1. General Policy .................................................................................................................. 3
2. Policy on Sensitive Information ..................................................................................... 4
3. Information Classification .............................................................................................. 5
4. Roles and Responsibilities ............................................................................................... 6
5. Mission-Critical Resources ............................................................................................ 8
7. Policy Review and Adoption .......................................................................................... 10
Appendices ......................................................................................................................... 11
   8.1. Information Security Procedures ............................................................................. 11
   8.2. Information Security Standards .............................................................................. 18
INFORMATION SECURITY POLICY

Title: Information Security Policy
Subject: Information Security
Policy No: ISO: 2013:01
Applies: University-wide
Issuing Authority: Vice President for Information Resources and Chief Information Officer
Responsible Officer: Vice President for Information Resources and Chief Information Officer

Date Adopted: 12-02-2013
Last Revision: 12-02-2013
Last Review:

1. General Policy Statement

All University faculty, students, staff, temporary employees, contractors, outside vendors and visitors to campus who have access to University-owned or managed information through computing systems or devices ("Users") must maintain the security of that information and those systems and devices.

Basic “minimum” requirements apply to all University-owned or managed information and systems and devices. These can be found in the attached Information Security Standards.

More extensive requirements apply to Sensitive Information and Mission-Critical Resources. These are discussed below and in the Procedures and Standards documents, which are found in the attached Information Security Procedures and Information Security Standards.

These Policies, Procedures, and Standards may be amended from time to time. Users will be notified of amendments through campus-wide email messages and announcements on the web site for Information Technology Services.

Scope

This policy and the related Procedures and Standards set forth security practices necessary to protect the ROWAN network and information. This policy does not supersede any applicable state or federal laws regarding access to or disclosure of information.

Audience

This policy applies to all Users accessing the ROWAN network or ROWAN information through computing devices owned by or managed through ROWAN or through permission granted by ROWAN. All Users must read this Policy Statement and the related Procedures and Standards in their entirety. If you have any questions about whether this Policy Statement applies to you or how it applies to you, please contact the Information Security Office at 856-256-4498.
Compliance

Failure to adhere to this Policy and the Procedures and Standards may put University information assets at risk and may have disciplinary consequences for employees up to and including termination of employment. Students who fail to adhere to this Policy or the Procedures and Standards will be referred to the Office of Student Affairs and may be expelled. Contractors and vendors who fail to adhere to this Policy and the Procedures and Standards may face termination of their business relationships with the University.

2. Policy on Sensitive Information

Sensitive Information, as defined below, in all its forms – written, spoken, electronically recorded, or printed – must be protected from accidental or intentional unauthorized modification, destruction, or disclosure. This policy statement addresses specifically the risks to privacy inherent in digital technologies.

The University requires all Users to protect the University’s Sensitive Information by adhering to the attached Procedures and Standards as they may be amended from time to time.

Users with access to Sensitive Information must adhere to all Information Security Policies, Procedures, and Standards including, but not limited to the following:

• Acceptable Use Policy
• Access Control Policy
• Incident Management Policy
• Mobile Computing and Removable Media Policy
• Remote Access Policy
• Workstation Use Policy
• General User Password Policy
• Policy and Standards for Electronic Media Disposal
• Policy on the Transmission of Sensitive Information (including PHI or PII)
• Protocol for Responding to Security Breaches of Sensitive Information (including PHI and PII)

Users who are third-party contractors and vendors must be made aware of this policy and their responsibilities for safeguarding the University’s Sensitive Information.

Sensitive Information includes all data, in its original and duplicate form, which contains:

• “Personal Identifying Information or PII,” as defined by the New Jersey Identity Theft
Protection Act. This includes employer tax ID numbers, drivers' license numbers, passport numbers, SSNs, state identification card numbers, credit/debit card numbers, banking account numbers, PIN codes, digital signatures, biometric data, fingerprints, passwords, and any other numbers or information that can be used to access a person's financial resources.

- “Protected Health Information or PHI” as defined by the Health Insurance Portability and Accountability Act (HIPAA).

- Student “education records,” as defined by the Family Educational Rights and Privacy Act (FERPA).

- “Customer record information,” as defined by the Gramm Leach Bliley Act (GLBA).

- “Card holder data,” as defined by the Payment Card Industry (PCI) Data Security Standard.

- Information that is deemed to be confidential in accordance with the New Jersey Public Records Act. Sensitive Information also includes any other information that is protected by University policy or federal or state law from unauthorized access.

Sensitive Information must be restricted to those with a legitimate business need for access. Examples of Sensitive Information may include, but are not limited to, Social Security numbers, system access passwords, some types of research data (such as research data that is personally identifiable or proprietary), public safety information, information concerning select agents, information security records, and information file encryption keys.

3. Information Classification

All Users must be aware of the classification of the various types of University information to which they have access in order to determine the proper controls for safeguarding the information. Regardless of classification, the integrity and accuracy of all information must be protected. Information must be classified according to the most sensitive detail it includes. Information recorded in several formats (e.g., source document, electronic record, printed report) must have the same classification regardless of format. Only two levels are to be used when classifying information:

(A) **Sensitive Information**: “Sensitive Information” is defined above. It is important to note that the unauthorized disclosure of Sensitive Information to individuals without a business need for access may violate laws or University policies and may have significant ramifications for the University, its employees, its students, or its business associates.

Decisions about the provision of access to Sensitive Information must always be made by the Steward (as defined below) of that Sensitive Information.

(B) **Public Information**: Public Information includes all information made or received by the University that does not constitute Sensitive Information. Sensitive Information that is disclosed without proper authorization does not, by virtue of its disclosure, become Public Information.

Many Users will find that some of the information to which they have access has been classified as Sensitive Information (e.g., employment records, student records) and some of it as Public
Information (e.g., most purchase contracts, most accounting records).

