coast mountain college

INF-018G

Account Management Guideline

Purpose

The purpose of this guideline is to establish a standard for the creation, administration, use, and removal of accounts that facilitate access to information and technology resources at Coast Mountain College (CMTN).

Overview

Computer accounts are the means used to grant access to CMTN's information systems. These accounts provide a means of providing accountability, a key to any computer security program, for CMTN usage.

This means that creating, controlling, and monitoring all computer accounts is extremely important to an overall security program.

Definitions

Account: Any combination of a User ID (sometime referred to as a username) and a password that grants an authorized user access to a computer, an application, the network, or any other information or technology resource.

Security Administrator: The person charged with monitoring and implementing security controls and procedures for a system. Whereas CMTN may have one Information Security Officer, technical management may designate a number of security administrators.

System Administrator: The person responsible for the effective operation and maintenance of information systems, including implementation of standard procedures and controls to enforce an organization's security policy.

Scope

This guideline applies to the employees, directors, volunteers, contractors, consultants, temporaries, and other workers at CMTN, including all personnel affiliated with third parties with authorized access to any CMTN information system.

Details

Accounts

- All accounts created must have an associated written request and signed management approval that is appropriate for the CMTN system or service.
- All accounts must be uniquely identifiable using the assigned username.
- Shared accounts on CMTN information systems are not permitted.
- Reference CMTN's Human Resources protocols for removing an employee's access while on a leave of absence or vacation.
- All default passwords for accounts must be constructed in accordance with INF-008. *Password Choice and Protection Guideline*.
- All accounts must have a password expiration that complies with IT-008, Password Choice and Protection Guideline.
- Concurrent connections may be limited for technical or security reasons.
- All accounts must be disabled immediately upon notification of any employee's termination.

Account Management

- The following items apply to System Administrators or designated staff:
    - Information system user accounts are to be constructed so they enforce the most restrictive set of rights and privileges or accesses required for the performance of tasks associated with an individual's account.
        - Further, to eliminate conflicts of interest, accounts shall be created so that no one user can authorize, perform, review, and audit a single transaction.
    - All information system accounts will be actively managed.
        - Active management includes the acts of establishing, activating, modifying, disabling, and removing accounts from information systems.
    - Access controls will be determined by following established procedures for new employees, employee changes, employee terminations, and leaves of absence.
    - All account modifications must have a documented process to modify a user account to accommodate situations such as name changes and permission changes.
    - Information system accounts are to be reviewed monthly to identify inactive accounts.
        - If an employee or third-party account is found to be inactive for 30 days, the owners (of the account) and their manager will be notified of pending disablement.
        - If the account continues to remain inactive for 15 days, it will be manually disabled.
    - A list of accounts, for the systems they administer, must be provided when requested by authorized CMTN management.
    - An independent audit review may be performed to ensure the accounts are properly managed.

Related Policies, Guidelines, and Other Resources

- INF-008G, *Password Choice and Protection Guideline*