Security Awareness and Training

ROWAN UNIVERSITY POLICY

Title: Security Awareness and Training
Subject: Information Security
Policy No: ISO:2014:02
Applies: University-Wide
Issuing Authority: Senior Vice President for Information Resources and Technology and Chief Information Officer
Responsible Officer: Information Security Officer
Date Adopted: 06/01/2014
Last Revision: 09/29/2023
Last Review: 09/29/2023

I. PURPOSE

This policy establishes the requirement for information security awareness, training and education for members of the Rowan community who have access to the University's information systems and information assets, in accordance with all applicable federal, state, and local laws governing the use of computers and the Internet.

II. ACCOUNTABILITY

Under the direction of the President, the Chief Information Officer and Information Security Officer 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. The Information Security Office (ISO) will provide and implement information security awareness, training and education for all members of the Rowan Community and ensure ongoing maintenance and enhancements to the training and education content.
2. All members of the Rowan Community who have access to information assets must complete all required security awareness training, including annual refresher training.
3. Remedial training will be required for any user whose account has been reported to be compromised
4. Security awareness training content will be reviewed and updated annually by ISO.
5. ISO will provide an annual security awareness training report and monthly updates to the Information Technology Security Board (ITSB).
6. Supervisors are responsible for ensuring that each of their direct reports completes their security awareness trainings.

VI. POLICY COMPLIANCE

Violations of this policy may subject the violator to the removal of system access or disciplinary actions, up to or including termination of employment or dismissal from a school, subject to applicable collective bargaining agreements and may subject the violator to penalties stipulated in applicable state and federal statutes. 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