# Security Incident Management Policy

ROWAN UNIVERSITY POLICY

**Title:** Security Incident Management Policy
**Subject:** Information Security
**Policy No:** ISO:2013:12
**Applies:** University-Wide
**Issuing Authority:** Senior Vice President for Information Resources and Technology and Chief Information Officer
**Responsible Officer:** Chief Information Security Officer
**Date Adopted:** 07/01/2013
**Last Revision:** 02/11/2022
**Last Review:** 02/11/2022

## I. PURPOSE

The purpose of this policy is to ensure that information security incidents are reported, assessed, and mitigated to protect Rowan University's information assets.

## II. ACCOUNTABILITY

Under the direction of the President, the Chief Information Officer and the Chief Information Security Officer shall implement and ensure compliance with this policy. The Executive Vice President, Senior Vice Presidents, Vice Presidents, Deans, and other members of management shall ensure compliance with this policy and support investigations and remediation of information security events or incidents involving their respective organizations' electronic information or information systems.

## III. APPLICABILITY

This policy applies to all members of the Rowan community, including faculty, staff, non-employees, students, attending physicians, contractors, covered entities, agents of Rowan, and visitors, who have been explicitly and specifically authorized to access and use any information asset, product or service that requires processing, transmitting, or storage of Rowan data or information.

## IV.DEFINITIONS

Refer to Rowan University Technology Terms and Definitions for terms and definitions that are used in this policy.

## V. POLICY

1. The Information Security Office (ISO) will manage the Security Incident Management program at Rowan University and is responsible for developing and managing the processes, tools, and policies necessary to respond to information security incidents.
2. The Security Incident Board is responsible for monitoring and reviewing security incidents as defined in the Security Incident Management program.
3. The Security Incident Management Program must ensure documentation and training is provided to ensure that:
    a. Security incidents are handled by appropriately authorized and skilled personnel identified by their roles and responsibility on the Security Incident Response Team.
    b. Appropriate levels of university management are informed of and involved in incident response.
    c. Security incidents are recorded and documented.

d. Information is provided on the university website, and through other training and communications channels, that explains how information security incidents should be reported and encourages the reporting of all incidents whether they are actual, suspected, threatened, or potential.
e. The impact of security incidents are understood and appropriate actions are taken to prevent further damage to the university.
f. Evidence is gathered, recorded and maintained in a form that will withstand internal and external scrutiny.
g. External bodies or data subjects are informed as required.
h. Security incidents are dealt with in a timely manner and normal operations restored.
i. Security incidents are reviewed by the Security Incident Review Board to identify improvements in policies and procedures.

4. Required Reporting Actions

    a. All members of the Rowan community are responsible for promptly reporting any security event or incident to the Technology Support Center by emailing support@rowan.edu or calling 856-256-4400.
    b. Types of Security Events and or Security Incidents to report:

        i. Any security event believed to be suspicious or considered an unauthorized attempt to access, use, steal, or damage Rowan's electronic information, information systems, or information technology infrastructure. This includes anomalous computer activity, missing computer equipment, etc.
        ii. Any security incidents a member of the Rowan Community may have been made aware of through other channels, including physical letters or emails from vendors of a product(s) used by the University currently or in the past

    c. The report should include:

        i. Date of security incident
        ii. Date of discovery
        iii. Type of security incident, such as fraud, data breach/exposure, theft, malware, phishing, etc.
        iv. Estimated number of individuals impacted and/or records exposed/breached
        v. A brief description of what occurred
        vi. How you became aware of the information security incident
        vii. Any other pertinent information

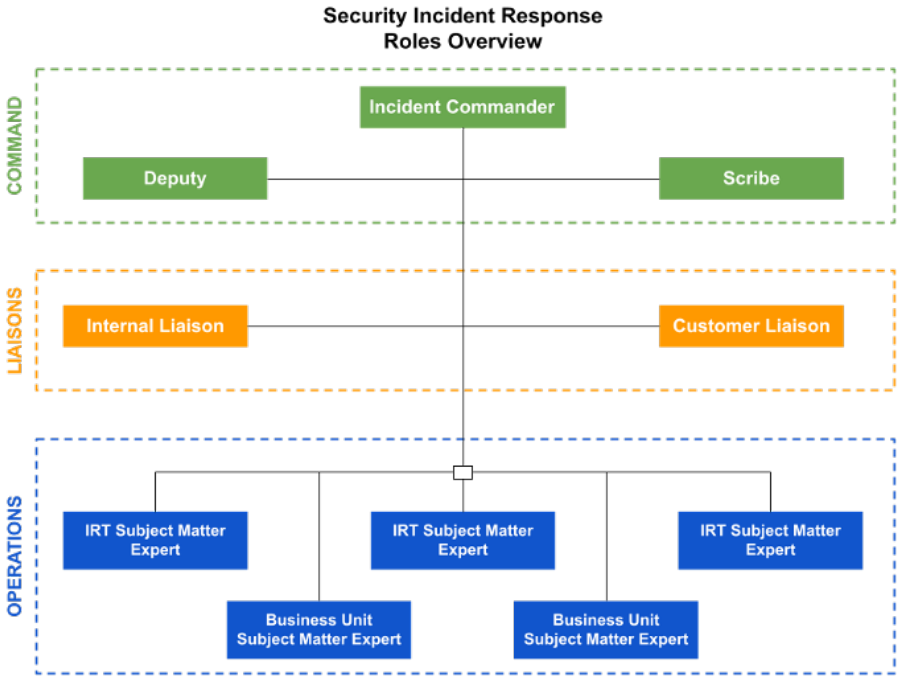
5. Response to an Information Security Incident Report

