Category: Information Security Legal and Compliance Responsible Office: Office of the Chief Operations Officer	Standard Title: Incident Response Standard Document Number: 6902 Effective Date: June 1, 2026 This policy item applies to: Community Colleges State-Operated Campuses Statutory Colleges System Administration Entities, Affiliates, and Third-Party Service Providers

Table of Contents

Section 1: Purpose and Scope 2
Section 2: Establishment of Institutional Incident Response Plans 2
Section 3: Incident Response Governance Components 3
Section 4: Incident Response Plan Phases and Documentation Requirements 4
Section 5. Preparation Phase 5
Section 6. Detection and Analysis 5
Section 7. Containment, Eradication and Recovery 6
Section 8. Post Incident Activities 7
Section 9. Definitions 7
Other Related Information 8
Related Policies and Procedures 8
Authority 9
History 9

Section 1. Purpose and Scope

1.1 Purpose

This Incident Response (IR) Standard establishes a comprehensive framework for identifying, responding to, and mitigating information security incidents across the university system. It aims to minimize the impact of security breaches, protect sensitive data, and ensure continuity of academic and administrative operations.

1.2 Scope

This standard applies to:

- State-operated institutions and community colleges.
- Statutory colleges, with respect to the sharing of information with other SUNY institutions.
- System Administration, the Information Technology and Exchange Center (ITEC), and the Student Information and Campus Administrative Systems (SICAS) program.
- Entities, affiliates, and third-party service providers that use the State University's data and/or information systems for their operations or the delivery of services.

And encompasses:

- All institutional data, including administrative, teaching and learning, clinical, and research. Institutional data is any data owned, licensed by, or under the direct control of SUNY, whether stored locally or with a cloud provider.
- Third-party vendors who collect, process, share, or maintain university institutional data, whether managed or hosted internally or externally.

Section 2. Establishment of Institutional Incident Response Plans

2.1 Implement and Maintain an Incident Response Plan

Standard: Institutions must draft, implement, and maintain an incident response plan. Institutional Incident Response Plans shall:

- Describe and identify the institutions' governance structure for responding to the technical, operational, financial, legal, and reputational impacts of security incidents.
- Documents the institutions Incident Response team structure and personnel contact information.

- Documents common processes and tasks associated with the corresponding incident response lifecycle phases[1].
- Defines criteria for the categorization and prioritization of security incidents.
- Specifies the individuals authorized to report security incidents to the institutions cyber insurance carrier and or activate resources available through said carrier.
- Defines the resources and management support needed to effectively maintain and mature an incident response capability.

Section 3. Incident Response Governance Components

3.1 IR Roles Responsibilities

Each campus must exercise their discretion and institutional knowledge when constructing their IR teams and designating team leaders. These roles should be based on the skills, functions, and needs attributable to that institution. At a minimum, institutional plans and/or procedures must identify and incorporate the following roles with commensurate responsibilities.

3.1.1 Document and Describe an Incident Response Team

Standard: Every institution's plan shall establish and identify an incident response team capable of addressing the technical, operational, financial, legal, and reputational aspects of security incidents. The IR team responsibilities section must include the individuals directly responsible for the following functions:

- **Technical Response Functions**: Detection, analysis, containment, eradication, system recovery, and post-incident technical review.
- **Management and Coordination Functions**: Legal risk assessment, business impact evaluation, communications management, external resource procurement, stakeholder coordination, and operational continuity oversight.
- **Executive Decision Authority**: Individuals specifically authorized to make determinations regarding technical isolation, legal and regulatory compliance, emergency procurement, insurance activation, and institutional communications and required external agency notifications.

3.2 Categorization and Prioritization of Security Incidents

[1] IR phases Referenced aligned to the NIST 800-61 rev. 2 "*Computer Security Incident Handling Guide.*"

This section will outline how security incident severity will be measured, how security incidents should be prioritized and who and when these ratings will be determined.

