Rock Valley College

Account Management

RVC Administrative Procedure (2:30.060)

Purpose

This Procedure establishes a standard for administering computing accounts that facilitate access or changes to Rock Valley College's institutional data. An account, at minimum, consists of a user ID and a password; supplying account information will usually grant access to some set of services and resources. This Procedure establishes standards for issuing accounts, creating password values, and managing accounts.

Scope

This Procedure is applicable to those responsible for the management of user accounts or access to shared information or network devices. Such information can be held within a database, application, or shared file space. This Procedure covers departmental accounts as well as those managed centrally.

Account Administrative Standards

Accounts that access electronic computing and information resources require prudent oversight. The following security precautions should be part of account management:

Issuing Accounts

1. The individuals responsible for managing Rock Valley College (RVC) data shall make decisions regarding access to the respective data that they keep (e.g., the Registrar, in compliance with applicable laws and Board policies and with guidance from the Department of Information Technology, will determine who has access to registration data, and what kind of access each user has). Account setup and modification shall require the signature (paper or electronic) of the requestor's supervisor.
2. The organization responsible for a resource shall issue a unique account to everyone authorized to access that networked computing and information resource. It is also responsible for the prompt deactivation of accounts, when necessary, i.e., accounts for terminated individuals shall be removed/disabled/revoked from any computing system at the end of the individual's employment or when continued access is no longer required; and the accounts of transferred individuals may require removal/disabling to ensure changes in access privileges are appropriate to the change in job function or location.
3. When establishing accounts, standard security principles of "least required access" to perform a function must always be used, where administratively

feasible. For example, a root or administrative privileged account must not be used when a non-privileged account will do.

4. The identity of users must be authenticated and the user must also agree to any applicable user agreement before providing them with account and password details. If an automated process is used, then the account holder should be asked to provide several information items that in totality could only be known by the account holder. In addition, it is highly recommended that stricter levels of authentication (such as face-to-face) be used for those accounts with privileged access (e.g., user accounts used for email do not require an identity validation process as thorough as for those user accounts that can be used to modify department budgets).
5. Passwords for new accounts should NOT be emailed to remote users UNLESS the email is encrypted.
6. The date when the account was issued should be recorded in an audit log or captured electronically.
7. All managers of accounts with privileged access to RVC data must sign a confidentiality agreement form that is kept in the department file under the care of a Human Resources representative or liaison.

Managing Accounts

1. All accounts shall be reviewed at least annually by the data owner and the Department of Information Technology to ensure that access and account privileges are commensurate with job function, need-to-know, and employment status.
2. All guest accounts (for those who are not official members of the RVC community) with access to RVC computing resources shall contain an expiration date of one year or the work completion date, whichever occurs first. All guest accounts must be sponsored by the appropriate authorized member of the administrative entity managing the resource.

Shared Accounts

Use of shared accounts is not allowed except as provided in this Procedure. In some situations, a provision to support the functionality of a process, system, device (such as servers, switches or routers), or application may be made (e.g., management of file shares) through the use of shared accounts. Such exceptions will require documentation which justifies the need for a shared account.

Each shared account must have a designated owner responsible for managing access to it. The owner is also responsible for the above-mentioned documentation, which should include a list of individuals who have access to the shared account. The documentation must be available upon request for an audit or a security assessment.

Administration of Password Changes

Guidelines for Password Resets

1. The identity of users must be authenticated before providing them with ID and password details. In addition, stricter levels of authentication (such as face-to-face) must be used for accounts with privileged access.
2. Whenever possible, passkeys should be used to authenticate a user when resetting a password or activating a guest account and should comply with the above standards. Passkeys provide one-time access to a system or application and require the user to change to a password of their choice upon initial login. Where passkeys are not feasible, pre-expired passwords should be used.
3. Automated password resets are available and may be used, provided a recognized and approved method is used, such as multiple, random challenge and response questions.
4. Passwords must be reset over an encrypted tunnel (SSL, or Virtual Private Network, for example).
5. Password change events should be recorded in an audit log.

Application and System Standards

Applications developed at Rock Valley College or purchased from a vendor should contain the following security precautions:

1. Where technically or administratively feasible, shared ID authentication should not be permitted.
2. Authentication should occur external to an application, i.e., applications should **not** implement their own authentication mechanism. Instead, external authentication services should be relied upon, provided by the host operating system, the web server, or the servlet container.
3. Passwords must **not** be stored in clear text or in any easily reversible form.
4. Role-based access controls should be used when feasible to support changes in staff or assigned duties.
5. Where technically or administratively feasible, systems should allow for lockouts after a set number of failed attempts (ten is the recommended number). Lockouts should be logged unless the log information includes password information.

Enforcement

All requests for clarifications or interpretations of this procedure should be directed to the Vice President of Operations/COO.

Implemented: March 2023