Account Management Policy

|  |  |
| --- | --- |
| Policy Area | IT Policy Library |
| Approved Date | December 31, 20XX |
| Approved By | Policy Committee |
| Effective Date | January 1, 20XX |
| Current Version | 1.0 |

# I. Overview

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

# II. Purpose

This policy establishes the rules for creating, monitoring, controlling, and removal of accounts.

# III. Scope

This policy applies to all ABC Company Staff that have access to ABC Company’s Information Resources.

# IV. Policy

The Chief Security Officer shall ensure:

* System components and data resources that each role needs to access for their job function including level of privilege required (e.g. user, administrator, etc.) for accessing such resources.
* Security mechanisms restrict access to privileged user IDs to least privileges necessary to perform job responsibilities and such access is based on job classification and function.
* Documented approval by authorized parties specifying required privileges.
* Access control systems for systems components with multiple users that restrict access based on a user’s need to know, and is set to “deny all” unless specifically allowed.

This access control system must include the following: coverage of all system components, assignment of privileges to individuals based on job classification and function, and default “deny-all” setting.

* The organization has implemented procedures for terminating access to sensitive information when a Staff member leaves or has a change in job duties.
* Procedures assign responsibility for removing IT and/or physical access. Procedures include timely communication of termination actions to ensure that the procedures are appropriately followed.
* Procedures are based upon initial access authorization and subsequent modification of a user’s right of access to a workstation, transaction, program, or process.
* Procedures are in place for establishing and modifying user access to sensitive information. Such procedures shall be formally documented and updated regularly.
* Every 90 days a review of the list of persons with access to sensitive information shall be performed to ensure they are valid. Any inactive user accounts shall be immediately removed or disabled.
* The organization assigns a unique name and/or number for identifying and tracking user and administration identity. Procedures require the user ID to be in a specific format and specify the format to be used. Procedures specify that the unique user ID be used to track user activity within information systems that contain sensitive information. In addition to assigning a unique ID, IT security
* Staff shall employ at least one of the following methods to authenticate all users: something known (e.g. password or passphrase), something they have (e.g. token device or smart card), something they are (e.g. biometric). Where other authentication mechanisms are used (e.g. physical or logical security tokens, smart cards, certificates, etc.), authentication mechanisms must be assigned to an individual account and not shared among multiple accounts. In addition, physical and/or logical controls must be in place to ensure only the intended account can use that mechanism to gain access.
* Shared user IDs shall not exist for system administration and other critical functions. Shared and generic user IDs are not to be used to administer Information Systems and components.
* Authentication procedures verify a person or entity seeking access to sensitive information is the one claimed. Policies specify the types of approved authentication mechanisms that are reasonable and appropriate and control the addition, deletion, and modification of User IDs, credentials, and other identifier objects.
* Configuration standards are developed for all system components. Such standards shall address all known security vulnerabilities and be consistent with industry accepted system hardening standards such as those recommended by the Center for Internet Security (CIS), International Standards Organization (ISO), SysAdmin Audit Network Security (SANS), and National Institute of Standards Technology (NIST).
* Security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties.
* An analysis of risks to determine when two-factor (multi-factor) authentication shall be implemented on user accounts and systems whether managed onsite or by a third-party provider. Two-factor authentication shall be required for remote network access originating from outside the network by personnel (including users and administrators) and all third-parties (including vendor access for support or maintenance). Note: Two-factor authentication requires two of the three authentication methods (i.e. something known, have, or biometric) be used to gain access to a system. Using two separate passwords is not considered two-factor authentication.

All accounts created must have an associated request and approval that is appropriate for the ABC Company system or service.

All users must sign the ABC Company non-disclosure agreement before access is given to an account. All accounts must be uniquely identifiable using the assigned user name.

IT security Staff shall:

* Always change all vendor supplied defaults and remove or disable unnecessary default or generic accounts before installing a system on the network. This includes firewalls, routers, servers, storage devices, wireless devices, etc. that are connected to sensitive data or used to transmit sensitive data.
* Ensure all default passwords are changed including, but not limited to, those used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals, Simple Network Management Protocol (SNMP) community strings, etc.).
* Change wireless vendor defaults for environments containing or transmitting sensitive data. This includes, but is not limited to, default wireless encryption keys, passwords, and SNMP community strings.
* Ensure all default passwords for accounts must be constructed in accordance with the ABC Company Password Policy. All accounts must have a password expiration that complies with the ABC Company Password Policy.

Accounts of individuals on extended leave (more than 30 days) will be disabled. All new user accounts that have not been accessed within 30 days of creation will be disabled. Any accounts that cannot be associated with a business process or business owner shall be disabled.

