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: Director of Information Security
Date Adopted: 07-01-2013
Last Revision: 08/08/2018
Last Review: 08/08/2018

I. PURPOSE

To ensure that information security incidents are reported, assessed, and their harmful effects are mitigated to protect Rowan University's information.

II. ACCOUNTABILITY

Under the direction of the President, the Chief Information Officer and the Director of Information Security 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, and agents of Rowan, as well as visitors, who have been explicitly and specifically authorized to access and use the University's information systems

IV.DEFINITIONS

1. *Application* – a computer program that processes, transmits, or stores University information and which supports decision-making and other organizational functions. It typically presents as a series of records or transactions. These records and transactions are generally accessible by more than one user.
2. *Availability* – the expectation that information is accessible by Rowan when needed.
3. *Business Unit* – the term applies to multiple levels of the University, such as a revenue generating unit or a functional unit (e.g., Compliance, Human Resources, IR&T, Legal, Finance, etc.). It may also be comprised of several departments (e.g., IR&T).
4. *Confidential Information* – the most sensitive information, which requires the strongest safeguards to reduce the risk of unauthorized access or loss. Unauthorized disclosure or access may 1) subject Rowan to legal risk, 2) adversely affect its reputation, 3) jeopardize its mission, and 4) present liabilities to individuals (for example, HIPAA/HITECH penalties). See University policy, Information Classification for additional clarification.
5. *Confidentiality* – the expectation that only authorized individuals, processes, and systems will have access to Rowan's information.

6. *Directory Information* – information identified by Rowan that may be released without prior consent of the student. (See Family Educational Rights and Privacy Act policy (00-01-25-05:00) for a comprehensive list of information categorized as Directory Information.)
7. *EPHI* – electronic patient health information.
8. Information System – consists of one or more components (e.g., application, database, network, or web) that is hosted in a University campus facility, and which may provide network services, storage services, decision support services, or transaction services to one or more business units.
9. *Personally Identifiable Information (PII)* – examples include full name, personal identification number (such as Social Security number, passport number, driver's license number, taxpayer identification number, bank information, or credit card number), mailing or email address, personal characteristics (such as photographic image, fingerprints, or other biometric information), or any combination of these.
10. *Private Information* – sensitive information that is restricted to authorized personnel and requires safeguards, but which does not require the same level of safeguards as confidential information. Unauthorized disclosure or access may present legal and reputational risks to the University. See University policy, Information Classification for additional clarification.
11. *Service Desk* – the University technology service team that receives and handles requests for technical support and requests for new or changes to technology and voice services
12. *Security Event* – a possible unauthorized attempt to compromise the confidentiality, integrity, or availability of the University's electronic information or information systems. It may be a local threat that can or has evolved to present a larger risk to the University.
13. *Security Incident* – an actual or possible breach of the University's safeguards that protect its electronic information, information technology infrastructure or services, or information systems (or dependent information systems), and presents a significant business risk to the University.
14. *Sensitive Information* – protected sensitive electronic information; information classified as confidential or private (such as intellectual property or other information deemed sensitive by a department, school, or unit).
15. *SIRT* – Security Incident Response Team.

V. REFERENCES

1. Family Educational Rights and Privacy Act 00-01-25-05:00

VI. POLICY

1. Actions that may represent a risk to the University's electronic information, information systems, or information technology infrastructure require a timely response to mitigate the risk to those assets and to the University's business services and operations.
2. To assist with these efforts, all members of the Rowan community must report any computer activity they believe to be suspicious or consider an unauthorized attempt to access, use, steal, or damage Rowan's electronic information, information systems, or information technology infrastructure (this includes missing computer equipment). Such security events can potentially negatively impact the confidentiality, integrity, and/or availability of the University's electronic information and information systems and threaten its businesses and overall mission. Reporting these events helps the University assess the risk and respond accordingly.
3. Members of the Rowan community should use their best judgment and err on the side of caution when deciding whether to report activity they believe may be suspicious or that constitutes a threat to the University or their respective organization.

VII. NON-COMPLIANCE AND SANCTIONS

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. Any individual who violates this policy shall be subject to discipline up to and including dismissal from the University as well as civil and criminal penalties. Sanctions shall be applied consistently to all violators regardless of job titles or level in the organization.

VIII. ATTACHMENT

1. Attachment 1, Appendix
2. Attachment B, Reporting Suspicious Computer Activity and/or Stolen Computer Equipment
3. Attachment C, Response To Suspicious Computer Activity and/or Stolen Computer Equipment

By Direction of the CIO:

Mira Lalovic-Hand,
SVP and Chief Information Officer

ATTACHMENT 1

APPENDIX

A. Event Categorization

This list is not comprehensive and other categories may be added to help with the reporting process. Security events must be categorized according to the potential impact or threat to the confidentiality, integrity, and availability of the University's electronic information and/or information systems. Categorization is necessary in order to assess the risk to the University's business services and operations, and to determine the appropriate response.

