General User Password

ROWAN UNIVERSITY POLICY

Title: General User Password Policy
Subject: Information Security
Policy No: ISO:2013:10
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: 07/26/2018
Last Review: 07/26/2018

I. PURPOSE

A growing number of information security threats result from unauthorized access to data stored on computers. Frequently, access to such data is controlled through the use of password authentication. The failure to protect data through the use of strong passwords can result in incidents that expose Sensitive Information and/or impact critical University services. Adherence to this policy is essential to ensure the security of information at the University, including Mission-Critical devices and devices storing or processing Sensitive Information.

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 any faculty member, staff member, student, temporary employee, contractor, outside vendor, or visitor to campus ("User") who has access to University-owned or managed information or the Rowan network through computing devices owned or managed through Rowan or through permission granted by Rowan University.

IV. DEFINITIONS

1. *"Information Security Incident*": Includes any incident that is known or has the potential to negatively impact the confidentiality, integrity, or availability of Rowan University information. This can range from the loss of a laptop or PDA to the virus infection of an end-user work station to a major intrusion by a hacker.
2. "*Mission-Critical Resource*": Includes any resource that is critical to the mission of the University and any device that is running a mission-critical service for the University or a device that is considered mission critical based on the dependency of users or other processes. Mission-critical services must be available. Typical mission-critical services have a maximum downtime of three consecutive hours or less. Mission-critical resources for Information Security purposes include information assets, software, hardware, and facilities. The payroll system, for example, is a Mission-Critical Resource.
3. "*Password Circulation*": An attempt to bypass the basic password requirement that prohibits reusing the same password within a specified period of time by changing the password repeatedly within a brief period of time in order to be able to reuse the password earlier than intended by the policy.

4. "*Password Policy Enforcement*": Password rules must be enforced according to the standards defined in the University's Password Policy for General Users.
5. "*Sensitive Information*": Sensitive Information includes all data, in its original and duplicate form, which contains:

    a. "Protected Health Information" as defined by HIPAA
    b. Student "education records," as defined by the Family Educational Rights and Privacy Act (FERPA)
    c. "Customer record information," as defined by the Gramm Leach Bliley Act (GLBA)
    d. "Card holder data," as defined by the Payment Card Industry (PCI) Data Security Standard

    Sensitive data also includes any other information that is protected by University policy or federal or state law from unauthorized access. This information must be restricted to those with a legitimate business need for access. Examples of sensitive information may include, but are not limited to, social security numbers, system access passwords, some types of research data (such as research data that is personally identifiable or proprietary), public safety information, information concerning select agents, information security records, and information file encryption keys.

V. POLICY

1. All passwords are to be treated as confidential Sensitive Information. This policy must be followed where technically feasible to the greatest extent possible.

    a. Users are required to use only account credentials for which they have been authorized. Attempts to log into an account other than those for which a User has been authorized are a violation of this policy.
    b. Use of default or general user accounts to run system services are prohibited.
    c. Any attempt to "crack" (decrypt) encrypted or hashed passwords is strictly prohibited.
2. Where technically feasible, passwords must not be shared with others except in emergency situations. In emergency situations, a password may be shared with a supervisor but must be changed immediately once there is no longer an emergency need. Examples of unauthorized sharing include sharing passwords with administrative assistants, coworkers or spouses.
    a. A password must never be inserted into plain text emails, stored unencrypted in computer files, or written down.
    b. A password must not have been used within the last 12 months. It is a violation of this policy to circulate quickly through passwords to bypass this provision.
    c. A password and user *ID* must share fewer than six (or, if shorter, the length of the user *ID*) consecutive common characters.
    d. A password must not be based on personal information, such as Social Security number, name or date of birth.
    e. A password should avoid words found in any English or foreign language dictionary.
    f. All users are responsible for maintaining the security of their passwords. In the event that an account is believed to have been compromised, the person detecting the incident should report the incident immediately to the IRT Support Desk. An account is deemed compromised if it is known or reasonably suspected that the account is being used by an unauthorized party. A compromise will affect the functionality of any account, and the account will not be restored until the risk associated with any such compromise has been mitigated.
    g. Vendor-supplied default and/or blank passwords shall be immediately identified and reset upon installation of the affected application, device, or operating system.
3. To ensure that passwords are of adequate strength, passwords for Users, systems, applications, and devices must meet, to the degree technically feasible, the following Information Security requirements:
    a. Password Requirements
        i. Password Expiration - Every 90 days
        ii. Minimum Length - 8 characters
        iii. Lock-Out Period - 30 minutes, following a maximum of 10 failed attempts to log in.
        iv. Renewed Log In Required - After 30 minutes of inactivity
            1. A password must contain at least one letter and at least one numerical digit.
            2. A password must contain at least one of these characters: !@#$%&*+={}?<>'"

3. A password must not: start with a hyphen, end with a backslash (), or contain a double-quote (") anywhere except as the last character.

VI. 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