3.2.1 Incident Severity ratings

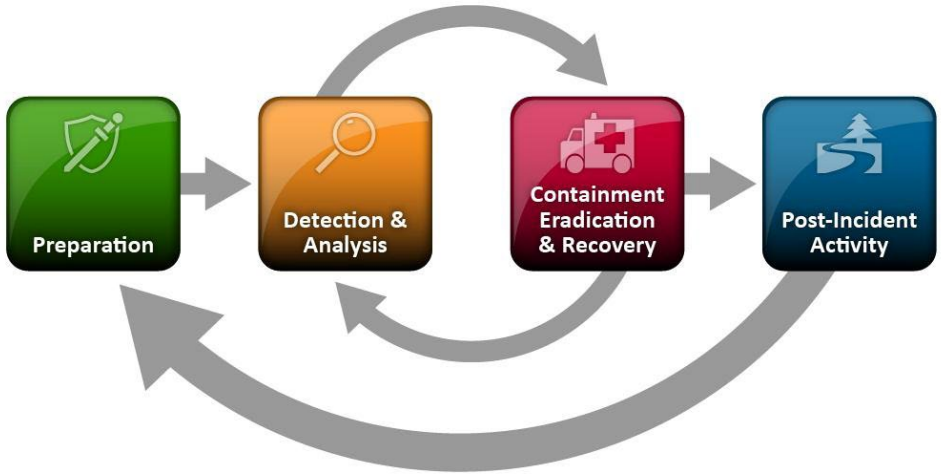
Standard: Each institution must implement and adopt a formal severity rating scale for categorizing information security incidents. The system must include at least three distinct classifications, with the severity rating criteria documented and included in the institution's incident response plan.

Section 4. Incident Response Plan Phases and Documentation Requirements

4.1 Incident Response Lifecycle

Standard: Institutional Incident Response plans shall document the plan process steps through a framework consistent with the NIST Incident Response Program Life Cycle:

1. Preparation
2. Detection and Analysis
3. Containment, Eradication, and Recovery
4. Post-Incident Activity.



4.2 External Resource Requirements for Significant Incidents

For all significant security incidents, it is presumed external resources with specific technical expertise in incident response such as a digital forensics and incident response firm (DFIR) will be required to assist with forensic analysis, root cause determination, and validate the eradication and assist in recovery processes, as well as to provide independent verification that

the incident has been properly contained and can be formally closed. Institutions should ensure that process documentation accurately reflects this presumption.

Section 5. Preparation Phase

5.1 Implement and Maintain Incident Response Procedures

Standard: Institutions must establish and maintain incident response procedures in addition to institutional IR plans. These procedures shall address all phases of the incident lifecycle phases.

5.2 Establish Secure Communications Channels

Standard: Institutional IR plans must identify and describe the availability of an alternative, out-of-band site with secure communication capabilities.

5.3 Plans and Procedures Maintenance

Standard: Institutions must review and update institutional incident response plans and procedures at least once annually. Updates shall incorporate industry best practices where feasible, internal, and external environment changes and lessons learned from prior incidents.

Section 6. Detection and Analysis

6.1 Identify and document the security event detection methods and instrumentation

Standard: Institutional IR plans shall document all security event detection methods, reporting mechanisms, and monitoring instrumentation deployed within the institutional environment.

6.2 Initial Security Event and Incident Investigation

Standard: Institutions shall establish and document clear procedures for the following:

- Initial assessment of detected security events, including personnel responsible for investigating.
- Escalation process for verified security alerts or reported incidents to Institutional IR team members.

- Formal incident designation processes and senior management notification requirements.

Section 7. Containment, Eradication and Recovery

7.1 Containment

Standard: Institutions must document their institutional strategy and or procedures for containing security incidents. This documentation must include, at a minimum:

- Specific steps and tools used for isolating affected systems and network segments or zones.
- Forensic evidence preservation and chain of custody establishment.
- In the event of a suspected account compromise, what are the immediate actions that must occur (e.g., Privilege revocation, password reset, key rotation etc.).

7.2 Eradication

Standard: Institutions must establish and document procedures for removing all elements of a security incident from the affected environment. This documentation must include:

- Institutional roles and responsibilities in coordinating with DFIR vendors during malware removal operations.
- Institution personnel necessary to perform vulnerability remediation, and removal of any persistence mechanisms used by threat actors.

