RUTGERS
THE STATE UNIVERSITY OF NEW JERSEY

UNIVERSITY POLICY

Policy Name:	Information Security Awareness, Training, and Education					
Section #:	70.1.4	**Section Title:**	Information Technology: Information Technology Policies		**Formerly Book:**	00-01-95-15:15 (Legacy UMDNJ)
Approval Authority:	Executive Vice President – Chief Financial Officer and University Treasurer		**Adopted:**	07/01/2013	**Reviewed:**	03/31/2021
Responsible Executive:	Senior Vice President and Chief Information Officer		**Revised:**	10/10/2013 (Updated title); 10/08/2014; 03/31/2021		
Responsible Office:	Office of Information Technology (OIT)		**Contact:**	oit-policies@oit.rutgers.edu		

1. **Policy Statement**

This policy establishes the requirement for Information Security Awareness Training for all members of the Rutgers, The State University of New Jersey community who have access to the University's information systems and to information classified as "Critical" or "Restricted" in accordance with the University's security and privacy policies, State and federal laws, and expectations before access to information or services is granted. Applicable laws include but are not limited to the Gramm-Leach-Bliley Act (GLBA), Health Insurance Portability and Accountability Act (HIPAA), Federal Information Security Management Act (FISMA), and Payment Card Industry Data Security Standards (PCI-DSS).

2. **Reason for Policy**

To ensure that the University community is informed and trained on the need for information security and in proper procedures for handling information classified as "Critical" or "Restricted" and the actions to be taken to maintain security and respond to suspected security incidents.

3. **Who Should Read This Policy**

This policy applies to all members of the University community.

4. **Resources**

University Policy: Information Technology - Section 70

University Policy: Clinical, Compliance, Ethics & Corporate Integrity – Section 100

University Policy 70.1.2: Information Classification

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 70.1.3: Incident Management

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.

Privileged Account - A user that is authorized (and therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform. Source: National Institute of Standards and Technology Computer Security Resource Center (NIST CSRC)

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

Technology standards - Established requirement of technical configuration parameters and associated values to ensure that management can secure University assets and comply with University policy and regulatory requirements relating to the secured access of University information.

6. **The Policy**

A. **Introduction:**

Access to the University's information technology resources is a privilege that requires all individuals with access to Critical or Restricted data to act responsibly and guard against abuses. Therefore, both the community as a whole and each individual user have an obligation to abide by the following requirements and responsibilities:

B. **Requirements:**

1. **Executive/Senior/Vice Presidents, Chancellors and Deans must:**
   a. establish, maintain, and disseminate documentation such as Technology Standards,

Procedures, and/or Guidelines to ensure compliance as stated in this Policy for the organizations under their purview

b. ensure that all members of the University community under their purview, including third party stakeholders (business associates, partners, contractors), that have access to Critical or Restricted data or Privileged Access complete the assigned Security Awareness Training (SAT) upon arrival at the University and the annual refresher thereafter.

2. **Directors and Department Chairs** must ensure that business units, schools, and departments, including third party stakeholders (business associates, partners, contractors), under their purview that have access to Critical or Restricted data complete Security Awareness Training (SAT) upon arrival at the University and the annual refresher thereafter.

3. **Users with access to University Information Technology Systems, information classified as "Critical" or "Restricted," or with Privileged Access must:**

a. complete all assigned training related to Information Security Awareness, as well as all mandatory, annual training courses as provided by the University;

b. adhere to all assigned and mandatory training related to Information Security Awareness as provided by the University; and

c. follow all of the University's applicable Information Technology policies, procedures, technical standards, and guidelines.

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

a. implement, maintain, and provide on-going information technology security awareness, training and education using various techniques such as awareness sessions, training, newsletter articles, email communication campaigns, and intranet website;

b. review the annual security awareness training content, working with all other relevant parties, to update training content as it pertains to Information Security Awareness topics;

c. provide an activity report to the Senior Vice President and Chief Information Officer, upon request.

5. **University Ethics and Compliance (UEC)** must**:**

a. establish and maintain the University's Security Awareness Training (SAT) program working with all other relevant parties to ensure appropriate content to communicate the aim of information security and the potential impact on the University based on user behavior;

b. ensure SAT is assigned to all members of the University community with access to the University's information technology resources or with access to Critical or Restricted data or with Privileged Access upon their arrival at the University or with a job function change and at least yearly thereafter;

c. review the annual SAT content, working with all other relevant parties, to update training content as it pertains to Compliance topics.

6. **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.

EXHIBIT

External References

Public Standards for IT Security Awareness and Training

Standard	Industry	Country	Awareness/Training Requirement
ISO/IEC Standard 27002:2013, "Information technology-Security techniques-Code of practice for information security controls"	Engineering	Int'l	Section 7.2.2 Information security awareness, education, and training: All employees of the organization and where relevant, contractors, should receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.
FISMA (Federal Information Security Management Act) NIST 800-53	Government Information, Operations and Assets	USA	Awareness Training (AT1) The organization develops, documents, and disseminates: a) a security awareness and training policy that addresses purpose, scope, roles, responsibilities, management, commitment, coordination among organizational entities, and compliance; and b) procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls.
HIPAA (Health Insurance Portability and Accountability Act of 1996)	Healthcare	USA	Security Final Rule 164.308 (a)(5)(i) (R) Implement a security awareness and training program for all members of its workforce (including management).
National Institute of Standards and Technology Special Publications 800-50 (October 2003) and 800-53a (July 2008) 800-16 Revision 1 (March 2009)	Engineering	USA	SP 800-16 Rev-1 Section 3.1 - To ensure that users of information and information systems understand the core set of key terms and essential information security concepts that are fundamental for the protection of information and information systems.