RUTGERS
THE STATE UNIVERSITY
OF NEW JERSEY

RUTGERS POLICY

Section: 70.1.3

Section Title: Information Technology

Policy Name: Incident Management

Formerly Book: N/A

Approval Authority: Senior Vice President for Administration

Responsible Executive: Vice President for Information Technology & Chief Information Officer

Responsible Office: Office of Information Technology (OIT)

Originally Issued: 10/8/2014

Revisions:

Errors or changes? Contact: oitpolicy@rutgers.edu

1. Policy Statement

This policy establishes responsibility and accountability for ensuring that security incidents are identified, contained, managed, investigated, and remediated.

2. Reason for Policy

To establish the requirement that all business and academic units manage security incidents appropriately.

3. Who Should Read This Policy

Parties with major responsibilities include Vice Presidents, Chancellors, Deans, Information Owners (data custodians), Information Managers and Information Users. This policy applies to all members of the University community including faculty, staff, students, covered entities, contractors, non-employees, and agents of the University.

4. Related Documents

Records Management, 30.4.5
Payment Card Acceptance Policy, 40.2.15
Copyright Policy, 50.3.7
Safeguarding Personal Information; Identity Theft Compliance Policy, 50.3.9
Gramm-Leach-Bliley Act (GLBA) Information Security Policy, 50.3.11
Red Flag Detection and Reporting Policy, 50.3.12
Acceptable Use Policy for Computing and Information Technology Resources, 70.1.1
Information Classification, 70.1.2
Protected Health Information Breach Notification 100.1.5
Rutgers Minimum Security Standards for Data Protection:
https://rusecure.rutgers.edu

5. Contacts

Information Protection and Security (IPS), Office of Information Technology (OIT)
848-445-8011
http://rusecure.rutgers.edu
abuse@rutgers.edu

6. The Policy

70.1.3 INCIDENT MANAGEMENT

A. Introduction:

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.

To assist with these efforts, all members of the Rutgers community must report any suspicious activity, unauthorized access, and missing or stolen equipment. In addition, any damage to Rutgers' electronic information, information systems, or the information technology infrastructure which includes data services or cloud providers must also be reported. Such security events can negatively impact the confidentiality, integrity, and/or availability of the University's electronic information and information systems and threaten its businesses and overall mission.

B. Requirements

1. Chancellors, Vice President for Information Technology & Chief Information Officer, Executive Vice President, Senior Vice Presidents, Vice Presidents, and Deans must:

a. Ensure the implementation of this policy by the organizations under their purview.

b. Ensure the support of investigations and remediation of information security events or incidents involving their organizations.

2. Deans, Directors and Department Chairs must:

a. Ensure that each business unit in their respective areas of oversight report security incidents in a timely manner. Unauthorized use, disclosure, loss or theft of Restricted or Internal information must be reported immediately.

b. Ensure that each business unit in their respective areas of oversight report incidents involving Protected Health Information (PHI) or if there is likelihood that PHI data is involved to the Office of Enterprise Risk Management, Ethics and Compliance (1-800-215-9664).

c. Ensure that each business unit in their respective areas of oversight report loss or theft of physical assets to University Police.

d. Ensure that each business unit in their respective areas of oversight develop, implement, and maintain a departmental Information Security Incident Response Plan and ensure that departmental personnel are aware of and understand the plan.

e. Ensure that each business unit in their respective areas of oversight maintain their network and abuse contact information.

f. Ensure that the departments respond and remediate security incidents reported by IPS within the required time constraints.

3. All users must

a. Report unauthorized use, disclosure, loss or theft of Restricted or Internal information immediately. The following steps must be taken:

i. Immediately report the unauthorized disclosure, loss, theft, or access of information to IPS and your departmental management.

ii. If PHI or a likelihood that PHI data is involved, call the Office of Enterprise Risk Management, Ethics and Compliance (1-800-215-9664).

iii. Report loss or theft of physical assets to University Police. If PHI or a likelihood that PHI data is involved, call the Office of Enterprise Risk Management, Ethics and Compliance.

b. Must become familiar and follow appropriate departmental Information Security Incident Response Plan.

c. Maintain confidentiality and share information on a need-to-know basis.

4. **Office of Enterprise Risk Management, Ethics and Compliance must**:

a. Coordinate the reporting of and response to reports of suspicious activities regarding PHI, including those involving the loss or theft of computer equipment as described in Rutgers policy 100.1.5, Protected Health Information Breach Notification.

b. Collect from each Rutgers organization assisting with the response all information related to the issue reported.

5. Information Protection Evaluation Team (IPET) must:

a. Coordinate the reporting of and response to reports of suspicious activities regarding Non-Public Personal Information (NPPI) as described in Rutgers policy 50.3.9, Safeguarding Personal Information**;** Identity Theft Compliance Policy.

b. Collect from each Rutgers organization assisting with the response all information related to the issue reported.

6. Treasury Operations must:

a. Coordinate the reporting of and response to reports of suspicious activities regarding Payment Card Industry (PCI) as described in Rutgers policy 40.2.15 Payment Card Acceptance Policy. Information including those involving the loss or theft of computer equipment.

b. Assess and determine the classification (e.g., Restricted or Internal) and type (e.g., PCI) of information involved.

c. Collect from each Rutgers organization assisting with the response all information related to the issue reported and document in accordance with PCI DSS requirements; Departmental Information Security Incident Response Plan.

7. Information Protection and Security must:

a. Forward incident reports to departments within one business day.

b. Advise departments on creation of security incident response plans.

c. Provide guidance for recovery and remediation.

d. Coordinate with other University organizations such as the Office of Enterprise Risk Management, Ethics and Compliance; University Police, Office of General Council, Information Protection Evaluation Team, Treasury Operations and others as appropriate.

e. Conduct Forensic investigations at the direction of the organizations identified in section (D), as appropriate.

C. Non-Compliance and Sanctions:

Failure to comply with this policy may result in denial or removal of access privileges to the University's electronic systems, disciplinary action under applicable University policies and procedures, civil litigation, and/or civil or criminal prosecution under applicable state and federal statutes.