RUTGERS
THE STATE UNIVERSITY OF NEW JERSEY

UNIVERSITY POLICY

Policy Name:	Incident Management					
Section #:	70.1.3	**Section Title:**	Information Technology: Information Technology Policies		**Formerly Book:**	00-01-95-15:10 (Legacy UMDNJ)
Approval Authority:	Executive Vice President – Chief Financial Officer and University Treasurer		**Adopted:**	10/08/2014	**Reviewed:**	04/12/2021
Responsible Executive:	Senior Vice President & Chief Information Officer		**Revised:**	04/12/2021		
Responsible Office:	Office of Information Technology (OIT)		**Contact:**	oit-policies@oit.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**

   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. **Resources**

   University Policy 30.4.5: Records Management

   University Policy 40.2.15: Payment Card Acceptance Policy

   University Policy 50.3.7: Copyright Policy

   University Policy 50.3.11: Gramm-Leach-Bliley Act (GLBA) Information Security Policy

   University Policy 50.3.12: Red Flag Detection and Reporting Policy

   University Policy 50.3.18: Data Breach Management

   University Policy: Information Technology - Section 70

University Policy 70.1.1: Acceptable Use Policy for Information Technology Resources

University Policy 70.1.2: Information Classification

Rutgers Minimum Security Standards for Data Protection

5. **Definitions**

Availability - The expectation that information is accessible by the University community when needed.

Confidentiality - The state of keeping information and/or materials private, with only authorized individuals, processes, and systems having access to view, use, or share.

Guidelines - Advice on the ways to comply with policy, written for non-technical users who have multiple options for secure information handling processes.

Integrity - The expectation that the University's information will be protected from intentional, unauthorized, or accidental changes.

Procedures - Step by step instructions and implementation details for personnel to perform specific tasks in ways that ensure the associated preventive, detective, and/or response mechanisms work as planned.

Technology standards - Established requirement of technical configuration parameters and associated values to ensure management can secure University assets and comply with University policy and regulatory requirements when accessing University information.

6. **The Policy**

A. **Introduction:**

Actions that may represent a risk to the University's electronic information, information systems, payment account acceptance, and processing methods 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. **Executive/Senior/Vice Presidents, Chancellors, 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.

c. Establish, maintain, and disseminate documentation, such as Technology Standards, Procedures, and/or Guidelines, to ensure compliance as stated in this Policy.

2. **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 Critical or Restricted information is a potential data breach and needs to be managed via University Policy 50.3.18: Data Breach Management.

b. Any unauthorized use, disclosure, loss, or theft of Critical or Restricted information is to be reported to the University Ethics and Compliance Office.

c. Ensure that each business unit in their respective areas of oversight report loss or theft of physical assets to the 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, including identification of causes and resolution of weaknesses that may have led to the incident, and ensure that departmental Supervisors and IT support staff are aware of and understand the plan.

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

f. Ensure that the departments respond and remediate security incidents reported by IT Risk, Policy and Compliance within the required time constraints.

g. Establish, maintain, and disseminate documentation, such as Technology Standards, Procedures, and/or Guidelines, to ensure compliance as stated in this Policy.

3. **All users must**

a. Report any suspected unauthorized use, disclosure, loss, or theft of Critical, Restricted, or Internal information immediately to their Supervisor and their IT support staff.

b. Maintain confidentiality of incidents in or pertaining to the University and share information only with their Supervisor and IT support staff.

4. **IT Risk, Policy and Compliance must:**

a. Receive and forward incident reports regarding University computers to departments within one business day.

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

c. Establish, maintain, and disseminate documentation, such as Technology Standards, Procedures, and/or Guidelines, to ensure compliance as stated in this Policy.

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.