Account Management Policy Template

Overview

Computer accounts are the means used to grant access to [COMPANY-NAME]'s information systems.

These accounts provide a means of providing accountability, a key to any computer security program, for [COMPANY-NAME] usage.

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

Purpose

This Account Management Policy is designed to effectively manage user accounts, ensuring the security of data and information technology systems within the organization. It sets forth guidelines for the creation, maintenance, and termination of access privileges to company resources.

The objective of this policy is to define a standard for creating, administering, using, and deactivating accounts that enable access to the information and technology resources at [COMPANY-NAME]

Policy Details

Account

- Every account created must be accompanied by a written request and management approval with a signature, suitable for the [COMPANY-NAME] system or service.

- Each account must be uniquely identified by its assigned username. The use of shared accounts on [COMPANY-NAME] information systems is strictly prohibited. For guidelines on disabling access during an employee's leave of absence or vacation, please refer to the Employee Access During Leave of Absence Policy.

- All initial passwords for accounts must be set in line with the [COMPANY-NAME] Password Policy.

- Additionally, all accounts should have password expirations that adhere to the [COMPANY-NAME] Password Policy.

- Technical or security considerations may restrict concurrent connections.

- Accounts must be deactivated immediately following any notice of an employee's termination.

Account Management

The following guidelines are directed towards System Administrators or designated personnel:

- System user accounts must be established to enforce the minimum necessary rights/privileges or accesses needed for the performance of duties specific to each user's role.

- Additionally, to prevent conflicts of interest, user accounts should be structured such that no single user has the ability to authorize, execute, review, and audit a single transaction on their own.

- All system accounts will be subject to active management, which includes setting up, activating, modifying, disabling, and removing accounts from information systems.

- Access controls will be determined by adhering to established protocols for new hires, employee transitions, terminations, and leaves of absence.

- All modifications to accounts must follow a documented procedure to address changes such as name updates and alterations in permissions.

- System accounts must undergo a monthly review to identify any that are inactive. If an account, whether it belongs to an employee or a third party, has been inactive for 30 days, the account owners and their manager will be notified about the impending deactivation. Should the inactivity persist for an additional 15 days, the account will be manually disabled.

- System Administrators must provide a list of the accounts they manage upon request by authorized [COMPANY-NAME] management.

- An independent audit may be conducted to verify that the accounts are being properly managed.