Category: Information Security **Responsible Office:** Office of Information and Technology	**Policy Title:** Incident Response Policy **Document Number:** **Effective Date:** August 1, 2021 **This policy applies to:** State-Operated Campuses Community Colleges Statutory Colleges System Administration

---

Summary

The State University of New York (SUNY) Incident Response Policy is a university wide policy that establishes an Incident Response program for managing risks throughout the incident detection, response, and remediation lifecycle.

This Policy is one of seventeen policies based on the principles established by the National Institute of Standards and Technology (NIST) of the United States Department of Commerce, required by SUNY for compliance with NIST 800-53. This Policy is outlined in Special Publication (SP) 800-53 under "Incident Response (IR)" Family Guidelines pursuant to the Federal Information Security Management Act (FISMA), Public Law (P.L.) 107-347.

Each SUNY campus utilizing SUNY Information Assets, Business Systems, and Information Technology Resources must adhere to the incident response program outlined in this Policy and must develop procedures that demonstrate compliance with the standards enumerated in this Policy. This Policy serves to be consistent with best practices associated with organizational information security management.

Policy

I. Purpose

This policy establishes the SUNY Information Security Incident Response Policy. This policy is designed to support risk mitigation activities that stem from computer security incidents by establishing an Enterprise Incident Response capability. In addition, it supports the incident management program and is one of four key Enterprise IT security practices that detect, analyze, prioritize and handle Information Security Incidents which may occur within SUNY.

II. Scope

This policy is applicable to all Information Assets, Business Systems, and Information Technology Resources owned and/or operated by SUNY. Any information not specifically identified as the property of other parties, that is transmitted or stored on SUNY's IT resources (including e-mail, messages and files) is the property of SUNY. All users of IT resources, including SUNY employees, contractors, vendors or others, are responsible for adhering to this policy.

III. Incident Response Guidance

All SUNY campuses must take action to implement the Identification and Authentication steps outlined in the NIST SP 800-53 "Incident Response (IR) Family guidelines" in accordance with this Policy. All controls will be implemented in accordance with the "LOW" baseline standard.

1. Incident Response Plan: (IR-1)
2. Incident Response Training: (IR-2)
3. Incident Handling: (IR-4)
4. Incident Monitoring: (IR-5)
5. Incident Reporting: (IR-6)
6. Incident Response Assistance: (IR-7)
7. Incident Response Plan: (IR-8)

Definitions

Information Asset:

Information in this context refers to data (e.g. characters, numbers, sounds, photos, etc.) that are structured, compiled, presented, processed or otherwise organized into a format that is useful or conveys meaning. Information Assets are such bits of information that hold value—financial, intellectual, or otherwise— to SUNY.

Information Technology Resources:

Information Technology Resources are the physical, technological, communicative and related resources with which SUNY processes, stores, organizes or exchanges information and data (e.g. hardware, software or intranet).

Event and/or Transaction:

For purposes of this Policy, an "event" or "transaction," at a minimum, will always include the following:

- User Access within a Business System
- User Transactions with respect to access of Information Assets, Business Systems, and Information Technology Resources
- Any technology access events or transactions specifically designated by the Functional/Business Unit as a circumstance which rises to the level of an "event" or "transaction" worthy of documentation in the form of access logs, documented access transactions, or other access to information assets that is recorded for purposes of audit and accountability.

Responsible Office

The Mohawk Valley Community College Information Technology Procedure Policy is available at the following: MVCC Information Technology Procedures Guide

Information Technology Department, Mohawk Valley Community College

For questions or comments, submit all inquiries and requests for future enhancements to the Executive Director of Information Technology.
Attention: Director of Information Technology, Mohawk Valley Community College, 1101 Sherman Drive, Utica, NY 13501-5394

Questions may also be directed to the Information Technology Helpdesk at:

Telephone: (315) 731-5711
Email: helpdesk@mvcc.edu

Related Procedures

SUNY Procedure, Information Security Guidelines, Procedure Document 6608.

Other Related Information

Federal
NIST National Institute of Standards and Technology, U.S. Department of Commerce, Information Technology Laboratory, Computer Security Division, Computer Security Resource Center.

- NIST 800-53
  - NIST Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, Revision 4, Joint Task Force Transformation Initiative, April 2013.
    - Summary: To achieve more secure information systems and effective risk management, document provides "guidelines for selecting and specifying security controls for organizations and information systems supporting the executive agencies of the federal government to meet the requirements of Federal Information Processing Standards (FIPS)

Publication 200, Minimum Security Requirements for Federal Information and Information Systems."