    a. The ISO has implemented a standard Security Incident Response methodology that consists of the following six sequential phases: Identify, Analyze, Contain/Mitigate, Eradicate/Remediate - Recover, and Lessons Learned. An outline of each phase is presented below.

        i. Identify: The Security Incident Response Team will review all information security reports to understand the incident and the potential impact. The Incident Response Team consists of the following key members:

            1. Incident Commander (IC)
            2. Deputy
            3. Scribe
            4. Subject Matter Expert

5. Customer Liaison/Internal Liaison




ii. Analyze: Reports that represent a risk to the University's Enterprise Information Systems or infrastructure require a response within 24 business hours by the incident response team to mitigate the risk to the University's assets, business services, and operations. Reports involving a breach of sensitive data (PHI, PII, HIPAA, FERPA, etc.) may have specific legal requirements for public announcement and reporting of the incident.
iii. Contain/Mitigate: Mitigation efforts will be made to prevent future occurrences of similar security incidents.
iv. Recover: All Security Incident Response procedures must be documented in the Rowan University Security Incident Response Management program to be reviewed and updated by the Information Security Office on an annual basis.
v. Lessons Learned: The Lessons Learned analysis provides feedback to improve the existing process and its related procedures. Following actions taken to resolve each security incident, this analysis shall be performed by the Security Incident Board, to evaluate the procedures taken and what further steps could have been taken to minimize the impact of the incident. A summary of all incidents must be presented on a quarterly basis by the CISO to the Security Incident Board.

6. Security Incident Response Stakeholder Authority and Responsibilities

a. The Security Incident Response Stakeholders includes but is not limited to ISO and IRT. Roles and responsibilities for specific groups and individuals during information security events at Rowan University are outlined below:

i. SVP and Chief Information Officer (CIO): The SVP/CIO provides information technology leadership across the entire university, advising on matters of information technology strategy, entrepreneurship, security, and investment. As necessary or appropriate, the SVP /CIO is responsible for being a conduit to other Rowan University executive officers during a suspected IT security incident.
ii. Chief Information Security Officer (CISO): The Chief Information Security Officer is the ultimate authority for interpretation and implementation of Information Security Incident Reporting, as well as for coordinating information security incident communications.

iii. Associate Director of Information Security: Serves as a backup to the Chief Information Security Officer in the event they are not available with all the same responsibilities. In addition, the Associate Director of Information Security serves as the Security Incident Response Team leader and is responsible for maintaining and reviewing the Security Incident Management program on an annual basis.
iv. Security Incident Response Team (SIRT): This team is a group of individuals who have been trained in incident management, each having distinct response roles. The team works under the direction of the Chief Information Security Officer and Associate Director of Information Security.
v. Security Incident Review Board: The Security Incident Review Board is represented by senior leadership from various campus units. The board is responsible for reviewing security incidents, how the incident was handled, and any lessons learned from the security incident. In addition, the board meets quarterly to discuss any incidents that occurred during that specific timeline and lastly the board determines whether an incident is escalated to the Cyber Insurance carrier.

## VI. POLICY COMPLIANCE

Failure to report or respond to an event or incident can expose the University to regulatory and/or statutory penalties, costly litigation, and undermine its mission and standing in the community. Violations of this policy may subject the violator to disciplinary actions up to or including termination of employment or dismissal from school, subject to applicable collective bargaining agreements and may subject the violator to penalties stipulated in applicable state and federal statutes. Students who fail to adhere to this policy or the procedures and standards will be referred to the Office of Student Affairs and may be expelled. Contractors and vendors who fail to adhere to this policy and the procedures and standards may face termination of their business relationships with the University. Sanctions shall be applied consistently to all violators identified in ***Section III Applicability*** regardless of job titles or level in the organization per the Acceptable Use Policy.

By Direction of the CIO:
Mira Lalovic-Hand,
SVP and Chief Information Officer