Privileged Account Management

ROWAN UNIVERSITY

Title: *Privileged Account Management Policy*
Subject: *Information Security*
Policy No: *ISO:2016:02*
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: *04/01/2016*
Last Revision: *07/03/2018*
Last Review: *07/03/2018*

I. PURPOSE

The purpose of this policy is to prevent inappropriate granting and use of privileged access by IRT staff, Application Super Users, Departmental System Administrators and any individual provided with privileged access to Rowan University information systems.

ii. ACCOUNTABILITY

Under the direction of the President, the Chief Information Officer, IRT Director(s) and Departments, Schools and Business Units, the Information Security Office (ISO) shall implement and ensure compliance with this policy.

III. APPLICABILITY

This policy applies to all individuals, University wide, with privileged access to computing systems, network communication, or the accounts, files, data, or processes of other users.

IV. DEFINITIONS

Privileged Accounts: An account which, by virtue of function, and /or security access, has been granted special privileges within the computer system, which are significantly greater than those available to the majority of users, including but limited to, local administrative accounts, privileged user accounts, domain administrative accounts, emergency accounts, service accounts, and application accounts.

V. REFERENCES

1. Rowan Acceptable Use Policyhttps://confluence.rowan.edu/display/POLICY/Acceptable+Use+Policy
2. Rowan Access Control Policy
3. Rowan General User Password Policyhttps://confluence.rowan.edu/display/POLICY/General+User+Password

VI. POLICY

1. Privileged access enables an individual to take actions which may affect computing systems, network communication, or the accounts, files, data, or processes of other users. Privileged access is typically

granted to system administrators, network administrators, staff performing computing account administration, or other such employees whose job duties require special privileges over a computing system or network. Privileged access might provide such users with technical access capabilities that are beyond their functional access authority such as upgrade their functional access authority.

2. Individuals with privileged access must not abuse their access capability and strictly respect their functional access authority limits, respect the rights of the system users, respect the integrity of the systems and related physical resources, and comply with any relevant laws or regulations. Individuals also have an obligation to familiarize themselves regarding any procedures, business practices, and operational guidelines pertaining to the activities of their local department. In particular, the privacy of information holds important implications for computer system administration at Rowan. Individuals with privileged access must comply with applicable policies, laws, regulations, precedents, and procedures, while pursuing appropriate actions to provide high-quality, timely, reliable, computing services.
3. Requirements:
    a. Privileged access shall only be granted to authorized individuals.
    b. Individuals may request privileged access from the Technology Owner. Each Technology Owner must establish, in coordination with the ISO, a standard process for review, approval, and provisioning of administrative access to systems and applications. This process must include proper segregation of duties and provide the ISO with the ability to monitor compliance with the established information security policies and processes.
    c. Users with privileged access will have two user IDs in situations where providing access to their standard user id will create unacceptable risk: one for normal day-to-day activities and one for performing administrative duties.
    d. Every privileged account must have its own unique password when provisioned as a dedicated administrative account.
    e. Administrators may only use their administrator account to perform administrative functions.
    f. Administrators may not use their privileged access for unauthorized viewing, modification, copying, or destruction of system or user data.
    g. Users with privileged access have a responsibility to protect the confidentiality of any information they encounter while performing their duties.
    h. Users with privileged access are responsible for complying with all applicable laws, regulations, policies, and procedures.
    i. Users with privileged access must always be aware that these privileges place them in a position of considerable trust. Users must not breach that trust by misusing privileges or failing to maintain a high professional standard.
    j. The Information Security Officer (ISO) will maintain a master list from the collected departmental privileged user accounts.
    k. The ISO will maintain the responsibilities of governance, oversight, and monitoring of the Privileged Account Management process
4. Non-Compliance and Sanctions
    a. 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