Information Security Policy

ROWAN UNIVERSITY POLICY

Title: Information Security Policy
Subject: Information Security
Policy No: ISO:2013:02
Applies: University-Wide
Issuing Authority: Senior Vice President for Information Resources and Technology and Chief Information Officer
Responsible Officer: Director of Information Security
Date Adopted: 09/01/2013
Last Revision: 02/06/2020
Last Review: 08/21/2019

I. PURPOSE

The purpose of this policy is to establish a framework for the protection of University information resources from accidental or intentional unauthorized access, modification, or damage in order to meet applicable federal, state, regulatory, and contractual requirements.

II. ACCOUNTABILITY

Under the direction of the President, the Chief Information Officer and Director of Information Security shall ensure compliance with this policy. The Vice Presidents, Deans, and other members of management will implement this policy in their respective areas.

III. APPLICABILITY

This policy applies to all members of the Rowan Community who access and use the University's electronic information and information systems.

IV. DEFINITIONS

Refer to Rowan University Technology Terms and Definitions for terms and definitions that are used in this policy.

V. POLICY

1. Information security is the protection of information from threats to ensure business continuity, minimize risks, and maximize university opportunities.
2. The Information Security Office (ISO) will manage the information security program at Rowan University and is responsible for developing strategies for managing the processes, tools, and policies necessary to prevent, detect, document and counter threats to information.
3. The information security program will be advised by the Information Technology Security Board (ITSB) which serves as the advisory board for information security governance at the university. The ITSB represents and advocates for the interest of the Rowan Community during decisions that impact information security at the University.
4. Information security requires a combination of policies and standards to manage information resources throughout its lifecycle.

a. Policy Development: Policies and standards are crucial to establishing, maintaining and monitoring proper information security practice and define responsibilities, shape processes and allow for oversight of critical information-related operations. At a minimum, the Information Security policies developed and enforced should include:

    i. Acceptable Use
    ii. Access Control
    iii. Business Continuity Management
    iv. Change Management
    v. Data Backup
    vi. Electronic Media Disposal
    vii. Encryption
    viii. Information Classification
    ix. Incident Management Policy
    x. Mobile Computing and Removable Media
    xi. Physical Security for IT Network Resources
    xii. Privileged Account Management
    xiii. Remote Access
    xiv. Security Awareness and Training
    xv. Security Incident Management
    xvi. Security Monitoring
    xvii. Transmission of Sensitive Information
    xviii. User Password
    xix. Workstation Use and Security

b. Policy Approval - The Information Security Office will follow the documented process for creating, reviewing and updating policies with final approval from the ITSB
c. Policy Exceptions - While exceptions to an information security policy or standard may weaken the protection of University information resources, they are occasionally necessary and standard procedures and documents should be in place to manage the exception as well as review the need for the exception periodically.
d. Policy Sanctions - The ISO is responsible for coordinating and enforcing sanctions against Rowan Community members who fail to comply with the University's information security policies.

5. The Information Security Office (ISO) will develop and maintain an information security risk management program to frame, assess, analyze, respond, and monitor risk. Guidance for this program will be based on the NIST 800-37 framework and security regulations such as HIPAA, PCI-DSS, FERPA, GLBA etc. Specific requirements under this program will include:

    a. Risk Analysis - In accordance with the Security Risk Analysis requirement under the Security Management Process of the HIPAA Security Rule (§164.308(a)(1)(ii)(A), Rowan University must conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of Electronic Protected Health Information (EPHI) held by the University via its role as a covered entity for Rowan Medicine. Based on guidance from Health and Human Service's (HHS) Office of Civil Rights (OCR), the risk analysis must at a minimum include the following nine elements:

        i. Scope of the Analysis
        ii. Data Collection
        iii. Identification and Documentation of Potential Threats and Vulnerabilities
        iv. Assessment of Current Security Measures
        v. Determination of the Likelihood of Threat Occurrence
        vi. Determination of the Potential Impact of Threat Occurrence
        vii. Determination of the Level of Risk
        viii. Final Documentation
        ix. Periodic Review and Updates to the Risk Assessment

    b. Risk Management Program - In accordance with the Risk Management requirement under the Security Management Process of the HIPAA Security Rule (§164.308(a)(1)(ii)(B), Rowan University must implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level. Accordingly, Rowan University should:

i. Ensure a thorough review of the risk analysis results are performed, and associated risk management plans are documented in the university risk register.
ii. Appropriate risk owners and key stakeholders are involved in this process in order to ensure adequate prioritization of risk and implementation of security measures to reduce those risks identified are addressed within an established timeline.

6. 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 an Owner/Steward, a Custodian, a Consumer/User or a User Manager as described within this Policy.

    a. Data Steward or Owner - is accountable for data assets from a business perspective and 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.
    b. Data Custodian - is accountable for data assets from a technical perspective and is the university employee responsible for the processing and storage of information or data on behalf of the Steward or Owner of that information or data.
    c. Consumer or User - A Consumer/User is any person authorized to read, enter, copy, query, download, or update information.
    d. User Managers - A User Manager is any University administrator, faculty member, or staff member who supervises or sponsors consumer/users or who handles University business unit administrative responsibilities. User Managers are responsible for overseeing their Consumer /Users’ access to Sensitive Information, including:

        i. Reviewing and approving all requests for access authorizations and ensuring it accurately reflect each Consumer/User’s role and required access.
        ii. Ensuring that the approved procedures are followed for employee suspensions, terminations, and transfers, and that appropriate measures are taken to revoke access privileges.
        iii. Revoking access privileges from students, vendors, consultants, and others when access is no longer necessary or appropriate.
        iv. Providing the opportunity for training needed to properly use computer systems.
        v. Reporting promptly to the Director of Information Security any potential or actual unauthorized access of University Sensitive Information in accordance with the University’s Protocol for Responding to Security Breaches of Certain Identifying Information.
        vi. Initiating appropriate actions when Information Security Incidents are identified in accordance with the Incident Management Policy.
        vii. Ensuring that any Information Security requirements are followed for any acquisitions, transfers, and surplus of equipment that processes or stores electronic information, including but not limited to computers, servers, smartphones, mobile devices, fax machines, and copiers.
    e. Information Security Office - The Director of Information Security overseeing the staff of the Information Security Office is responsible for:

        i. Developing an Information Security Strategy approved by the Chief Information Officer and the Information Technology Security Board (ITSB).
        ii. Developing and maintaining the University Information Security Program to provide University services for:

            1. Security Governance and Oversight
            2. Information Security Policies, Procedures, and Standards
            3. Network Security Protection and Monitoring
            4. Endpoint Security Protection and Monitoring
            5. Vulnerability Management
            6. Information Security Incident Management
            7. Annual Security Risk Assessments
            8. Information Security Consulting

9. Information Security Awareness
10. Information Security Design and Architecture
11. Technology Risk Management
12. Third Party Security Reviews

iii. Serving as the University Security Officer for HIPAA, FERBA, GLBA, and PCI.
iv. Serving as the University Security Liaison to all Local, State, and Federal Government Agencies and Law Enforcement.

VI. POLICY COMPLIANCE

Violations of this policy may subject the violator to disciplinary actions up to or including termination of employment or dismissal from school, subject to applicable collective bargaining agreements and may subject the violator to penalties stipulated in applicable state and federal statutes. 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. Affiliates, 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. Sanctions shall be applied consistently to all violators regardless of job titles or level in the organization per the Acceptable Use Policy.

By Direction of the CIO:

Mira Lalovic-Hand,
SVP and Chief Information Officer