- Summary of NIST SP 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, NIST Computer Security Division, February 19, 2014.
  - Summary: Provides an overview of NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, which was published April 30, 2013.
- NIST Special Publication 800-53, NIST SP 800-53 database of security controls and associated assessment procedures defined in NIST SP 800-53 Revision 4, Recommended Security Controls for Federal Information Systems and Organizations.
  - Security Controls and Assessment Procedures for Federal Information Systems and Organizations - Control Families, NIST Special Publication 800-53 (Rev. 4).
    - AC - Access Control
    - AU - Audit and Accountability
    - AT - Awareness and Training
    - CM - Configuration Management
    - CP - Contingency Planning
    - IA - Identification and Authentication
    - IR - Incident Response
    - MA - Maintenance
    - MP - Media Protection
    - PS - Personnel Security
    - PE - Physical and Environmental Protection
    - PL - Planning
    - PM - Program Management
    - RA - Risk Assessment
    - CA - Security Assessment and Authorization
    - SC - System and Communications Protection
    - SI - System and Information Integrity
    - SA - System and Services Acquisition

- NIST 800-171
  - NIST Special Publication 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations, June 2015.
- NIST 800-83 Rev 1
  - NIST Special Publication 800-83 Rev 1, Guide to Malware Incident Prevention and Handling, July 2013.
- NIST 800-61 Rev 2
  - NIST Special Publication 800-61 Rev 2, Computer Incident Handling Guide, August 2012.

New York State

- New York State Cyber Incident Reporting Procedures.

- New York State Information Technology Standard Number: NYS-S13-005, Cyber Incident Response Standard.

SUNY System Administration

- State University of New York Procedure Number: 6608, Information Security Guidelines - Campus Programs & Preserving Confidentiality.
- State University of New York Cyber Incident Reporting Procedure, update 2016

Forms

There are no forms related to this Policy.

Authority

SUNY Policy, Information Security Policy, Document 6900, Adopted by the SUNY Board of Trustees on September 14th, 2016.

History

SUNY Procedure, Information Security Guidelines, Procedure Document 6608 became effective on February 1, 2008.

Appendices

There are no appendices related to this Policy.

P-IRO-01: INCIDENTS RESPONSE OPERATIONS

Control Objective: The organization develops, implements and governs processes and documentation to facilitate the implementation of an enterprise-wide incident response policy, as well as associated standards, controls and procedures. [1]

Control: Mechanisms exist to facilitate the implementation of incident response controls.

Procedure / Control Activity: Systems Security Manager [OV-MGT-001], in conjunction with Integrated Security Incident Response Team (ISIRT) Leader [XX-CIR-002], Disaster Recovery Team Leader [XX-CON-003], Business Continuity Team Leader [XX-CON-005], Cyber Defense Incident Responder [PR-CIR-001] and Executive Cyber Leadership [OV-EXL-001]:

(1) Uses vendor-recommended settings and industry-recognized secure practices to ensure controls are sufficient for managing enterprise-wide incident response that includes:
    a. A formal, documented Incident Response Plan (IRP); and
    b. Processes to facilitate the implementation of the incident response processes and associated controls.
(2) On at least an annual basis, during the [1st, 2nd, 3rd, 4th] quarter of the calendar year, reviews the process for non-conforming instances. As needed, revises processes to address necessary changes and evolving conditions. Whenever the process is updated:
    a. Distributes copies of the change to key personnel; and
    b. Communicates the changes and updates to key personnel.
(3) If necessary, requests corrective action to address identified deficiencies.
(4) If necessary, validates corrective action occurred to appropriately remediate deficiencies.
(5) If necessary, documents the results of corrective action and notes findings.
(6) If necessary, requests additional corrective action to address unremediated deficiencies.

Control Objective: The organization regularly updates incident response strategies to keep current with business needs and technology changes. [2]

Control: Mechanisms exist to regularly update incident response strategies to keep current with business needs, technology changes and regulatory requirements.

