RUTGERS
THE STATE UNIVERSITY
OF NEW JERSEY

RUTGERS POLICY

Section: 70.1.4

Section Title: Information Technology

Policy Name: Information Security Awareness, Training and Education

Formerly Book: N/A

Approval Authority: Senior Vice President for Administration

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

Responsible Office: Office of Information Technology (OIT)

Originally Issued: July 1, 2013

Revisions: Originally 00-01-95-15:15 at UMDNJ; 10/10/2013 (Updated title); 10/8/2014

Errors or changes? Contact: oitpolicy@rutgers.edu

1. **Policy Statement**
   This policy establishes the requirement for Information Technology (IT) Security Awareness, Training and Education for members of the Rutgers, The State University of New Jersey, community who have access to the University's information systems and restricted data in accordance with Gramm-Leach-Bliley Act (GLBA) and PCI (Payment Card Industry) and Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 (HIPAA) laws.

2. **Reason for Policy**
   To ensure that the University community is properly informed and trained on information security and in handling restricted data according to its value, legal requirements, sensitivity, and criticality to the University.

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**
   Information Classification, 70.1.2

   See EXHIBIT for external references

5. **Contacts**
   oithelp@rutgers.edu

6. **The Policy**

70.1.4 INFORMATION SECURITY AWARENESS, TRAINING AND EDUCATION

A. Introduction:

Access to the university's information technology resources is a privilege that requires each member with access to 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. Vice Presidents, Chancellors and Deans:

a. Ensure that members of the Rutgers community that have access to restricted data complete Security Awareness Training (SAT) upon arrival at Rutgers.
b. Ensure that members of the Rutgers Community that have access to restricted data complete the annual refresher training course.

2. Information Users with access to restricted data:

a. Responsible to complete the annual training course Information Security Awareness training and education provided by Rutgers.
b. Responsible for adhering to the Information Security Awareness Training and Education provided by Rutgers.
c. Responsible to follow Rutgers's Information security policies.

3. The Information Protection and Security (IPS):

a. Responsible for implementing, maintaining, and providing on-going information technology security awareness, training and education using various techniques such as awareness sessions, training, newsletter articles, email and an intranet website.
b. Reviewing the annual security, awareness training content.
c. Responsible for providing an annual activities report to the Vice President for Information Technology and Chief Information Officer, upon request.

.

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.

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.
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.