System Administrators or other designated staff:

* Are responsible for removing the accounts of individuals that change roles within ABC Company or are separated from their relationship with ABC Company.
* Must have a documented process to modify a user account to accommodate situations such as name changes, accounting changes and permission changes.
* Must have a documented process for periodically reviewing existing accounts for validity
* Are subject to independent audit review.
* Must provide a list of accounts for the systems they administer when requested by authorized ABC Company management.
* Must cooperate with authorized ABC Company management investigating security incidents.
* Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server. For example, web servers, database servers, and DNS should be implemented on separate servers. Where virtualization technologies are in use, implement only one primary function per virtual system component.
* Enable only necessary services, protocols, daemons, etc., as required for the function of the system.
* Implement additional security features for any required services, protocols, or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.
* Configure system security parameters to prevent misuse.
* Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.
* Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access management and other non-console administrative access.
* Maintain an inventory of Information Systems and related components.
* Verify user identity before modifying any authentication credential. For example, performing password resets, provisioning new tokens, or generating new keys.

Users of Information Systems shall be notified:

* Prior to gaining access to a system where system usage is monitored, recorded, and subject to audit.
* By using the system, he/she has granted consent to such monitoring and recording.
* Unauthorized use is prohibited and subject to criminal and civil penalties.
* If the operating system permits, each initial screen (displayed before user logon) shall contain warning text to the user and the user shall be required to take positive action to remove the notice from the screen.

Security personnel must ensure effective administration of users' computer access to maintain system security, including user account management, auditing, and the timely modification or removal of access. The following are important user administration considerations:

* User account management – Staff shall have a process for requesting, establishing, issuing, and closing user accounts. In addition, Staff should track users and their respective access authorizations.
* Audit and management reviews – on an annual basis, security personnel shall review system user accounts. Reviews should examine the levels of access each individual has, conformity with the concept of least privilege (access to system components and data to only those individuals whose job requires such access), whether all accounts are still active, whether management authorizations are up-to-date, whether required training has been completed, etc. These reviews must be conducted on an application-by-application and on a system wide basis.
* Detecting unauthorized/illegal activities. Mechanisms besides auditing and analysis of audit trails must be used to detect unauthorized and illegal acts. Rotating Staff in sensitive positions, which could expose a scam that required a Staff member’s presence, and periodic rescreening of personnel help manage risks.

Termination of a Staff member may be classified as either friendly or unfriendly. Friendly terminations must be accomplished by implementing a standard set of procedures for outgoing or transferring Staff. This normally includes:

* Removal of access privileges, computer accounts, authentication tokens.
* The control of keys to the office and/or office furniture and equipment.
* The briefing on the continuing responsibilities for confidentiality and privacy.
* Return of ABC Company property.
* Replacement staff ability to access data.

Information security responsibilities and duties that remain valid after termination or change shall be defined, communicated to the appropriate Staff, and enforced.

ABC Company requires terminating Staff to document procedures or filing schemes (e.g. how and where documents are stored on the hard disk). Staff must be instructed whether or not to "clean up" their computer before leaving. If cryptography is used to protect data, the availability of cryptographic keys to management personnel must be ensured.

Unfriendly Terminations have a potential for adverse consequences. In addition to the above, Staff shall do the following:

* System access must be terminated as quickly as possible when a Staff member is leaving a position under less than friendly terms. If Staff are to be immediately terminated, system access must be removed at the same time (or just before) Staff is notified of the dismissal.
* When a Staff member notifies ABC Company of a resignation, and it can be reasonably expected that it is on unfriendly terms, system access must be immediately terminated.
* During the "notice of termination" period, it may be necessary to assign the individual to a restricted area and function. This may be particularly true for Staff capable of changing programs or modifying the system or applications.
* In some cases, physical removal of the Staff member from ABC Company’s offices may be necessary.
* Upon termination, Staff returns any items or assets that belong to ABC Company.
* Upon change in Staff duties, the Owner of an asset shall determine the appropriate change in Staff access rights to Information Resources.

# V. Enforcement

Any Staff member found to have violated this policy may be subject to disciplinary action, up to and including termination.

# VI. Distribution

This policy is to be distributed to all ABC Company Staff who use Information Resources.

**Policy History**

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Description | Approved By |
| 1.0 | 1/1/20XX | Initial policy release |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**References:**

COBIT APO01.01-03, APO01.11, APO12.02, APO12.07, APO13.01-02, APO13.07, DSS01.05

GDPR Article 25, 32

HIPAA 164.308(a)(3)(ii)(A), 164.308(a)(3)(ii)(B)

ISO 27001 A.7.2.1, A.8.1.2-3

NIST SP 800-37 3.3

NIST SP 800-53 AC-1-3

NIST Cybersecurity Framework PR.AC, DE.DP-2, RS.RP-1

PCI 7.1-3, 8.1-2