Section: 70.2.4  70.1.4

Section Title: Legacy UMDNJ policies associated with Information Technology 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 information assets in accordance with Family Educational Rights and Privacy Act (FERPA) and Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 (HIPAA) laws, 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 set a requirement for the education and training of University personnel related to Information Security. 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
This policy applies to any individual responsible for the management, operation, and/or maintenance of the legacy UMDNJ information technology services and/or environment. If you are uncertain whether this policy applies to you, please contact your direct supervisor. 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
N/A Information Classification, 70.1.2

See EXHIBIT for external references

5. Contacts
oit@rutgers.edu

6. The Policy

70.2.4 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:

I. Requirements:

A.—— The Information Security Office (ISO) will provide Information Security
Awareness, Training and Education for members of the Rutgers community.

B.—— Members of the Rutgers community that will have access to information assets
must complete Security Awareness Training (SAT) upon arrival at Rutgers.

C.—— Members of the Rutgers community that will have access to information assets
must annually complete refresher training.

D.—— Security, awareness and training content must be reviewed annually by ISO.

E.—— The ISO will provide an annual activities report to the Vice President for
Information Technology and Chief Information Officer.

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.

II. Responsibilities:

A. Vice Presidents, Chancellors, Presidents of Healthcare Units and Deans shall ensure each member of the Rutgers community has completed the Security Awareness Training.

B. The Information Security Office (ISO) is 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.

III. Non-Compliance and Sanctions

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.
## External References

### Public Standards for IT Security Awareness and Training

<table>
<thead>
<tr>
<th>Standard</th>
<th>Industry</th>
<th>Country</th>
<th>Awareness/Training Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO/IEC Standard 27002:2005, “Information technology – Security techniques – Code of practice for information security management”. First edition 2005-06-15</td>
<td>Engineering</td>
<td>Int’l</td>
<td>Section 8.2.2 7.2.2 Information security awareness, education, and training: All employees of the organization and, where relevant, contractors and third-party users should receive appropriate awareness and training and regular updates in organizational policies and procedures, as relevant for their job function.</td>
</tr>
<tr>
<td>HIPAA (Health Insurance Portability and Accountability Act of 1996)</td>
<td>Healthcare</td>
<td>USA</td>
<td>Security Final Rule 164.308 (a)(5)(i) (R) Implement a security awareness and training program for all members of its workforce (including management).</td>
</tr>
<tr>
<td>National Institute of Standards and Technology Special Publications 800-50 (October 2003) and 800-53a (July 2008) 800-16 Revision 1 (March 2009)</td>
<td>Engineering</td>
<td>USA</td>
<td>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.</td>
</tr>
<tr>
<td>Family Educational Rights and Privacy Act of 1974</td>
<td>Education</td>
<td>USA</td>
<td>Faculty, staff, and students who have access to protected records will be required to complete training as appropriate.</td>
</tr>
</tbody>
</table>

All regulations and procedures are subject to amendment.