7.3 Recovery

Standard: Institutions must establish and maintain documented processes for the secure reconstitution and restoration of the affected systems to known good state. The processes where feasible shall include:

- System restoration to verified secure baselines.
- For data recovery, institutions must employ versioned, immutable backups with offline storage capabilities.
- Steps for validating system integrity and security control verification.
- Approval processes and authorization protocols for DFIR-led reintroduction of systems to the production environment.

7.4 Evidence Collection

Standard: Institutions must implement measures to preserve evidence throughout the incident lifecycle, for potential forensic analysis and legal proceedings. This shall include maintaining detailed logs of all actions taken, securing copies of affected systems and data, identification of a secure storage location and establishing a clear chain of custody for all preserved evidence.

Section 8. Post Incident Activities

Standard: Institutions must document and establish a process for conducting a postmortem analysis that assesses the institution's response and captures lessons learned from the security incident and sharing identified weaknesses or deficiencies with institutional leadership.

Section 9. Definitions

Affected System: Any information system, network component, application, or data repository that has been compromised, modified, accessed without authorization, or otherwise impacted by a security incident. This includes systems that have been isolated or taken offline as part of containment efforts.

Chain of Custody: The chronological documentation showing the collection, control, transfer, analysis, and disposition of physical or electronic evidence. The chain of custody establishes proof of integrity for evidence potentially used in legal or administrative proceedings, documenting who collected the evidence, when and where it was collected, and who has had access to it.

Escalation Process: The process and/or criteria for elevating security events or incidents to appropriate institutional personnel, IR team members, or leadership based on severity, scope, or potential impact. Escalation processes can include notification chains or decision-making authority.

Information Security Incident: An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits, or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. This includes both confirmed and suspected security events that require investigation and potential response.

Security Event: Any observable occurrence in an information system or network that may indicate a possible security concern but has not been confirmed as an incident. Security events require initial assessment to determine whether they represent actual security incidents requiring full incident response procedures or are benign anomalies.

Significant Incident: A security incident of sufficient severity or scope that external specialized resources (such as DFIR firms) are required to assist with forensic analysis, root cause determination, eradication validation, and recovery processes. Significant incidents typically involve potential data breaches, widespread system compromise, or substantial operational disruption.

Other Related Information

Standards Bodies Guidance:

- NIST SP 800-61 Rev. 2: Computer Security Incident Handling Guide
- NIST SP 800-53 Rev. 5: Security and Privacy Controls for Information Systems and Organizations
- NIST Cybersecurity Framework (CSF) 2.0
- CIS Critical Security Controls v8 (Control 17: Incident Response Management)

Federal Laws:

- Federal Educational Rights and Privacy Act (FERPA) - Information available on the SUNY Compliance FERPA webpage
- Health Insurance Portability and Accountability Act (HIPAA) - Information available on the SUNY Compliance HIPAA webpage
- Gramm-Leach-Bliley Act (GLBA) - Information available on the SUNY Compliance GLBA webpage

New York State Laws:

- NYS Information Security Breach & Notification Law (General Business Law § 899-aa and State Technology Law § 208)
- NYS Stop Hacking and Improve Electronic Data Security Act (SHIELD Act)

Related Policies and Procedures

SUNY Policy Document No. 6900 - University-Wide Information Security Policy

SUNY Procedure Document No. 6610 - Legal Proceeding Preparation (E-Discovery) Procedure

SUNY Data Transparency Policy

Authority

State University of New York Board of Trustees Resolution, No. 2024-48

NYS Education Law §351, NY EDN Title 1, Article 8, §351 (State University Mission).

In case of questions, readers are advised to refer to the New York State Legislature site for the menu of the Laws of New York State.

History

Following a significant revision of the SUNY University-wide Information Security Policy in September of 2025, SUNY will be enacting a series of IT Information Security Standards. These standards are nested under Policy 6900 and provide detailed technical and operational requirements that translate policy principles into actionable institutional controls and procedures.
