**COMPANY Logo**

**Information Security Policies:** Access Control Management

Effective Date:

**COMPANY Logo**

Revised:

Approved by: CISO (or equivalent) Approved on: 00/00/20

Approved by: COO Approved on: 00/00/20

Approved by: Board of Directors Approved on: 00/00/20

# Purpose

The purpose of the Access Control Management Policy is to implement requirements and specific protective measures within COMPANY (“COMPANY”) to be taken to control access to data, computers (desktop, server, mainframe, portable devices, etc), networks, accounts, and web sites. These access controls provide enforcement of specified authorization rules based on positive identification of users and the systems or information they are permitted to access. This policy:

* Defines requirements for identifying and authenticating users in order to control access to authorized users with the proper privileges
* Manages admission to system and network resources based on predefined authorization rules
* Ensures authentication based on the identity of the user or client machine attempting to log on
* Grants the authenticated user access to specific resources based on COMPANY policies and the permission level assigned to the user or user group

# Scope

This policy applies to Users (employees, contractors, vendors, consultants, or other persons) having access to COMPANY computing assets or information. It applies to all systems used to conduct COMPANY business, and applies to internal COMPANY information and information shared with and received from third parties.

# Roles and Responsibilities

## The RACI Chart below shows the assignment of functional and cross-functional activities. The roles are as follows:

| R - Responsible is the organizational title responsible for doing the work.A - Accountable is the organizational title for who is accountable for the work being done.C - Consulted is the organizational title that provides necessary information.I - Informed is the organizational title that receives information. **Milestone or Task** | Governance / Risk Management | Chief Information Security Officer (or equivalent) | Information Security Organization / IT | Remote Users | Users |
| --- | --- | --- | --- | --- | --- |
| User Access Controls | C | A | R | I | I |
| Identification and Authentication | C | A | R | I | I |
| Privilege Management | C | A | R | I | I |
| Password Management | C | A | R | R | R |
| Password Controls Standard | C | A | R | R | R |
| Network Access Control | C | A | R | I | R |
| Operating System Access Control | C | A | R | I | R |
| Application and DB Access Control | C | A | R | I | R |
| Remote Access Control | C | A | R | R | I |
| Security of Remote Devices | C | A | R | R | I |
| Internet / VPN Access | C | A | R | R | I |
| Dial-In / Modem Access | C | A | R | R | I |
| Wireless Access | C | A | R | R | I |

# Policy Statements

# The Access Control Management Policy is implemented to restrict access to COMPANY resources and assets, including information to those with a legitimate business requirement.

This is accomplished via the following:

## User Access Controls

* + 1. IT must maintain documented standards and procedures which dictate proper user access.
    2. IT must implement measures to enforce the control of user access to the information within COMPANY computer systems.
    3. IT must implement user access control measures to allow users access to only the information, functions, and resources within a computer system required to perform their job related duties.
    4. IT must require modifications to user access to computer systems to be based on changes to a User’s job responsibilities.
    5. IT must remove user access from a computer system when triggered by an official departure notification that is provided by the HR Department in response to a termination event.
    6. Users must complete the appropriate system-specific account form to request modification to access to computer systems.

## Identification and Authentication

* + 1. IT must control authentication to a computer system using a unique UserID and Password.
    2. IT must configure all COMPANY computer systems to require the user to provide proper identification and present an authentication credential (e.g., password) when initially accessing a system.
    3. IT must assign a unique UserID to Users with access to a COMPANY computer system.
    4. IT must minimize and, where possible, eliminate the use of the guest UserID.
    5. IT must ensure computer system credentials (e.g., passwords) are compliant with COMPANY credential standards, as described in the *Passwords Control Standard*.
    6. Where system or application limitations require the use of passwords that do not meet established standards, IT must ensure password usage is as close to meeting the COMPANY standards as is technically possible.
    7. IT must create authorized service accounts for COMPANY computer system resources (e.g., print servers) that have unique service account IDs and passwords.
    8. IT must activate UserIDs for temporary staff (e.g., contractors and consultants) only during those periods when the temporary staff is actively performing service for COMPANY.
    9. Users must be prohibited from sharing UserIDs.
    10. Users must be prohibited from simultaneous logins to a COMPANY computer system by one UserID from different network addresses or workstations.
    11. Users must use a password protected screen saver. All desktops, servers, laptops, and mobile devices, connected to COMPANY’s network must employ the automatic screen lock feature if there is no activity for 15 minutes.
    12. Users must manually lock their computers when they leave their workstation unattended, even if they will be away for less than 15 minutes.