1. Incident Types

TYPE	DESCRIPTION
Attempted Intrusion	A significant and/or persistent attempted intrusion that stands out above the daily activity and could result in unauthorized access of the target electronic information or information system.
Denial of Service	Intentional or unintentional denial of service (successful or persistent attempts) that affects or threatens to affect a critical service or denies access to all or one or more large portions of the University's network.
Malicious Code	All instances of successful infection or persistent attempts at infection by malicious code, such as viruses, Trojan horses, or worms.
Policy Violation	Access or use of the university's electronic information or information systems that violates Rowan policies and may present a risk to the University's electronic information or information systems.
Reconnaissance Activity	Instances of unauthorized port scanning, network sniffing, resourcing mapping probes and scans, and other activities that are intended to collect information about vulnerabilities in the University's network and to map network resources and available services.
Social Engineering	An instance (or instances) where an attacker uses human interaction to obtain or compromise information about the University, its personnel, or its information systems.
System Compro	

mise /Intrusion	All unintentional or intentional instances of system compromise or intrusion by unauthorized persons, including user-level compromises, root (administrator) compromises, and instances in which users exceed privilege levels.
Unautho rized Use	Any activity that is not recognized as being related to University business or normal use.

2. Incident Severity Levels

Rating the severity of an incident is a subjective measure of its threat to Rowan's operations. The severity level helps determine the priority for handling the incident, who manages the incident, and the incident response plan.
The following factors help determine severity level:

- *Scope of impact*, such as department, school or unit, campus, or University-wide.
- *Criticality* of the information system.
- *Sensitivity of the information* stored on or accessed through the system or service.
- *Probability of propagation*. Is the incident contained or can it spread beyond its current boundaries?

SEVERITY	**DESCRIPTION**
Critical	Potential operational disruption across a campus or all campuses. May have one or more of the following characteristics: • Possible breach of multiple critical information systems. • Involves a significant number of sensitive records. • May result in a breach notification to a significant number of patients, students, and/or employees. • Is likely to be the subject of national or regional press coverage. • Is likely to result in notification to a federal or state regulator. • Could otherwise negatively impact or present a significant to the University.
High	Potential operational disruption of a school or unit (e.g., Camden or SOM University Hospitals). May have one or more of the following characteristics: • Possible breach of multiple critical information systems. • Involves a significant number of sensitive records. • May result in a breach notification to a significant number of patients, students, and/or employees. • Is likely to be the subject of national or regional press coverage. • Is likely to result in notification to a federal or state regulator. • Could otherwise negatively impact or present a significant risk to the University.
Medium	Impact to a business unit that is serious and possibly results in an operational disruption. May have one or more of the following characteristics: • Is the result of malicious activity. • Could or has resulted in the breach of one or more of the business unit's critical information systems. • May result in a breach notification to a significant number of patients, students, and/or employees. • Involves a significant number of sensitive records handled by the business unit.

	• Is an unauthorized attempt to access, use, or steal sensitive records handled by the business unit.
Low	Impact to a business unit is minor and may present an operational risk if not addressed immediately. May have one or more of the following characteristics: • Is the result of intentional attempts to breach a critical information system? • Is the result of multiple SPAM or virus attacks targeting the business unit?

B. INCIDENT HANDLING AND REPORTING

The Incident Report must include:

- Name of the business unit.
- Name of the school or unit.
- Contact information of the person reporting the event (name, telephone, and email address). If the security event is an anonymous report forwarded by the Office of Ethics, Compliance and Corporate Integrity, use the name of the compliance officer who sent the report.
- Physical location of the affected information system.
- The classification of the information, i.e., confidential, private, internal, or public.
- The type of information, such as, EPHI, student information, or financial information.
- Date and time when the suspicious activity was detected.
- Date and time when the suspicious activity was reported.
- Incident type and severity level. This information may change during the course of an investigation, and initially only reflects the assessment at the time of detection and reporting. The SIRT will update this information during the course of the investigation.
- Suspected method of intrusion or attack.
- Suspected origin or cause of event or incident.
- Remediation methods.

Lessons Learned

Prepare a Lessons Learned report for incidents. The report must include the standard incident report information and establish the steps necessary to prevent or limit the risk of the incident recurring. The report shall be submitted to the Chief Information Officer, the Office of Ethics, Compliance and Corporate Integrity, and the Office of Legal Management. The report may be submitted to other University entities when necessary.

ATTACHMENT 2

REPORTING SUSPICIOUS COMPUTER ACTIVITY and/or STOLEN COMPUTER EQUIPMENT

A. Users

1. If they detect a security breach or believe computer activity to be suspicious, and/or computer equipment (including mobile devices and removable media) is missing, users must report it to their manager or other managerial authority in their organization.
2. Theft of computer equipment must also be reported to Public Safety and the Information Security Office (ISO).