4. Roles and Responsibilities

In addition to knowing the classification of each piece of University information to which they have access as either “Sensitive Information” or “Public Information,” Users must be aware of whether, with respect to that information, they serve as a Steward, a Custodian, a Consumer/User, a User Manager, or an Information Security Liaison, as described within this Policy.

**Steward of Information or Data:** The Steward is the University employee responsible for the approval of the creation of a collection of information or data or the primary user of that information or data. For example, the Registrar is the Steward for much of the University’s student information. The Vice President for Human Resources is the Steward for much of the University’s employee information.

**Custodian of Information or Data:** The Custodian is responsible for the processing and storage of information or data on behalf of the Steward of that information or data.

**Consumer/User:** A Consumer/User is any person authorized to read, enter, copy, query, download, or update information.

**User Managers:** A User Manager is any University administrator, faculty member, or staff member who supervises Consumer/Users or who handles University business unit administrative responsibilities. User Managers are responsible for overseeing their Consumer/Users’ access to Sensitive Information, including:

- Reviewing and approving all requests for access authorizations and ensuring it accurately reflect each Consumer/User’s role and required access.
- Ensuring that the approved procedures are followed for employee suspensions, terminations, and transfers, and that appropriate measures are taken to revoke access privileges.
- Revoking access privileges from students, vendors, consultants, and others when access is no longer necessary or appropriate.
- Providing the opportunity for training needed to properly use computer systems.
- Reporting promptly to the Executive Director and Information Security Officer and to the Office of University Counsel any potential or actual unauthorized access of University Sensitive Information (security breach) in accordance with the University’s Protocol for Responding to Security Breaches of Certain Identifying Information.
- Initiating appropriate actions when Information Security Incidents are identified in accordance with the Incident Management Policy.
- Ensuring that any Information Security requirements are followed for any acquisitions, transfers, and surplus of equipment that processes or stores electronic information, such as computers, servers, smartphones/PDAs, and certain copiers.
Information Security Liaison: Each University business unit that is responsible for maintaining its own information technology services must have a designated Information Security Liaison as well as a designated backup Information Security Liaison. The duties and responsibilities of the Security Liaison are described in detail in the Security Liaison Policy.

Key responsibilities for the individuals serving in each of the above roles are discussed in the Information Security Procedures and Standards, which are attached. In addition, the University’s Executive Director and Information Security Officer will work with Stewards, Custodians, User Managers, Consumer/Users, and Information Security Liaisons to develop and implement prudent security policies, procedures, and controls, in consultation with the Office of University Counsel.

Chief Information Security Officer: The responsibilities of the Chief Information Security Officer and the staff of the Information Security Office include:

- Developing an Information Security Strategy approved by the Chief Information Officer and Data Governance Committee.
- Developing and maintaining a University Information Security Program to provide University services for:
  - Security Governance and Oversight
  - Network Security Protection
  - Endpoint Security Protection
  - Vulnerability Management
  - Incident Management
  - Annual Security Risk Assessments
  - Information Security Consulting
  - Information Security Policies, Procedures, and Standards
  - Information Security Awareness
  - Information Security Design and Architecture
  - Technology Risk Management
  - 3rd Party Security Reviews
- Serving as the University Security Officer for HIPAA, FERBA, GLBA, and PCI
- Service as the University Security Liaison to all Local, State, and Federal Government Agencies and Law Enforcement
5. Mission-Critical Resources

Mission-Critical Resources, as defined below, must be protected from accidental or intentional unauthorized modification, destruction, or disclosure.

The University expects members of its faculty, staff, and student body to understand and mitigate the risks to privacy inherent in digital technologies. The University also requires members of its faculty, staff, and student body to protect the University’s Mission-Critical Resources by adhering to the Information Security Procedures and Standards attached. Users who are third-party contractors and vendors must also be made aware of this policy and their responsibilities for safeguarding the University’s Mission-Critical Resources.

Definition of A Mission Critical Resource: A Mission-Critical Resource includes any resource that is critical to the mission of the University and any device that is running a mission-critical service for the University or a device that is considered mission critical based on the dependency of users or other processes. Mission-critical services must be available. Typical mission-critical services have a maximum downtime of three consecutive hours or less. Mission-Critical resources for Information Security purposes include information assets, software, hardware, and facilities. The payroll system, for example, is a Mission-Critical Resource.

Mission-critical computer systems and the infrastructure required to support them must be installed in access-controlled areas. In addition, the area in and around a computer facility housing Mission-Critical Resources must afford protection against fire, water damage, and other environmental hazards, such as power outages and extreme temperature situations.

Each University business unit housing Mission Critical Resources is required to establish procedures to provide emergency access to those Resources in the event that the assigned Custodians or Stewards are unavailable, or when operating in an emergency.

Additional responsibilities for individuals working with Mission-Critical Resources are discussed in the Information Security Procedures and Standards, which are attached.

For additional information on the University’s information security policies, procedures, standards, and practices, please see:

• Information Security Procedures
• Information Security Standards
• Data Governance Policy
• Software Acquisition Policy
• Acceptable Use Policy
• Access Control Policy
• Data Classification Policy
• Incident Management Policy
• Vulnerability Management Policy
• Remote Access Policy
• Workstation Use Policy
• General User Password Policy
• Policy and Standards for Electronic Media Disposal
• Policy on the Transmission of PHI or PII
• Protocol for Responding to Security Breaches of PHI and PII
• Security Awareness and Training Policy
• Security Liaison Policy
7. Policy Review and Adoption

This policy has been reviewed and adopted under the direction of Rowan’s Data Governance Committee and Chief Information Officer (CIO):

______________________________
Mira Lalovic-Hand
Vice President and CIO
Division of Information Resources and Technology