Incident Response Policy

Document Number: ITS-0012 **Date Published(sys):** 7/8/2021

General Description

Purpose:

It is vital to the University community that computer security incidents that threaten the security or privacy of confidential information are properly identified, contained, investigated, and remedied. According to Texas Senate Bill 122 Section 48.102, the University "shall implement and maintain reasonable procedures, including taking any appropriate corrective action, to protect and safeguard from unlawful use or disclosure of any sensitive personal information collected or maintained in the regular course of business."

The purpose of this policy is to provide the basis of appropriate response to incidents that threaten the confidentiality, integrity, and availability of university digital assets, information systems, and the networks that deliver the information. The Incident Response Policy provides a process for documentation, appropriate reporting internally and externally, and communication to the community as part of an ongoing educational effort. Finally, the policy establishes responsibility and accountability for all steps in the process of addressing computer security incidents.

Scope:

The Incident Response Policy applies to all members of the Trinity University community. The Trinity University community (hereafter described as the "University community") includes faculty and staff members, students, alumni, guests, and contractors. This Policy also includes computing or network devices owned, leased, or otherwise controlled by Trinity University. Additionally, incidents involving confidential information apply to any computing or network device, regardless of ownership, on which confidential or restricted information is stored or by which access to confidential or restricted information might be gained. (Examples include, but are not limited to: a home computer containing confidential data, a mobile device on which credentials are stored which could be used to access confidential data, a server housed in an off-site facility.)

Policy Content

Intrusion attempts, security breaches, theft or loss of hardware and other security related incidents perpetrated against the University must be reported to Information Technology Services (ITS). Anyone with knowledge, or a reasonable suspicion, of an incident which violates the confidentiality, integrity, or availability of digital information, will make an immediate report to the following e-mail address: infosec@trinity.edu.

The Director of Networks, Security and Systems, in collaboration with other appropriate staff, shall determine if a reported incident IS or IS NOT a confidential information Security Incident.

If the incident IS NOT considered a confidential information Security Incident, the incident shall be referred to a Systems Administrator who shall insure that the incident is handled in accordance with the procedures described herein. The Director of Network, Security, and Systems, shall inform the Director and Chief Information Officer. The Director and Chief Information Officer will inform the Director of Risk Management.

If the Director of Networks, Security and Systems, in collaboration with other appropriate staff, determines that the incident IS a confidential data security incident, an Incident Response Team is formed. The purpose of the Incident Response Team is to determine a course of action to appropriately address the incident. The Chief Information Officer shall designate the membership of the Incident Response Team. Normally, membership will include appropriate individuals from ITS, offices with primary responsibility for the compromised data, and the Office of Risk Management.

It is the responsibility of the Incident Response Team to assess the actual or potential damage to the University caused by the Confidential Data Security Incident, and to develop and execute a plan to mitigate that damage. Incident Response Team members will share information regarding the incident outside of the team only on a need-to-know basis and only after consultation with and consensus by the entire team.

The Incident Response Team should review, assess, and respond to the incident for which it was formed according to the following factors, in decreasing order of priority:

- Safety - If the system involved in the incident affects human life or safety, responding in an appropriate, rapid fashion is the most important priority.
- Urgent concerns - Departments and offices may have urgent concerns about the availability or integrity of critical systems or data that must be addressed promptly. Appropriate ITS staff shall be available for consultation in such cases.
- Scope - Work to promptly establish the scope of the incident and to identify the extent of systems and data affected.
- Containment - After life and safety issues have been resolved, identify and implement actions to mitigate the spread of the incident and its consequences. Such actions might well include requiring that affected systems be disconnected from the network.
- Preservation of evidence - Promptly develop a plan to identify and implement steps for the preservation of evidence, consistent with needs to restore availability. The plan might include steps to clone a hard disk, preserve log information, or capture screen information. Preservation of evidence should be addressed as quickly as possible in order to restore availability of the affected systems as soon as practicable.
- Investigation - Investigate the causes and circumstances of the incident, and determine future preventative actions.
- Incident-specific risk mitigation - Identify and recommend strategies to mitigate the risk of harm arising from this incident.