Procedure / Control Activity: Systems Security Manager [OV-MGT-001], in conjunction with Cyber Defense Incident Responder [PR-CIR-001] and Integrated Security Incident Response Team (ISIRT) Leader [XX-CIR-002]:

(1) Implements appropriate administrative and technical means to ensure that on at least an annual basis, during the [1st, 2nd, 3rd, 4th] quarter of the calendar year, reviews:
    a. Incident Response Plans (IRPs);
    b. Results from tests and/or exercises; and
    c. After Action Reviews (AARs) from real-world incidents.
(2) As needed, revises processes to address necessary changes and evolving conditions. Whenever the process is updated:
a. Distributes copies of the change to key personnel; and
b. Communicates the changes and updates to key personnel.
(3) If necessary, requests corrective action to address identified deficiencies.
(4) If necessary, validates corrective action occurred to appropriately remediate deficiencies.
(5) If necessary, documents the results of corrective action and notes findings.
(6) If necessary, requests additional corrective action to address unremediated deficiencies.

P-IRO-13: ROOT CAUSE ANALYSIS (RCA) & LESSONS LEARNED

Control Objective: The organization incorporates lessons learned from analyzing and resolving cybersecurity and privacy incidents to reduce the likelihood or impact of future incidents.[3]

Control: Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity and privacy incidents to reduce the likelihood or impact of future incidents.

Procedure / Control Activity: Systems Security Manager [OV-MGT-001], in conjunction with Asset Owner [XX-AST-001], Cyber Defense Incident Responder [PR-CIR-001] and Integrated Security Incident Response Team (ISIRT) Leader [XX-CIR-002]:

(1) Implements appropriate administrative means to ensure every incident concludes by:
    a. Performing a Root Cause Analysis (RCA) following events that trigger usage of the Integrated Security Incident Response Team (ISIRT); and
    b. Incorporating lessons learned in updates to Incident Response Plans (IRPs).
(2) On at least an annual basis, during the [1st, 2nd, 3rd, 4th] quarter of the calendar year, reviews the process for non-conforming instances. As needed, revises processes to address necessary changes and evolving conditions. Whenever the process is updated:
    a. Distributes copies of the change to key personnel; and
    b. Communicates the changes and updates to key personnel.
(3) If necessary, requests corrective action to address identified deficiencies.
(4) If necessary, validates corrective action occurred to appropriately remediate deficiencies.
(5) If necessary, documents the results of corrective action and notes findings.
(6) If necessary, requests additional corrective action to address unremediated deficiencies.

IR-2

P-IRO-05: INCIDENT RESPONSE TRAINING

Control Objective: The organization:[1]

- Trains personnel in their incident response roles and responsibilities; and
- Provides refresher training.

Control: Mechanisms exist to train personnel in their incident response roles and responsibilities.

Procedure / Control Activity: Systems Security Manager [OV-MGT-001], in conjunction with Asset Owner [XX-AST-001], Cyber Defense Incident Responder [PR-CIR-001] and Integrated Security Incident Response Team (ISIRT) Leader [XX-CIR-002]:

1. Implements appropriate administrative and technical means to conducts periodic incident scenario sessions for personnel associated with the incident handling team to ensure that they understand current threats and risks, as well as their responsibilities in supporting the incident handling team.
2. On at least an annual basis, during the [1st, 2nd, 3rd, 4th] quarter of the calendar year, reviews the process for non-conforming instances. As needed, revises processes to address necessary changes and evolving conditions. Whenever the process is updated:
    a. Distributes copies of the change to key personnel; and
    b. Communicates the changes and updates to key personnel.
3. If necessary, requests corrective action to address identified deficiencies.
4. If necessary, validates corrective action occurred to appropriately remediate deficiencies.
5. If necessary, documents the results of corrective action and notes findings.
6. If necessary, requests additional corrective action to address unremediated deficiencies.

IR-4

P-IRO-02: INCIDENT HANDLING

Control Objective: The organization: [1]

- Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication and recovery;
- Coordinates incident handling activities with contingency planning activities; and
- Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training and testing / exercises and implements the resulting changes accordingly.

Control: Incident handling mechanisms exist to cover preparation, detection and analysis, containment, eradication and recovery.

