Physical Security for IT Network Resources

ROWAN UNIVERSITY POLICY

Title: Physical Security for IT Network Resources
Subject: Information Security
Policy No: ISO:2016:03
Applies: University-Wide
Issuing Authority: Senior Vice President for Information Resources and Technology and Chief Information Officer
Responsible Officer: Senior Director, Infrastructure Services
Date Adopted: 04/01/2016
Last Revision: 04/11/2019
Last Review: 04/11/2019

I. PURPOSE

The purpose for this policy is to outline physical security measures to safeguard all Rowan University information technology network resources against unlawful and unauthorized physical intrusion, as well as environmental (e.g. fire, flood) and other physical threats. Information Security issues considered include:

- Unlawful access may be gained with the intent of theft, damage, or other disruption of operations.
- Unauthorized and illegal access may take place covertly (internal or external source) to steal, damage, or otherwise disrupt operations.
- Destruction or damage of physical space may occur due to environmental threats such as fire, flood, wind, etc. Loss of power may result in the loss of data, damage to equipment and disruption of operations.

II. ACCOUNTABILITY

Under the direction of the President, 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 implement this policy in their respective areas.

III. APPLICABILITY

This policy applies to all members of the Rowan Community.

IV. DEFINITIONS

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

V. POLICY

1. Designation of Secure Areas to Protect IT Resources - Areas within a building that house critical information technology services shall be designated as secure areas. Data centers, server rooms, and network closets are designated secure areas.
2. Dedicated Purpose - Secure areas should not be shared with or used with any function other than legitimate IT resources. In those instances where a dedicated purpose is not feasible, a policy exception must be approved by the Chief Information Officer.

3. Physical Security Methods - Physical security methods should be used to control access to secure areas. These methods include, but are not limited to, locked doors, locked data cabinets, secured cage areas, vaults, ID cards, cameras, and biometrics. Security methods should be commensurate with the security risk.
4. Documented Provisioning Procedures - Processes and procedures for provisioning access to secure areas must be documented.
    a. The Director of Facilities at each campus must establish, in coordination with the ISO, a standard process for review, approval, and provisioning of access to secured areas.
    b. Information Technology Resource Managers must establish, in coordination with the ISO, a standard process for review, approval, and provisioning of access to secured areas.
    c. The Information Security Office (ISO) must monitor compliance with established processes.
5. Least Privilege Access - The principle of least privilege must be followed when granting access to secure areas and facilities that contain secure areas.
    a. Building access should be restricted to authorized personnel only (when applicable).
    b. Personnel, including full and part-time staff, contractors and vendors should be granted access only to facilities and systems that are necessary for the fulfillment of their job responsibilities.
6. Visitor Access - Individuals not regularly assigned to access secure areas are considered visitors.
    a. Visitors must present identification to access secure areas.
    b. Visitors accessing secure areas must be escorted and their activity must be monitored.
    c. Visitors access records must be maintained by the member of the Standard Access group escorting the Non-Standard Access member accessing the physical space. Records should include name, organization, signature, date/time of access and purpose of visit. Such inventories are subject to periodic ISO review.
7. Control of Physical Access Devices - Access cards, combinations, keypads, and keys must be secured against theft, loss, or damage.
    a. Combinations should be changed when compromised, or when individuals with access are transferred or terminated.
    b. Keys are a backup form of access to the designated physical space. Key/Lock inventories should be setup by Facilities and keys should be distributed to Public Safety, Network Services and Facilities. Such inventories are subject to periodic ISO review.
    c. Lost or stolen cards/keys must be reported to the ISO immediately.
8. Monitor Physical Access - Physical access to secure areas must be monitored to detect and respond to physical security incidents.
    a. Automated mechanisms should be employed to monitor physical access to secure areas.
    b. Physical access logs of secure areas should be reviewed on a monthly basis.
    c. Removal of individuals who no longer require access must be done in a timely manner.
    d. Results of access reviews must be coordinated with the ISO incident response team.
9. Environmental Controls - Environmental controls must be implemented to protect the University's investment in critical information technology resources.
    a. Fire suppression and detection devices/systems must be installed and maintained.
    b. Temperature and humidity controls must be installed and maintained.
    c. When present, sprinkler systems should provide master shutoff or isolation values.
    d. Data centers must be supported by backup power generators that are properly installed and maintained.

VI. POLICY COMPLIANCE

Violations of this policy may subject the violator to 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