B. Managers

1. On notification of the activity or theft, managers must contact their local compliance officer and the ISO to initiate an assessment of the activity and/or initiate an investigation of the missing equipment.
2. If student information is potentially involved, managers must also contact their local Registrar office.

C. Communications and Assessment

1. Coordination and Compliance Assessment
    a. The Office of Ethics, Compliance and Corporate Integrity is the lead assessor for all reports of suspicious activities and/or missing computer equipment. They will coordinate and manage the communications amongst all parties involved with response to the event.
2. Information Security Risk Assessment
    a. The Information Security Office (ISO) will assess if the event presents a larger security risk to the University's electronic information, information systems, or information technology infrastructure across a campus (or campuses).

ATTACHMENT 3

RESPONSE TO SUSPICIOUS COMPUTER ACTIVITY and/or STOLEN COMPUTER EQUIPMENT

A. Response

1. To assist Compliance with the investigation and respond to reports of suspicious activity, Compliance may request the services of Public Safety, the Office of Legal Management, the Information Security Office.
2. The Office of Legal Management is to be informed of suspected data breaches to ensure the timely and appropriate engagement of the University's risk mitigation partners and service providers.
3. The Information Security Office and IRT management will keep the SIRT apprised of any reports that involve potential threats to the University's information technology infrastructure, services, and dependent information systems across the campus.
4. Security Incident Response Team
    a. Consists of representatives from the Information Security Office, IRT, Office of Emergency Management, Office of Legal Management, Office of Ethics, Compliance and Corporate Integrity, and Department of Public Safety.
    b. Members of other Rowan organizations may become engaged in the incident response, depending on its categorization.

B. Incident Categorization

Security incidents must be categorized according to the standards listed in the appendix. Categorization is necessary in order to uniformly assess the risk to the University's operations and determine the appropriate response.

C. Incident Handling And Reporting

1. Investigation Timeframe
    a. Management personnel, technology personnel, and security response teams must begin investigating a reported event within 24 hours of the initial report of suspicious activity.
    b. The Office of Ethics, Compliance and Corporate Integrity must be informed of suspicious activity related to EPHI.
    c. The local Registrar office must be informed of suspicious activity related to education records.
2. The Incident Report must include the elements listed in the appendix.
3. Lessons Learned

Prepare a Lessons Learned document for incidents. The document must include the standard

incident report information and establish the steps necessary to prevent or limit the risk of the incident recurring.

4. Record Retention
   Prepare and retain documentation for all evaluations of suspicious activity and incidents. See the Requirements section for additional information about record retention.

D. Requirements

1. Communications
   a. All communications (electronic or physical documents) related to suspicious activity or actual events and incidents must be retained according to legal requirements and the University's records management requirements.
   b. Communications that may affect the integrity of an investigation are not to be destroyed or altered in any manner.
2. Physical Assets
   a. Hardware
   b. Hardware related to an investigation of suspicious activity and that may affect the integrity of an investigation is not to be destroyed or altered in any manner.
   c. Documents
      i. Physical and electronic documents related to an investigation of suspicious activity that may affect the integrity of an investigation are not to be destroyed or altered in any manner.
      ii. Physical and electronic documents must be retained according to legal requirements and the University's records management requirements.

E. Key Responsibilities

1. The Director of Information Security shall develop, implement, and maintain an Information Security Incident Response Plan. The plan will support the Office of Ethics, Compliance and Corporate Integrity Data Breach Policy and Response Plan.
2. Users shall:
   a. Report to their manager or other managerial authority (within 24 hours of detection) any computer activity they believe is suspicious or outside the normal course of business, regardless if conducted by an outside person or member of the Rowan community.
   b. Report to their manager or other managerial authority and to Public Safety (within 24 hours of detection) the loss or theft of computer equipment and/or electronic storage media such as USB drives, disks, etc.
3. Department managers and supervisors shall immediately:
   a. Report to their local compliance officer or the Office of Ethics, Compliance and Corporate Integrity reports of suspicious activity or loss or theft of computer equipment.
   b. Report to their school's dean or unit's Vice President suspicious activity that potentially presents a risk to their organization and to the University.
   c. Report suspicious activity involving education records to the local Registrar office.
4. Office of Ethics, Compliance and Corporate Integrity shall:
   a. Coordinate the reporting of and response to reports of suspicious activities, including those involving the loss or theft of computer equipment.
   b. Assess and determine (along with the Office of Legal Management) the classification (e.g., Confidential, Private) and type (e.g., EPHI, PII) of information involved.
   c. Collect from each Rowan organization assisting with the response all information related to the issue reported.
5. The Information Security Office (ISO):

a. Assess the information and technology risks to the University's electronic information, information systems, and information technology infrastructure.
b. Report to the SIRT any technology risks that may impact the University's business services and operations across a campus (or campuses).
c. Remediate technology risks as deemed appropriate to secure the operations of the University.
d. Document lessons learned.

6. The ISO and the Office of Legal Management shall engage risk mitigation service partners as appropriate.