## Privilege Management / Authorization

* + 1. IT must document account authorization procedural guidelines. These controls include identifying and authorizing user access requests, managing user accounts, addressing user access attempt failures, etc.
    2. IT must process requests regarding access to COMPANY computer systems and applications via the approved and documented authorization procedural guidelines.
    3. IT must use a computer system-specific account form to record authorization.
    4. IT must implement controls to limit user access to COMPANY information on computer systems based on user permissions / authorization assigned on a “need to know” basis.
    5. IT must grant user access to COMPANY information on computer systems based on a User’s job responsibilities.
    6. IT must periodically review user access to COMPANY computer systems.
    7. IT must document and monitor user permissions / authorization on COMPANY computer systems.
    8. Upon termination, IT must revoke the terminated User’s access to COMPANY computer systems within 24 hours; or sooner if requested by HR or Senior Management.

## Password Management

* + 1. The Information Security Organization must perform a periodic review of the password strength controls to ensure that the passwords conform to the *Password Controls Standard*.
    2. IT must enforce password (credential) administration and controls in a consistent manner.
    3. IT must ensure passwords are not displayed on the screen as they are keyed in.
    4. IT must immediately change every compromised computer system or sensitive password on affected computer systems. Under these circumstances, IT must reload a trusted version of the operating system and all security related software. Under these circumstances, IT must review all recent changes to user and system privileges for unauthorized modification.
    5. IT must establish the identity of the User requesting a password change prior to resetting the password.
    6. IT must communicate passwords following the secure password communications guidelines. This includes directly providing the passwords to the User, to their voicemail, to their Manager, and the use of temporary one-time passwords. This does not include emailing unencrypted passwords to the User.
    7. Users must select passwords so that they are difficult to guess in compliance with documented password standards.
    8. Users must not use the same passwords for COMPANY computer systems that they use for external or personal computer systems.
    9. Users must use different passwords for remote access over insecure networks (i.e., the Internet) from the User’s “internal” passwords.
    10. Users must ensure passwords are not written down or left in a place where unauthorized persons might discover them.
    11. Users must be prohibited from intentional disclosure or sharing of passwords.
    12. Users must encrypt passwords, except for one-time use passwords, when held in storage for any significant period of time or when transmitted across the network.
    13. Users must not store passwords for user accounts in readable form, in batch files, automatic login scripts, software macros or terminal function keys. If necessary, service account passwords may be stored in readable form.
    14. Users must not send passwords through e-mail unencrypted.

## Password Controls Standard

* + 1. **Password Controls Standard**: Passwords must follow all standards defined in the *Passwords Control Standard*. The following are a summary of the basic password standards:
    2. **Password Length**: Passwords must have a minimum length of 8 characters or more characters and not allow null passwords.
    3. **Password Expiration**: Passwords must be changed every 90 days. When available the expiration-warning period is set to 14 days. For systems that track expiration in weeks, the password must be set to expire every 13 weeks.
    4. **Password History**: When available, the password history feature must be set to remember the last 8 previously used passwords (i.e., the new password cannot be the same as the last 8 passwords).
    5. **Account Lockout**: When available, the maximum number of logon attempts must be set to 5. This ensures account lock out after 5 unsuccessful (failed) logon attempts.
    6. **Complexity**: Passwords must be furthered strengthened by requiring a combination of at least three of the following four character types: numeric, lowercase, uppercase, special character (i.e., non-alphabetic character such as a numeral or punctuation).

