Information Security Risk Management Policy

Document Number: ITS-0026 **Date Published(sys):** 5/16/2022

General Description

Purpose:

The Information Security Risk Management Policy is intended to help manage security and privacy risks, and to facilitate compliance with applicable federal and state laws and regulations, as well as protect the confidentiality, integrity, and availability (CIA) of Trinity system components and IT resources and enable informed decisions regarding risk tolerance and acceptance.
This document has been developed to provide guidelines for managing security and privacy risks, and:

- To ensure that managing system-related security and privacy risk is consistent with the mission and business objectives of the organization and risk management strategy established by the senior leadership.
- To achieve privacy protections for individuals and security protections for information and information systems through the implementation of appropriate risk response strategies.
- To facilitate the integration of security and privacy requirements and controls into the enterprise architecture, acquisition processes, and systems engineering processes.

Scope:

This policy and supporting procedures encompass all system components that are owned, leased, rented, operated, maintained, and otherwise controlled by Trinity University or a third-party on behalf of Trinity University, and also applies to any system or system components, both internally and externally, that interact with these systems.

- Internal system components are those owned, operated, maintained, and controlled by Trinity and includes but is not limited to all network devices (firewalls, routers, switches, load balancers, other network devices), servers (both physical and virtual servers, along with the operating systems and the underlying application(s) that reside on them) and any other system components deemed in scope.

- External system components are those owned, operated, maintained, and controlled by any entity other than Trinity, but for which such external resources may impact the confidentiality, integrity, and availability (CIA) and overall security of the description of "Internal system components".
- While Trinity does not have the ability to provision, harden, secure, and deploy another organization's system components, the University will follow best practices by obtaining all relevant information ensuring that such systems are safe and secure.

Exceptions:

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

Policy Content

① Roles & Responsibilities

Implementing and adhering to organizational policies and procedures is a collaborative effort, requiring a true commitment from all personnel, including management, internal employees, and users of system components, along with vendors, contractors, and other relevant third parties. Additionally, by being aware of one's roles and responsibilities as it pertains to the 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 systems environment, while also assisting other applicable personnel in their day-to-day operations.
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 University system components. Additionally, Users are to report instances of non-compliance to senior authorities, specifically those by other users. Users, while undertaking day-to-day operations, may also notice issues that could impede the safety and security of

	Trinity University system components and are to also report such instance immediately to senior authorities
Vendors, Contractors, another Workforce	Responsibilities for such individuals and organizations are much like those stated for 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
Chief Information Officer - CIO	Reports to other members of senior management on a regular basis regarding all aspects of the organization's information systems posture. Responsible for ensuring that risk assessments are conducted on Information Systems, using the University approved process. Oversees personnel with significant responsibilities for security and ensures they are adequately trained. Assists senior organizational officials concerning their security responsibilities.
Chief Information Security Officer - CISO	Responsible for implementing systems and specifications to facilitate compliance with this policy. Responsible for developing and maintaining security policies, procedures, and control techniques to address security requirements. Establishes a risk management strategy for the organization that includes a determination of risk tolerance.
CORE Infrastructure System Administrators	Responsible for assessing and mitigating risks using the University approved processes. Assess organization-wide security risk and update the risk assessment results on an ongoing basis.
ITS Managers	Responsible for ensuring that information systems under their control are assessed for risk and that identified risks are mitigated, transferred, or accepted. In coordination with the Chief Information Security Officer, is responsible for the development and maintenance of the security and privacy plans and ensures that the system is operated in accordance with the selected and implemented controls.
System Owners	Responsible for addressing the operational interests of the user community (i.e., users who require access

	to the system to satisfy mission, business, or operational requirements) and for ensuring compliance with security requirements. Decides who has access to the system (and with what types of privileges or access rights).

② Policy

The University must develop and maintain an Information Security Risk Management Process and other tools and mechanisms to frame, assess, respond, and monitor information security related risks.

All Information Systems, information assets, and business processes that involve non-public information at Trinity must be assessed for risk to the University that results from threats to the integrity, availability, and confidentiality of Trinity Data. Assessments must be completed prior to purchase of, or significant changes to, an Information System; and at least every 2 years for systems that store, process, or transmit Restricted Data.

ITS will conduct ongoing assessments of threats and risks related to information assets and business processes, to determine the need of safeguards, countermeasures, and controls. Trinity University senior leadership had adopted an IT risk-averse posture.

Risks identified by a risk assessment must be mitigated or accepted prior to the system being placed into operation.

