# Security Incident Response Policy for Chicago State University Systems

## Policy Statement

The CSU Security Incident Response Policy defines the responsibilities of CSU staff when responding to or reporting security incidents. It delineates roles within the Computer Security Incident Response Team (CSIRT) and outlines which members of University administration should be involved in different types of security incidents.

## Purpose

The purpose of the CSU Security Incident Response Policy is to describe the requirements for dealing with security incidents.

## Scope

The CSU Incident Management Policy applies to individuals that use any CSU Information Resource.

## Definitions

**Security Incident -** is defined as any actual or suspected event that may adversely impact the confidentiality, integrity, or availability of data or systems used by the University to process, store, or transmit that data. Examples of events that could constitute a security incident include:

- Unauthorized access to data by an outsider or insider not authorized to access that data
- An endpoint (desktop, laptop, server, or mobile device) infected by malware. "Malware" is a broad category encompassing Trojans, worms, viruses, ransomware, and other malicious programs
- Reconnaissance activities such as scanning the network for security vulnerabilities when scans are performed by outsiders or insiders not authorized to perform such scans
- Denial of Service attacks (performed by outside or inside entities)
- Web site defacements
- Violations of CSU information security policies
- Unpatched vulnerabilities on systems connected to the CSU network
- Discovery of an unregistered or non-centralized server in violation of the Server Hosting Policy.

**Event** - is an exception to the normal operation of IT infrastructure, systems, or services. Events may be identified through the use of automated systems; reported violations to the ISO, Compliance/Privacy, or other university department; or in the course of normal system reviews including system degradation/outage. It is important to note that not all events become security incidents.

**ITD Resources / Information 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 Technology Department Leader** is the most senior University employee responsible for the security program and its operation.

**Information System** is a major application or general support system for storing, processing, or transmitting University Information. An Information System may contain multiple subsystems. Subsystems typically fall under the same management authority as the parent Information System. Additionally, an Information System and its constituent subsystems generally have the same function or mission objective, essentially the same operating characteristics, the same security needs, and reside in the same general operating environment.

**Information Technology Department** is the individual(s) or Unit responsible for the overall procurement, development, integration, modification, and operation and maintenance of an Information System. This individual or Unit is responsible for making risk tolerance decisions related to such Information Systems on behalf of the University and is organizationally responsible for the loss, limited by the bounds of the Information System, associated with a realized information security risk scenario.

University's Information Security Office, responsible for coordinating the development and dissemination of information security policies, standards, and guidelines for the University.

**Unit** is a college, department, school, program, research center, business service center, or other operating Unit of the University.

**University Information** is any communication or representation of knowledge, such as facts, data, or opinions, recorded in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual, owned or controlled by or on behalf of the University.

**University-Related Persons / Employee / Staff** are University students and applicants for admission, University employees and applicants for employment, Designated Campus Colleagues (DCCs), alumni, retirees, temporary employees of agencies who are assigned to work for the University, and third-party contractors engaged by the University and their agents and employees.

**Associate / "Contractor", Third-party or 3rd party** is someone officially attached or connected to the College who is not a student or employee (e.g., contractors, vendors, interns, temporary staffing, volunteers.)

## Roles and Responsibilities

**Information Security Leader**—The Information Security Leader is responsible for assessing the initial scope of a security incident, assembling the Enterprise Incident Management Team, and appointing the Incident Manager.

**Security Incident reporting**—All members of the University community are required to report actual or suspected security incidents. All suspected security incidents should be reported to the help desk at (773) 995-2963 or helpdesk@csu.edu

**Security Incident response manager**—This role is designated by the Information Security Leader and will lead the response to the incident. This is a technical role and will coordinate the work of log collection, evidence preservation, and analysis activities.

### Enterprise Incident Management Team:

When a breach of "Confidential" data has been declared, the following University administration roles will be added to the incident response team:

- Senior administrator for impacted unit(s)
- Chief Information Officer
- Information Security Leader
- Representative from the Office of General Counsel
- Public Relations / Press Relations / Communications
- Chief Internal Auditor
- Others on an as-needed basis

The Enterprise Incident Management Team will work with the Public Relations / Press Relations / Communications to determine when and how to inform individuals outside the EIMT regarding the incident.

Members of the Enterprise Incident Management Team and all IT staff shall receive annual incident response training. Tabletop exercises recreating a significant security incident will be conducted at minimum every two years.

## Incident Severity Levels

Incident response will be addressed based on the severity of the incident. Incident severity takes several factors into account: sensitivity of the data involved, number of end users impacted, and its overall impact on the ability of the University to fulfill its mission. Incident severity also will be used to determine who manages an incident, who is informed about an incident, and the extent and immediacy of the response to the incident.