## Network Access Control

* + 1. IT must control user access to both internal and external networked services.
    2. IT must ensure user access to networks and network services do not compromise the security of the network services.
    3. IT must ensure users are only provided with access to the network services that they have been specifically authorized to use.
    4. IT must implement automatic equipment identification as a means to authenticate connections from specific locations and equipment.
    5. IT must control physical and logical access to diagnostic and configuration ports.
    6. IT must segregate networks groups of information services, users, and information systems.
    7. IT must implement routing controls for networks to ensure that computer connections and information flows do not breach the access control policy of the business applications.
    8. IT must limit logical access to networking hardware and software to properly authorized IT personnel.
    9. IT must limit access to programmable network devices (e.g., routers, bridges) to properly authorized IT personnel.
    10. IT must immediately change/deactivate Vendor supplied “default” passwords.
    11. IT must ensure that access to device maintenance software is not accessible via the network.
    12. IT must limit the use of network diagnostic tools to specifically designated personnel in accordance with their job responsibilities.
    13. IT must limit access to all network configuration and security-related data, such as dial-up and callback numbers to authorized users.
    14. IT must prevent routers and bridges from disclosing the configuration of the internal network to external entities.

## Operating System Access Control

* + 1. IT must control access to operating system accounts by a secure log-on procedure.
    2. IT must limit operating system account access to allow users access to only the information and functions required to perform their duties.
    3. IT must log all operating system account access and modifications. Logs must be reviewed regularly.
    4. IT must not give out information necessary to access operating systems via system accounts or other highly privileged accounts to any user without approval. The list of individuals authorized to grant access to system or other highly privileged accounts must be reviewed annually.
    5. IT must not use Root logins; the ability to hold users accountable must be implemented.
    6. IT must restrict access to operating system and other systems software to properly authorized personnel.
    7. IT must change or deactivate all vendor-supplied passwords.
    8. IT must limit the use of diagnostic tools to trained support personnel, consistent with their job responsibilities.
    9. IT must restrict and tightly control the use of utility programs that might be capable of overriding system and application controls.
    10. IT must ensure safeguards exist to prohibit application programs from modifying the operating system.
    11. IT must prohibit users of applications residing on LAN's from making any changes to the operating system.

## Application and Database Access Control

* + 1. IT must restrict access to application software and information contained in databases to authorized users.
    2. IT must restrict access to information and application system functions by users and support personnel.
    3. IT must have a dedicated or isolated computing environment for sensitive systems.
    4. IT must limit access to COMPANY production programs to properly authorized users.
    5. IT must ensure that development and data processing users do not have the ability to make changes to COMPANY production programs or information, except through the approved configuration control mechanism.
    6. IT must log all access and modifications to applications and databases. Logs must be reviewed regularly.
    7. IT must limit application and database access to allow users access to only the information and functions required to perform their duties.
    8. IT must deny unauthorized users access to program libraries.

## Remote Access Control

* + 1. IT must manage remote access to COMPANY’s information and information resources.
    2. IT must limit remote access to COMPANY’s information and resources to authorized entry points.
    3. IT must implement controls to strongly authenticate users remotely connecting to and accessing COMPANY’s information and resources.
    4. IT must ensure that a user that remotely connects to the network must be authenticated, preferably via the use of dual-factor authentication methods (smart cards or tokens).
    5. Users must not share their login or password with anyone, including assistants, other COMPANY employees, or family members.
    6. Users must not make modifications of any kind to the remote access connection.

## Security of Remote Devices

* + 1. IT must implement safeguards to ensure that all machines (whether COMPANY-owned or personally-owned) used to remotely access COMPANY’s network implement all information security policies such as anti-virus, password controls, data handling and protection controls, updated software and patches, etc.
    2. IT must ensure that by accessing the COMPANY network remotely with personal equipment, users understand that their machines are a de facto extension of the COMPANY network, and as such are subject to the same rules and regulations that apply to COMPANY-owned equipment, i.e., their machines must be configured to comply with all COMPANY Information Security Policies.
    3. IT must ensure that all hosts that are connected to COMPANY’s internal networks via remote access technologies use the most up-to-date anti-virus software, this includes personal computers.
    4. IT must ensure that all users understand that reconfiguration of a home user's equipment for the purpose of split-tunneling or dual homing is not permitted at any time.
    5. IT must ensure that personal firewalls are used by all machines that remotely access the COMPANY network.
    6. IT must ensure that third party remote connections comply with stated COMPANY connectivity requirements.

