Transmission Sensitive Information Policy

ROWAN UNIVERSITY POLICY

Title: Transmission of Sensitive Information Policy
Subject: Information Security
Policy No: ISO:2013:06
Applies: University-Wide
Issuing Authority: Senior Vice President for Information Resources and Technology and Chief Information Officer
Responsible Officer: Information Security Officer
Date Adopted: 07/01/2013
Last Revision: 10/04/2023
Last Review: 10/04/2023

I. PURPOSE

This policy is required to comply with regulations related to the protection of sensitive information in transit including, but not limited to Protected Health Information (PHI) and Personal Identifying Information (PII) from unauthorized access and to protect against data breaches. This policy sets forth requirements for the transmission or receipt of sensitive information on the Rowan University network.

II. ACCOUNTABILITY

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

III. APPLICABILITY

This policy applies to all users accessing the Rowan Network or University information through computing devices owned or managed the University. 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 are "users."

IV. DEFINITIONS

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

V. POLICY

1. All sensitive information including Protected Health Information (PHI), confidential and Personal Identifying Information (PII) (as defined in the Information Classification Policy) that is transmitted or received by Rowan University's computer systems, including mobile devices, must be encrypted in accordance with the requirements of the Encryption Policy when transmitted over wireless or public networks, including when transmitted via FTP and electronic mail.
2. Examples of when encryption is required include, but are not limited to:

    a. A University employee, student, contractor, or vendor sending or receiving the University's PHI, confidential data or PII using his/her home's Internet Service Provider (ISP) connection (e.g.cable company or DSL).

b. Any transmission of PHI, confidential data or PII sent over any home, public, hotel, or the unsecured campus wireless network. Use of the RowanSecure campus wireless network does not require VPN as long as one is transmitting to a destination within the campus.

c. A University employee, student, contractor, or vendor sending or receiving the University's PHI, confidential data or PII to a destination address outside the campus network.

d. Any vendor transmissions of PHI or PII sent over the Internet.

e. Use of a PDA to transmit PHI, confidential data or PII over a public network.

3. Encryption is not required for a University employee who uses an on-campus workstation, with a wired connection to the University network, to transmit a document to another University user or to save a document containing PHI, confidential data or PII to his/her University-managed network folder.

VII. NON-COMPLIANCE AND SANCTIONS

Violation of this policy may subject the violator to disciplinary actions, up to or including termination of employment or dismissal from a school, and may subject the violator to penalties stipulated in applicable state and federal statutes.

By Direction of the CIO:

Mira Lalovic-Hand,
SVP and Chief Information Officer