# Account Management Policy

To use this template, simply replace the text in dark grey with information customized to your organization. When complete, delete all introductory or example text and convert all remaining text to black prior to distribution.

# Purpose

Describe the factors or circumstances that mandate the existence of the policy. Also state the policy’s basic objectives and what the policy is meant to achieve.

The quality and integrity of [Company Name’s] information system accounts are the only legitimate method by which [Company Name] information systems may be accessed. Without active account management, the potential exists that legitimate users can use these accounts for illegitimate purposes. Additionally, the potential exists that these accounts can be usurped and used illegitimately to access [Company Name]’s information systems.

# Scope

Define to whom and to what systems this policy applies. List the employees required to comply, or simply indicate “all” if all must comply. Also indicate any exclusions or exceptions, i.e. those people, elements, or situations that are not covered by this policy or where special consideration may be made.

The Account Management Policy applies to all employees of [Company Name], including all temporary or contract workers. Specifically, it includes:

* Mainframes, servers, and other devices that provide centralized computing capabilities.
* SAN, NAS, and other devices that provide centralized storage capabilities.
* Desktops, laptops, and other devices that provide distributed computing capabilities.
* Routers, switches, and other devices that provide network capabilities.
* Firewalls, IDP sensors, and other devices that provide dedicated security capabilities.

# Definitions

Define any key terms, acronyms, or concepts that will be used in the policy. A standard glossary approach is sufficient.

# Governing Laws & Regulations

If applicable, list any laws or regulations that govern the policy or with which the policy must comply. Confirm with the legal department that the list is full and accurate. If there are no pertinent governing laws or regulations, delete this section.

# Policy Statements

Describe the rules that comprise the policy. This typically takes the form of a series of short prescriptive and proscriptive statements. Sub-dividing this section into sub-sections may be required depending on the length or complexity of the policy.

1. All information system accounts will be actively managed by appropriate administrative staff. Active management includes the acts of establishing, activating, modifying, disabling, and removing accounts from information systems.
2. Information system accounts are to be constructed such that they enforce the most restrictive set of rights/privileges or accesses required for the performance of tasks associated with that account. Further, accounts shall be created such that no one account can authorize, perform, review, and audit a single transaction to eliminate conflicts of interest.
3. Information system accounts are to be reviewed to identify accounts with inappropriate privileges (either too high or too low) on an [indicate frequency – suggest quarterly] basis. Should information system accounts be discovered with inappropriate privileges, those privileges will be manually reset to the established level.
4. Information system accounts are to be reviewed to identify inactive accounts. Should information system accounts that are associated with an employee or third party be discovered that have been inactive for [indicate interval – suggest 30 days], the owners of the account will be notified of pending disablement. Should the account continue to remain inactive for [indicate interval – suggest 30 days]it will be manually disabled.
5. Login attempts to information systems will be restricted such that after [indicate count – suggest five]failed attempts within a [indicate interval – suggest fifteen minutes], they will be locked out. Lockout will be automatically lifted after [indicate interval – suggest one hour]or may be manually lifted by [indicate process – suggest an identity-authenticated call to the help desk].

**Relevant Procedures**

Consider creating formal procedure documents that reinforce and support the policy statements above. Note, it is best practice to house policies and procedures in separate documents to keep the content focused and reduce the number of times the policy must be reapproved by senior management.

Create user accounts to optimize security:

* + - * + Accounts must be created with the minimal set of permissions (also known as least privilege) and functions (also known as job segregation) as required by the role. Accounts should be created with the following restrictions:

*System administrative access (install, configure, modify, and patch system software).*

*Account administrative access (create, delete, and modify accounts and permissions).*

*Review administrative access (review activities of other administrators).*

*Full content access (read, write, edit, and delete data).*

*Limited content access (read, write, and edit data).*

*Restricted content access (read and write data).*

*Minimal content access (read data).*

Actively manage user accounts on information systems:

* + - * + Perform user account review to ensure that users are provided with appropriate accounts and account permissions:

*Validate each system user’s role within the organization.*

*Review system accounts and account permissions for each user.*

*Validate that each user’s account and account permissions meet the requirements established by the role.*

* + - * + Should the account review determine that users have insufficient accounts or account permissions, the required accounts and/or permissions must be provided:

*Where accounts exist but permissions are insufficient, modify the account to include appropriate permissions as per the requirements of the positional role.*

*Where accounts do not exist, create accounts with appropriate permissions as per the requirements of the positional role.*

*Review created accounts and assigned permissions to ensure they meet the requirements of the role.*

* + - * + Should account review determine that users have inappropriate accounts or account permissions, those accounts and/or permissions must be rescinded:

*Eliminate extraneous permissions in allowed accounts.*

*Revoke access to, and eliminate permissions in, extraneous accounts.*

*Review system logs to catalog the activity of the account.*

*Upon completion of all review and investigation, permanently delete any extraneous accounts.*

# Non-Compliance

Clearly describe consequences (legal and/or disciplinary) for employee non-compliance with the policy. It may be pertinent to describe the escalation process for repeated non-compliance.

Violations of this policy will be treated like other allegations of wrongdoing at [Company Name]. Allegations of misconduct will be adjudicated according to established procedures. Sanctions for non-compliance may include, but are not limited to, one or more of the following:

1. Disciplinary action according to applicable [Company Name] policies;
2. Termination of employment; and/or
3. Legal action according to applicable laws and contractual agreements.

# Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Version ID** | **Date of Change** | **Author** | **Rationale** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |