Information Security

Stevenson University Incident Response Plan

Last Updated: January 10, 2025

OFFICE OF INFORMATION TECHNOLOGY
STEVENSON UNIVERSITY

Table of Contents

Overview

Purpose: This plan describes the framework used to ensure that information security incidents involving any Stevenson University technology resources are managed in an effective and consistent manner. It defines the roles and responsibilities, classification of incidents, and phases of response activities. This plan helps Stevenson:

- Reduce the risk of information security incidents
- Meet legal and regulatory compliance

Owner: Chief Information Officer, Office of Information Technology.

Approval: This plan is reviewed annually by university leadership.

Definitions

Cloud computing service: Any function provided by an agreement with an external organization that includes the ability to store or transmit electronic information.

Software: Any code, program or application designed to perform specific functions on a device.

Technology resource: Any device, software or service that stores or transmits electronic information as part of its function.

Device: Any equipment or hardware that stores or transmits electronic information. This includes computers, mobile devices, network equipment, phones, and server systems.

User: Someone who is provided access to technology resources, including students, faculty, staff, contractors and other approved individuals or groups.

Event of interest: Any observable occurrence within a system, network or other technology resource that needs to be investigated to determine if it is an information security incident.

Information security incident: Any event that threatens the confidentiality, integrity, or availability of Stevenson University information. This includes any violation or imminent threat of violation of information security policies, acceptable use policies, or standard security practices.

Security incident response playbook: A set of procedures defined for a specific type of security incident.

Credential harvesting: A type of phishing attack where victims are duped into providing their account and password information.

Data Breach: The intentional or unintentional release of secure or private information to an untrusted environment.

Roles and Responsibilities

Groups

Crisis Management Team (CMT) A group of leaders organized under the Stevenson's Crisis Management Plan. The group includes representatives from university groups that may be required assist in information security incident response, including Human Resources, Campus Security, Marketing & Digital Communications, etc.

Office of Information Technology (OIT) – Leads most areas of this plan, with guidance from the CMT.

Cyber Incident Response Team (CIRT) – A team assembled to lead the response to each security incident. The composition of the team will be determined by the Chief Information Officer based on the type and severity of the incident. A Security Incident Response Playbook, if available, will also be used to determine CIRT members.

Individuals

Chief Information Officer - Directs overall investigations and response. Coordinates with outside counsel and senior leadership regarding compliance with legal obligations. Coordinates with the CMT and reports security incidents to senior management and the Board of Trustees, as appropriate.

Director Of Network and Infrastructure – Leads the CIRT. Leads coordination with law enforcement and other outside organizations when directed by the CIO or CMT. Coordinates updates and changes to this plan.

Methodology

Stevenson's security incident response methodology is based on the National Institution of Science and Technology's Computer Incident Response Handling Guide (NIST Special Publication 800-61 Revision 2), which outlines several phases and activities within each phase.

Incident Response Phase – Prepare

1. Incident handling resources. The Office of Information Technology (OIT) prepares the Cyber Incident Response Team (CIRT) with the following:
    a. Security incident response playbooks. Playbooks contain detailed and specific steps for various types of security incidents.
    b. Communication. OIT uses a communication and collaboration process used for information technology emergencies, including security incidents, which provides flexibility and resiliency.
    c. Training. Tabletop exercises are run periodically to test and improve playbooks and improve the team's response handling skills.
2. Incident prevention. See Stevenson's Information Security Plan for details on the following areas: a. Risk assessments.
    b. Host/system and network security protection.
    c. User awareness and training.

Incident Response Phase – Detect & Analyze

1. Detection sources and reporting process. OIT detects potential security events from the following sources:

Source	Description	Reporting
Help Desk/Tech Support Center	Includes: online ticketing system, phone number, walk-in offices	Email, phone call, in-person
OIT staff	Information from users, vendors, other systems, etc.	Email, phone call, in-person, system reports
SecureIT mailbox	Dedicated shared mailbox for anyone to send suspicious emails	Email
Microsoft cloud environment	Azure and Microsoft Office 365	Email alerts, management console dashboards and reports
Infrastructure monitoring	Several tools used to monitor and alert on various operational conditions	Email alerts, management console dashboards and reports
Endpoint protection	Endpoint protection management console	Console alerts and monthly reports
Network perimeter monitoring	Firewall management console	Email alerts, management console dashboards and reports
Third-party monitoring sources	HaveIBeenPwnd, REN-ISAC	Email alerts
Public sources	Educause email list-servs, social media, traditional news sources	Email, manual web browsing

2. Incident analysis. OIT triages any event of interest to determine whether it is a security incident using several processes, including security playbooks and OIT's overall emergency response procedures. Once OIT has identified an event as a security incident, the Chief Information Officer (or designated alternate) is notified to perform the next actions to determine the category and severity of the incident.

3. Incident classification. Each security incident is classified into one of the following categories:

   Category 0 - Test/Exercise. Used for any approved test or exercise, such as internal or external network penetration tests.

   Category 1 - Data Theft. Any attempted or successful destruction, manipulation, or disclosure of sensitive, confidential or proprietary information. Includes any incident requiring breach notification or resulting in financial loss (Business Email Compromise - BEC). Does not include most typical phishing attacks/attempts (Categories 3 and 5).

   Category 2 - Denial of Service. Any attack that successfully prevents or impairs the normal authorized functionality of networks, systems or applications by exhausting resources. This activity includes being the victim or participating in an attack.

   Category 3 - Compromised technology asset. Any incident with the intent to obtain unauthorized access to a technology asset: host, network device, account, service etc. Includes malware-infected hosts and attempts to access computer or cloud service accounts, whether successful or not.

Category 4 - Improper Usage. Any violation of acceptable computing use policies by a student, faculty member or staff member.

Category 5 – Phishing. Any attempt to collect sensitive information via electronic communication, including email, social media accounts, SMS/text, phone call, etc. Includes attempts with financial scams to obtain money. Does not include account compromise attempts that may have been initiated by credential harvesting phishing attacks (Category 3) or data theft incidents (Category 1).

Category 6 – Investigation. Unconfirmed events that are potentially malicious or anomalous activity deemed by the reporting entity to warrant further review. This also includes any activities that do not have measurable impact - scans, probes.

Category 7 - Loss or Theft of Equipment. The loss or theft of any device storing sensitive information.

4. Incident severity. The overall incident severity is determined by the highest severity of three key impact areas: Function, Information and Recovery:

Impact category	No severity	Low severity	Medium severity	High severity
Functional impact - Consider not only the current functional impact of the incident, but also	No effect to the institution's ability to provide all	Minimal effect: the institution can still provide all critical	Institution has lost the ability to provide a critical service to a	Institution is no longer able to provide some
the likely future functional impact of the incident if it is not immediately contained.	services to all users.	services to all users, but has lost efficiency.	subset of system users.	critical services to any users.
Information impact - Consider how the compromised information will impact the institution's overall mission, finances or reputation. Includes exposure, exfiltration, change or deletion.	No information was compromised.	Information considered public or not sensitive was compromised or potentially compromised.	Proprietary information that could have financial or reputational impact was compromised or potentially compromised.	Information with legal or regulatory data breach obligations was compromised or potentially compromised.
Recovery impact - Consider the effort necessary to recover from an incident and weigh that against the value the recovery effort will create, and any requirements related to incident handling.	No effort needed for recovery.	Time to recovery is predictable with existing resources.	Time to recovery is predictable with additional resources.	Time to recovery is unpredictable; additional resources and outside help are needed; or recovery is not possible.

5. Incident initial response and notification.
    a. During the analysis phase, OIT leaders will designate individuals need to be part of the CIRT for the specific incident. CIRT members will be notified using OIT's emergency response procedures.
    b. The CIRT leader will work with the CIO to notify others following this table:

	Low Severity	Medium Severity	High Severity
CIRT initial response time	24 hours	60 minutes	30 minutes
Notification groups	OIT Leadership	OIT Leadership	CMT. OIT Leadership
Notification interval	Weekly	Daily	Every 2 hours until CIRT determines new schedule

    c. External notification. The university's Crisis Management Plan outlines the process for communicating to outside parties, including customers, law enforcement and other individuals and organizations.

Incident Response Phase – Contain and Eradicate

After the initial notification and assembly of the CIRT, the CIRT will begin containment and eradication activities. If available, playbooks will be used. Here are key containment and eradication activities:

1. Identify and execute containment strategy. Containment is important before an incident overwhelms resources or increases damage. An essential part of containment is decision-making (e.g., shut down a system, disconnect it from a network, disable certain functions, etc.). Acceptable risks in dealing with incidents should be reviewed when developing containment strategies.
2. Gather and preserve evidence. Although the primary reason for gathering evidence is to resolve the incident, it may also be needed for legal proceedings. In such cases, it is important to clearly document how all evidence, including compromised technology resources, has been preserved.
3. Identify attackers and root cause. Although this information can be important, incident handlers should generally stay focused on containment, eradication, and recovery. Identifying an attacker can be a time consuming process that can prevent a team from achieving its primary goal—minimizing the business impact.
4. Eradicate all malicious components involved in the incident. It is important to identify all affected technology resources so that they can be remediated. For some incidents, eradication is either not necessary or is performed during recovery.

Incident Response Phase – Recover

Once the CIRT had determined that a security incident has been contained and eradicated, the next phase is to recover from the incident. Here are key recovery activities:

1. Identify and execute a recovery strategy. In most cases, recovery should be done in a phased approach so that remediation steps are prioritized.

2. Establish steps to confirm affected systems are functioning normally. Recovery may involve such actions as restoring systems from clean backups, rebuilding systems from scratch, replacing compromised files with clean versions, installing patches, changing passwords, and tightening network perimeter security
3. Determine any monitoring requirements. Higher levels of system logging or network monitoring are often part of the recovery process. Once a resource is successfully attacked, it is often attacked again, or other resources within the organization are attacked in a similar manner.

Incident Response Phase – Post-Incident Activities

1. Conduct lessons learned session. Meeting with all involved parties after a major incident, and optionally periodically after lesser incidents as resources permit, can be extremely helpful in improving security measures and the incident handling process itself.
2. Collect and measure incident response metrics. Lessons learned activities should produce a set of objective and subjective data regarding each incident. A study of incident characteristics may indicate systemic security weaknesses and threats, as well as changes in incident trends.
3. Determine evidence retention requirements. Some factors that should be considered regarding any evidence gathered during a security incident:
    a. Potential prosecution. If it is possible that the attacker will be prosecuted, evidence may need to be retained until all legal actions have been completed.
    b. Data Retention. Follow any existing data retention policies for specific types of evidence gathered, such as email, system logs, etc.
    c. Cost. Retaining hardware can be costly over long periods of time. Retaining large amounts electronic data also has IT administration costs.

Appendix

Public documents:

1. National Institution of Science and Technology's Computer Incident Response Handling Guide (NIST Special Publication 800-61 Revision 2): https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
2. Stevenson Crisis Management Plan: https://www.stevenson.edu/about/campus-services/campussecurity/documents/Crisis_management_plan.pdf

Institutional documents (some documents requires valid credentials):

1. SU Now Information Security portal: https://now.stevenson.edu/oit
2. Stevenson University Security Information Security Plan: https://www.stevenson.edu/about/campus-services/office-information-technology/
3. Stevenson University Data Governance Plan: https://www.stevenson.edu/about/campus-services/office-information-technology/