Procedure / Control Activity: Cyber Defense Incident Responder [PR-CIR-001], in conjunction with Integrated Security Incident Response Team (ISIRT) Leader [XX-CIR-002]:

1. Leverages SUNY System Administration's Cybersecurity Incident Response Program (CIRP) to:
    a. Investigate notifications from detection systems.
    b. Identify and assess the severity and classification of incidents.
    c. Define appropriate actions to take in response to the incident, in accordance with SUNY System Administration's Incident Response Plan (IRP).
    d. Respond with appropriate remediation actions to minimize impact and ensure the continuation of business functions.
    e. As necessary, update the IRP, based on lessons learned from the incident.
2. On at least an annual basis, during the [1st, 2nd, 3rd, 4th] quarter of the calendar year, reviews the process for non-conforming instances. As needed, revises processes to address necessary changes and evolving conditions. Whenever the process is updated:
    a. Distributes copies of the change to key personnel; and
    b. Communicates the changes and updates to key personnel.
3. If necessary, requests corrective action to address identified deficiencies.
4. If necessary, validates corrective action occurred to appropriately remediate deficiencies.
5. If necessary, documents the results of corrective action and notes findings.
6. If necessary, requests additional corrective action to address unremediated deficiencies.

IR-5

P-IRO-09: INCIDENT MONITORING & TRACKING

Control Objective: The organization documents, monitors and reports cybersecurity and privacy incidents. [1]

Control: Mechanisms exist to document, monitor and report cybersecurity and privacy incidents.

Procedure / Control Activity: Systems Security Manager [OV-MGT-001], in conjunction with Systems Security Analyst [OM-ANA-001], Integrated Security Incident Response Team (ISIRT) Leader [XX-CIR-02 and Cyber Defense Incident Responder [PR-CIR-001]:

1. Implements appropriate physical, administrative and technical means to implement mechanisms to monitor for cybersecurity incidents.
2. Maintains situational awareness through aggregating and correlating event data from multiple sources and sensors:
    a. Helpdesk / service desk incidents;
    b. Security Incident Event Manager (SIEM);
    c. File Integrity Monitor (FIM);
    d. Data Loss Prevention (DLP);
    e. Intrusion Detection System / Intrusion Prevention System (IDS / IPS); and
    f. Network Access Control (NAC).
3. On at least an annual basis, during the [1st, 2nd, 3rd, 4th] quarter of the calendar year, reviews the process for non-conforming instances. As needed, revises processes to address necessary changes and evolving conditions. Whenever the process is updated:
    a. Distributes copies of the change to key personnel; and
    b. Communicates the changes and updates to key personnel.
4. If necessary, requests corrective action to address identified deficiencies.
5. If necessary, validates corrective action occurred to appropriately remediate deficiencies.
6. If necessary, documents the results of corrective action and notes findings.
7. If necessary, requests additional corrective action to address unremediated deficiencies.

IR-6

P-IRO-10: INCIDENT REPORTING

Control Objective: The organization:[1]

- Requires personnel to report suspected security incidents to organizational incident response personnel within organization-defined time-periods; and
- Reports security incident information to designated authorities.

Control: Mechanisms exist to report incidents:

- Internally to organizational incident response personnel within organization-defined time-periods; and
- Externally to regulatory authorities and affected parties, as necessary.

Procedure / Control Activity: Systems Security Manager [OV-MGT-001], in conjunction with Cyber Defense Incident Responder [PR-CIR-001] and Integrated Security Incident Response Team (ISIRT) Leader [XX-CIR-002]:

1. Leverages SUNY System Administration's Cybersecurity Incident Response Program (CIRP) to:
    a. Report actual or suspected cybersecurity incidents by:
        i. Requiring users to report system weaknesses, deficiencies, and/or vulnerabilities through appropriate management channels as quickly as possible; and
        ii. Involving management in suspected cybersecurity events quickly as possible.
    b. If a breach occurs, commence breach notification procedures without unreasonable delay, except:
        i. When a law enforcement agency has determined that notification will impede a criminal investigation; or
        ii. In order to discover the complete scope of the breach and restore the integrity of the system.
2. On at least an annual basis, during the [1st, 2nd, 3rd, 4th] quarter of the calendar year, reviews the process for non-conforming instances. As needed, revises processes to address necessary changes and evolving conditions. Whenever the process is updated:
    a. Distributes copies of the change to key personnel; and
    b. Communicates the changes and updates to key personnel.
3. If necessary, requests corrective action to address identified deficiencies.
4. If necessary, validates corrective action occurred to appropriately remediate deficiencies.
5. If necessary, documents the results of corrective action and notes findings.

If necessary, requests additional corrective action to address unremediated deficiencies

IR-7

P-IRO-11: INCIDENT REPORTING ASSISTANCE

Control Objective: The organization provides an incident response support resource that offers advice and assistance to users of systems for the handling and reporting of security incidents.[1]

Control: Mechanisms exist to provide incident response advice and assistance to users of systems for the handling and reporting of actual and potential security and privacy incidents.

