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: Director of Information Security
Date Adopted: 07/01/2013
Last Revision: 08/08/2018
Last Review: 08/08/2018

I. PURPOSE

This policy is required to comply with legal requirements regarding 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 Director of Information Security 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

1. **"*Encryption*"** – the process of transforming information using an algorithm to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key.
2. **"*Personal Identifying Information*" (PII)** – Personal Identifying Information 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 info that can be used to access a person's financial resources.
3. **"*Protected Health Information"* (PHI)** – Information covered by the Health Insurance Portability and Accountability Act (HIPAA).
4. **"*Public Network"*** – Any network outside the Rowan University network.
5. ***"Secure Backup"* (Encryption Recommended)** – The process of making a backup copy of information for the purpose of data recovery with security safeguards present to ensure the backup copy of the data remains protected from unauthorized access at all times. This may include physical protections as well as encryption to safeguard the backup information.

V. REFERENCES

1. HIPAA http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/

VI. POLICY

1. All sensitive information including Protected Health Information (PHI) and Personal Identifying Information (PII) (as defined below) that is transmitted or received by Rowan University's computer systems, including mobile devices, must be encrypted 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 or PII using his/her home's Internet Service Provider (ISP) connection (e.g.cable company or DSL), unless both (a) using a VPN connection, and (b) transmitting only to a destination within the campus network.
    b. Any transmission of PHI or PII sent over any home, public, hotel, or the unsecured campus wireless network, unless both (a) using a VPN connection, and (b) transmitting only to a destination within the campus network. Use of the UNC-Secure 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 or PII to a destination address outside the campus network. (Encryption is required in this case, even if a VPN connection is used.)
    d. Any vendor transmissions of PHI or PII sent over the Internet.
    e. Use of a PDA to transmit PHI 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 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