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: Information Security Officer
Date Adopted: 07/01/2013
Last Revision: 09/06/2023
Last Review: 09/06/2023

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 Information Security Officer 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

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

V. POLICY

1. All passwords are to be treated as confidential sensitive information.
    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. 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. When changing a password, the new one 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 Technology Support Center at support@rowan.edu. 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 the following Information Security requirements:
    a. Password Requirements
        i. A password must contain at least one letter and at least one numerical digit.
        ii. A password must contain at least one of these characters: !@#$%&*+={}?<>'"
        iii. A password must not: start with a hyphen, end with a backslash (), or contain a double-quote (") anywhere except as the last character.
    b. Password Expiration: Every 180 days
    c. Minimum Length: 8 characters
    d. Lock-Out Period: 30 minutes, following a maximum of 10 failed attempts to log in.
    e. Renewed Log In Required: After 30 minutes of inactivity

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. Any exceptions to this policy must be approved by the Information Security Office.

By Direction of the CIO:

Mira Lalovic-Hand,
SVP and Chief Information Officer