested annually.
- Designated personnel or contracted vendor(s) are available for 24/7 incident response and monitoring coverage for any evidence of unauthorized activity, detection of unauthorized wireless access points, critical Intrusion Detection Systems (IDS) alerts and/or reports of unauthorized critical system or content file changes.
- Staff with responsibilities for security breach responses is periodically trained.
- Monitoring and responding to alerts from security systems including detection of unauthorized wireless access points constitute an important component of the Incident Response plan.
- Processes are in place to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments as needed.

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 action. 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 Violation
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 ITS.
- If Protected or Restricted Information is found, secure the information, and immediately inform ITS.

Terms & Definitions

Terms and Definitions:

Term:	Definition:
Authorized User	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.
Data Owner	Department or person(s) responsible for security oversight of particular Protected or Restricted Information. Risk Management or the ITS Security Administrator may be consulted to determine the Data Owner.
SSL (Secure Sockets Layer)	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.
Transport Layer Security (TLS)	and its predecessor, Secure Sockets Layer (SSL) - both frequently referred to as "SSL", are cryptographic protocols that provide communications security over a computer network.
Public Information	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

Term:	Definition:
	international statute, regulation, or law.
Non-Public Information	**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. Trinity employees must protect Trinity business-related data, whether on a Trinity-issued device or on a personal device used for business purposes and delete or preserve Trinity data as required. **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 (Identity Theft Enforcement & Protection Act).
Personal Identifiable Information or PII	The Family Educational Rights and Privacy Act (FERPA) 2008 regulations (34 CFR § 99) define personally identifiable information for education data and student education records as any data that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. Information that distinguishes or traces an individual includes, but is not limited to student’s name, student’s parents or family name, Student family address, SSN / Passport / Driver’s license number, and Biometric data. Linked or linkable information that combined with other information about or related to an individual, may allow to identify, trace, or locate a person. This may include date of birth, email address, credit card information, phone number, and Education information.

Related Documents

Related Documents:

Document Type:	Document Name:	Document Number:
Policy	Records Retention	BUSO-0020

Related Content:

Securing Information – Data Type Examples

Revision Management

Revision History Log:

Revision #:	Date:	Recorded By:
v1.0	4/27/2022 11:28 AM	Ben Lim
v2	3/11/2022 3:09 PM	Dan Carson
v1.0	8/14/2019 3:48 PM	Courtney Cunningham

Vice President Approval:

Name:	Title:
Ben Lim	Chief Information Officer