Residual risks must only be accepted on behalf of the University by a person with the appropriate level of authority as determined by the Chief Information Officer and Chief Information Security Officer. Approval authority may be delegated if documented in writing, but ultimate responsibility for risk acceptance cannot be delegated. The Chief Information Officer is responsible for risk treatment or risk acceptance. Most common types of information security risk assessments include but are not limited to standard asset-based or scenario-based risk assessments, third-party security risk assessments, cloud security assessments, privacy impact assessments, among others.

③ Risk Management Process

The Risk Management system is dynamic and is designed to adapt to Trinity University's developments and any changes to the organization's risk profile over time. The Risk Management system is based on a structured and systematic process which considers Trinity University's internal and external risks. The Risk Management system includes the Risk Management Policy and is continuous, throughout the team

risks are identified and in turn treated. The main elements of the risk management process are as follows:

Communicate and Consult

Communicate and consult with internal and external stakeholders as appropriate at each stage of the risk management process and concerning the process as a whole.

Establish the Context

Establish the external, internal, and risk management context in which the rest of the process will take place. The criteria against which risk will be evaluated should be established and the structure of the analysis defined.

Identify Risks

Trinity will identify risks (threats or opportunities) following established procedures and the Risk Management Policy and document the risk in the security and risk assessment register. Identify where, when, why, and how events could prevent, degrade, delay, or enhance the achievement of University's objectives.

Record Risks

Any risks identified should be documented on a security and risk assessment register, to be maintained by the Chief Information Officer, or designee.
Document the net effect of all identified threats and opportunities, by assessing:

- Likelihood of threats and opportunities (risks) to occur
- Impact of each risk
- Treatment of Risk (Mitigation or Acceptance)

Evaluate Risks and Respond

Compare the estimated levels of risk against the pre-established criteria and consider the balance between potential benefits and adverse outcomes. This enables decisions to be made about the extent and nature of treatments required. Trinity will review the security and risk assessment register and plan actions or responses that are designed to mitigate threats and

maximize opportunities.

Monitor and Review

After the risk responses and implementation has been completed, the performance of the risk management solution will be monitored, measured, and reviewed. Plans are likely to change over time as business initiatives change. Risk may come from any internal or external event that may affect the ability to operate efficiently and effectively.

Internal Risks are those risks that specifically relate to University business and are generally within the organization's control. This includes risks such as employee, strategic, operational, and financial risk.

External Risks are those risks that are outside the control of the University. This includes risks such as the Covid19 virus and its ability to morph into other variants, legislative and congressional decisions, court rulings, US military command decisions, and market conditions.

Performance Evaluation

Consequences of Policy Violation:

Any behavior in violation of this policy is cause for disciplinary action and violations of this policy may result in, but are not limited to, any or all the following:

- Loss of university computing, email and/or voice mail privileges
- Disconnection from the residential hall internet network
- University judicial sanctions as prescribed by the student code of conduct
- Reassignment or removal from university housing and/or suspension or expulsion from the university
- Prosecution under applicable civil or criminal laws

Violations will be adjudicated, as appropriate, by the CIO, the Office of the Dean of Students, the Office of Housing and Residential Life, and/or the Office of Human Resources.
An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Terms & Definitions

Terms and Definitions:

Term:	Definition:
Asset Owner	The term ‘owner’ identifies an individual or entity that has approved management responsibility for controlling the production, development, maintenance, use and security of the assets. The term ’owner’ does not mean that the person actually has any property rights to the asset. (Extract from ISO 27001:2005)
Control	Process or procedure to reduce risk.
Inherent Risk	Level of risk before Risk Treatments (controls) are applied
IT Resources	Include computing, networking, communications, application, and telecommunications systems, infrastructure, hardware, software, data, databases, personnel, procedures, physical facilities, cloud-based vendors, Software as a Service (SaaS) vendors, and any related materials and services
Information Security Risk Management (ISRM)	Program that consistently identifies and tracks information security risks, implements plans for remediation, and guides strategic resource planning
Residual Risk	Level of risk that remains after Risk Treatments (controls) are applied to a given Risk
Risk	Possibility of suffering harm or loss or the potential for realizing unwanted negative consequences of an event.
Risk Assessment	Process of taking identified risks and analyzing their potential severity of impact and likelihood of occurrence.
Risk Management	The process of identifying, assessing, and controlling threats to an organization's capital and earnings.
Risk Treatment	Process of managing assessed or identified risks. Risk treatment options are risk avoidance (withdraw from), sharing (transfer), modification (reduce or mitigate) and retention (acceptance)

Revision Management

Revision History Log:

Revision #:	Date:	Recorded By:
v2.0	5/16/2022 3:46 PM	Ben Lim

Revision #:	Date:	Recorded By:
v1.0	4/21/2022 12:33 PM	Dan Carson

Vice President Approval:

Name:	Title:
Ben Lim	Chief Information Officer