### *High*

A security incident will be considered "high" if any of the following characteristics are present:

I. Threatens to impact (or does impact) systems critical to the University's ability to function normally. This includes but is not limited to email, courseware, human resources, financials, internet connectivity, or portions of the campus network
II. Poses a serious threat of financial risk or legal liability
III. Threatens to expose (or does expose) "Confidential" data as defined by the Data Classification & Handling Policy
IV. Threatens to propagate to or attack other networks, or organizations internal or external to the University
V. Terroristic threats or other threats to human life or property when received by the IT Security Office

### *Medium*

A security incident will be considered "medium" if any of the following characteristics are present:

I. Threatens to impact (or does impact) a significant number of systems or people. The University can still function, but a group, department, unit, or building may be unable to perform its mission
II. Systems impacted contain only Public or Internal data
III. Impacts a non-critical system or service

### *Low*

Low severity incidents have no characteristics from the "medium" or "high" categories and may include the following:

I. Only a small number of people or systems are impacted
II. Systems impacted contain only Public data
III. Little to no risk of the incident spreading or impacting other organizations or networks

## Security Incident Response Summary Table

The following table summarizes how IT security incidents will be handled based on severity. It includes response times, who will manage each type of incident, and reporting requirements.

| Incident Severity | Response Time | Incident Response Manager | Who to Notify | Incident Report Required? |
|---|---|---|---|---|
| High | Immediate | Information Security Leader | • CIO<br>• Unit administrator (Vice Provost, Dean, etc.)<br>• General Counsel<br>• Internal Audit<br>• Others on a need-to-know basis | Yes |
| Medium | 4 hours | Information Security Leader or ITD Operations Delegate | • CIO<br>• Unit administrator (Vice Provost, Dean, etc.)<br>• General Counsel<br>• Internal Audit<br>• Others on a need-to-know basis | If requested by IT Security Officer, CIO, or other administrator |
| Low | Next business day | Information Security Leader or ITD Operations Delegate | • CIO<br>• Unit administrator (Vice Provost, Dean, etc.)<br>• General Counsel<br>• Internal Audit | No |

| | | | | |
|---|---|---|---|---|
| | | | • Others on a need-to-know basis | |

## Policy

### Security Incident Reporting

- Personnel are required to promptly report possible or known information security and confidentiality violations to CSU ITD; including the following:
    - Infrastructure incident: any event considered to be a malicious action that causes a failure, interruption, or loss in availability to any CSU Information Resource.
    - Data incident: any loss, theft, or compromise of CSU information.
    - Unauthorized access incident: any unauthorized access to a CSU Information Resources.
- Potential incidents and threats reported from event logging, vulnerability management, and other monitoring activities must be reported to CSU ITD.
- All reported incidents must be assessed by the Information Security Leader to determine the threat type and activate the appropriate response procedures.

### Response Team

- Security Incident Response Commander will establish and provide overall direction to a CSU Security Incident Response Team (SIRT).
- The Security Incident Response Commander is responsible for overseeing the creation, implementation, and maintenance of an Incident Management Plan.
- CSU SIRT members have pre-defined roles and responsibilities which can take priority over normal duties. Any additional CSU staff member may be called upon to assist in resolving an incident.
- The SIRT will respond to any new threat to CSU information systems or data following the Incident Management Plan.
- The Incident Response Commander must report the incident to:
    - CSU Executive Management
    - Any affected customers and or/partners
    - Local, state, or federal law officials as required by applicable statutes and/or regulations.
- The Security Incident  Response Commander or individual delegated by the CIO or University President, will coordinate communications with any outside organizations.
- The Security Incident Management Plan must be tested by the ISRT no less than annually.
- The ISRT must participate in training activities specific to the organization's Security Incident Response Plan at least annually or upon significant change to the organization.

## Policy Exceptions and Maintenance

Waivers from certain and specific policy provisions may be sought following the CSU Waiver Process. There are no exceptions to any provisions noted in this policy until and unless a waiver has been granted.

## Enforcement

This Security Incident Response Policy supplements and compliments all other related information security policies, it does not supersede any such policy or vice versa. Where there are any perceived or unintended conflicts between CSU policies, they must be brought to the attention of CSU for immediate reconciliation.

Failure to report an information security incident may subject the user to disciplinary action including, but not limited, to suspension of the user's access to electronic information resources. Users also should be aware of other possible consequences under University policies and federal, state, or local laws, particularly those related to computer crime and copyright violation.

Personnel found to have violated any provision of this policy may be subject to sanctions up to and including removal of access rights, termination of employment, termination of contract(s), and/or related civil or criminal penalties.

## References

- NIST CSF: PR.IP, DE.DP, DE.AE, RS.RP, RS.CO, RS.AN, RS.MI, RS-IM, RC.CO

## Version History

| Version | Modified Date | Next Review | Approved Date | Approved By | Comments |
|---|---|---|---|---|---|
| 1.0 | 11/3/2022 | 11/1/2023 | 11/6/2022 | Donna Hart | |
| | | | | | |
| | | | | | |