Procedure / Control Activity: Systems Security Manager [OV-MGT-001], in conjunction with Asset Owner [XX-AST-001], Cyber Defense Incident Responder [PR-CIR-001] and Integrated Security Incident Response Team (ISIRT) Leader [XX-CIR-002]:

1. Implements appropriate administrative and technical means to provide an incident response support resource that offers advice and assistance to users of systems for the handling and reporting of security incidents through:
    a. Establishing a direct, cooperative relationship between its incident response capability and external providers;
    b. Identifying organizational incident response team members to work with external providers;
    c. Providing the following incident response support resources:
        i. Help desk support;
        ii. Integrated incident response teams; and
        iii. Access to forensics services.
2. On at least an annual basis, during the [1st, 2nd, 3rd, 4th] quarter of the calendar year, reviews the process for non-conforming instances. As needed, revises processes to address necessary changes and evolving conditions. Whenever the process is updated:
    a. Distributes copies of the change to key personnel; and
    b. Communicates the changes and updates to key personnel.
3. If necessary, requests corrective action to address identified deficiencies.
4. If necessary, validates corrective action occurred to appropriately remediate deficiencies.
5. If necessary, documents the results of corrective action and notes findings.
6. If necessary, requests additional corrective action to address unremediated deficiencies.

IR-8

P-IRO-04: INCIDENT RESPONSE PLAN (IRP)

Control Objective: The organization: [1]

- Develops an incident response plan that:
  - Provides the organization with a roadmap for implementing its incident response capability;
  - Describes the structure and organization of the incident response capability;
  - Provides a high-level approach for how the incident response capability fits into the overall organization;
  - Meets the unique requirements of the organization, which relate to mission, size, structure and functions;
  - Defines reportable incidents;
  - Provides metrics for measuring the incident response capability within the organization;
  - Defines the resources and management support needed to effectively maintain and mature an incident response capability; and
  - Is reviewed and approved by designated officials within the organization;
- Distributes copies of the incident response plan to incident response personnel (identified by name and / or by role) and organizational elements;
- Reviews the incident response plan on an organization-defined frequency;
- Revises the incident response plan to address system / organizational changes or problems encountered during plan implementation, execution or testing; and
- Communicates incident response plan changes to incident response personnel (identified by name and / or by role) and organizational elements.

Control: Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.

Procedure / Control Activity: Systems Security Manager [OV-MGT-001], in conjunction with Cyber Defense Incident Responder [PR-CIR-001] and Integrated Security Incident Response Team (ISIRT) Leader [XX-CIR-002]:

1. Leverages SUNY System Administration's Cybersecurity Incident Response Program (CIRP) to develop Incident Response Plans (IRPs) for situation-specific incidents.
2. Uses vendor-recommended settings and industry-recognized secure practices to ensure controls are sufficient for triaging security-related events and ensuring timely incident response actions by:
   a. Being prepared to respond immediately to cybersecurity-related incidents;
   b. Incident Response Plans (IRPs) exist for reasonably-expected situations;
   c. Testing the IRP at least annually;
   d. Designating specific personnel to be available on a 24/7 basis to respond to alerts;
   e. Providing appropriate training to staff with security breach response responsibilities;
   f. Including alerts from intrusion detection, intrusion prevention, and file integrity monitoring systems;
   g. Developing a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments;
   h. Ensuring the plan addresses the following, at a minimum:
      i. Roles, responsibilities, and communication and contact strategies in the event of a compromise;
      ii. Specific incident response procedures;
      iii. Business recovery and continuity procedures;
      iv. Data backup processes;
      v. Analysis of legal requirements for reporting compromises;
      vi. Coverage and responses of all critical system components; and
      vii. Reference or inclusion of incident response procedures from legal or contractual sources, if applicable.

3. On at least an annual basis, during the [1st, 2nd, 3rd, 4th] quarter of the calendar year, reviews the process for non-conforming instances. As needed, revises processes to address necessary changes and evolving conditions. Whenever the process is updated:
    a. Distributes copies of the change to key personnel; and
    b. Communicates the changes and updates to key personnel.
4. If necessary, requests corrective action to address identified deficiencies.
5. If necessary, validates corrective action occurred to appropriately remediate deficiencies.
6. If necessary, documents the results of corrective action and notes findings.
7. If necessary, requests additional corrective action to address unremediated deficiencies.