If, in the judgment of the Chief Information Officer, the incident might reasonably be expected to cause significant harm to the subjects of the data or to Trinity University, the Chief Information Officer may recommend to the President that a Senior Response Team be established. The Senior Response Team shall be comprised of senior-level administrators designated and recommended by the Chief Information Officer or Vice President and the Office of Risk Management. The Senior Response Team will determine whether Trinity University should make best efforts to notify individuals whose personally identifiable information might have been at risk due to the incident. In making this determination, the following factors shall be considered:

- Legal duty to notify
- Length of compromise
- Human involvement
- Sensitivity of compromised data
- Existence of evidence that data were compromised
- Existence of evidence that affected systems were compromised for reasons other than accessing and acquiring data
- Additional factors recommended for consideration by members of the Incident Response Team

ITS shall maintain a log of all confidential information Security Incidents, recording the date, type of confidential information affected, number of subjects affected (if applicable), summary of the reason for the breach, and corrective measures taken.

ITS shall issue a report for every confidential information Security Incident describing the incident in detail, the circumstances that led to the incident, and a plan to eliminate the risk of a future occurrence.

ITS shall provide annually to the Chief Information Officer a report containing statistics and summary-level information about all known confidential information Security Incidents, along with recommendations and plans to mitigate the risks that led to those incidents.

Performance Evaluation

Consequences of Policy Violation:

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

- Attending a class or meeting on Security Incident issues, as well as successful completion of a follow up quiz;
- Loss of University computing, email and/or voice mail privileges;
- Disconnection from the residential hall network;
- University judicial sanctions as prescribed by the student Code of Conduct;
- Monetary reimbursement to the University or other appropriate sources;
- Reassignment or removal from University housing and/or suspension or expulsion from the University;
- Prosecution under applicable civil or criminal laws;
- Employees may be subject to disciplinary action.

Violations:
Reports of data and systems compromises and the exposure of personal and restricted information should be immediately reported to: infosec@trinity.edu

Terms & Definitions

Terms and Definitions:

Term:	Definition:
Confidential Information	Sensitive personally-identifiable information that must be safeguarded in order to protect the privacy of individuals and the security and integrity of systems and to guard against fraud. This includes, but is not limited to: • Social Security numbers • Credit and debit card numbers • Bank account or other financial account numbers • Salary information • FERPA protected information • HIPAA protected information • Passwords, passphrases, PIN numbers, security codes and access codes • Tax returns • Credit histories or reports • Background check reports Additionally, proprietary information, data, information, or intellectual property, in which the University has an exclusive legal interest or ownership right may also be considered confidential information. Examples include, but are not limited to: • Financial information • Business planning data

Term:	Definition:
	• Data, software, or other material from third parties which the University has agreed to keep confidential
Malware	Any software designed with malicious intent. Examples include, but aren't limited to: • Viruses • Worms • Trojan horses • Spyware
Security Incident	Any event that threatens the confidentiality, integrity, or availability of University systems, applications, data, or networks. Examples of University systems include, but are not limited to: • Servers • Desktop computers • Laptop computers • Workstations • Mobile devices • Network equipment Examples of Security Incidents include, but aren't limited to: • Unauthorized access • Intentionally targeted but unsuccessful unauthorized access • Accidental disclosure of Confidential Data • Infection by malware • Denial-of-service (DoS) attack • Theft or loss of a University system • The theft or physical loss of computer equipment known to store SSNs • Loss or theft of tablets, smartphones or other mobile device • A server known to have sensitive data is accessed or otherwise compromised by an unauthorized party • A firewall accessed by an unauthorized entity • A DDoS (Distributed Denial of Service) attack • The act of violating an explicit or implied security policy • A virus or worm uses open file shares to infect from one to hundreds of desktop computers • An attacker runs an exploit tool to gain access to a University server’s

Term:	Definition:
	password file
Sensitive Personal Information	As defined by the Texas Senate Bill 122 means “an individual’s first name or first initial and last name combination with any one or more of the following data elements (when the name or data element is not encrypted): • Social security number • Driver’s license or government issued identification number • Account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to an individual’s financial account. • Does not include publicly available information that is lawfully made available to the general public from the Federal government or a state or a local government” (2-3).

Revision Management

Revision History Log:

Revision #:	Date:	Recorded By:
v1.0	8/14/2019 3:34 PM	Courtney Cunningham

Vice President Approval:

Enter Vice President(s) that are responsible for approving this document

Name:	Title:
Gary Logan	Vice President for Finance & Administration