Overview

Computer accounts are the means used to grant access to SDCC's information systems. These accounts provide a means of providing accountability, a key to any computer security program, for SDCC usage. This means that creating, controlling, and monitoring all computer accounts is extremely important to an overall security program.

Purpose

The purpose of this standard is to establish a standard for the creation, administration, use, and removal of accounts that facilitate access to information and technology resources at SDCC.

Audience

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

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 SDCC 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.

Standard Detail

Accounts

- All accounts created must have an associated written request and signed management approval that is appropriate for the SDCC system or service.
- All accounts must be uniquely identifiable using the assigned username.
- Shared accounts on SDCC information systems are not permitted.
- All default passwords for accounts will be constructed in accordance with the SDCC Password Policy.
- All accounts must have a password expiration that complies with the SDCC Password Standard.
- 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 should be constructed so that they enforce the most restrictive set of rights/privileges or accesses required for the performance of tasks associated with an individual's account. Further, to eliminate conflicts of interest, accounts should 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 leave 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 SDCC management.

An independent audit review may be performed to ensure the accounts are properly managed.