## Internet / VPN Access

* + 1. IT must limit VPN access to users as needed by their job function.
    2. IT must ensure that all remote users must connect via centralized communications servers. IT must ensure VPN gateways are set up and managed by COMPANY IT. All remote access must be monitored.
    3. IT must ensure that COMPANY users with remote access privileges understand that when remotely connected to the COMPANY network the computer or workstation cannot be connected to any other network at the same time (with the exception of personal networks that are under the complete control of the user).
    4. IT must ensure the user understands they are responsible for selecting an Internet Service Provider (ISP), coordinating installation, installing any required software, and maintaining security controls.
    5. IT must ensure that the user understands it is their responsibility to ensure that unauthorized users are not allowed access to COMPANY networks via their VPN connection.
    6. IT must ensure that when actively connected to the corporate network, VPNs must force all traffic to and from the PC over the VPN tunnel: all other traffic will be dropped.
    7. IT must ensure VPN users are automatically disconnected from the COMPANY network after thirty minutes of inactivity. The user must then logon again to reconnect to the network.
    8. IT must ensure pings or other artificial network processes are not used to keep the connection open.
    9. IT must ensure the VPN concentrator is limited to an absolute connection time of 8 hours.

## Dial-In / Modem Access

* + 1. IT must ensure that analog data lines are not attached to computers on COMPANY’s network unless authorized by management.
    2. IT must control dial-in connections to gain access to the COMPANY network using one-time password authentication.
    3. IT must ensure users with dial-in access privileges understand a dial-in connection to the COMPANY network is not to be used by non-employees to gain access to COMPANY information system resources.
    4. IT must ensure users who are granted dial-in access privileges must remain constantly aware that dial-in connections between their location and COMPANY are literal extensions of COMPANY network, and that they provide a potential path to COMPANY’s most sensitive information.
    5. IT must strongly discourage internal or external modems on desktop computers and workstations.
    6. IT must register all authorized desktop modems. Where modems are allowed, they must be restricted to outbound calling only.
    7. IT must prohibit remote access server software on desktop computers and workstations.

## Wireless Access

* + 1. IT must ensure all wireless LAN access uses corporate-approved vendor products and security configurations.
    2. IT must utilize a corporate-approved Virtual Private Network (VPN) configured to drop all unauthenticated and unencrypted traffic for all computers with wireless LAN devices.
    3. IT must ensure all wireless implementations:
* Maintain point to point hardware encryption of at least 56 bits
* Support a hardware address that can be registered and tracked, i.e., a MAC address
* Support and employ strong user authentication which checks against an external database such as TACACS+, RADIUS or something similar
  + 1. IT must ensure the SSID is configured such that it does not contain any identifying information about COMPANY, e.g.; company name, division title, employee name, or product identifier.

# Compliance with Policies

# Use of COMPANY’s network, systems, hardware and applications represents the User’s consent to the terms of the policies described here, including consent for COMPANY to monitor and audit content and/or use. A User’s failure to comply with Information Security Policies may lead to disciplinary action to include one or more of the following:

* Oral and/or written warning or notification of violation to User(s) involved and supervisor(s)
* Suspension of network, system or application access or electronic communications privileges permanently or for a set period
* Repossession of electronic devices or hardware permanently or for a set period
* Electronic messages may be blocked or rejected if the message contains inappropriate content
* Written warning to the User’s HR file
* Suspension from work
* Education course related to the infraction paid for by the User
* Regulatory discipline or censure
* Termination of employment

Users consent by reading this policy at time of hiring and at each annual evaluation by signing an Information Security Policy Acknowledgement form.

# Questions

Users are encouraged to contact the Chief Information Security Officer (CISO) or the Information Security Organization with any questions or concerns. It is critical for all Users to consult supervisors and/or the Information Security Organization about “red flags” (any suspicious activities giving rise to concerns about whether such activities meet or potentially violate Information Security Policies). All Users are encouraged to raise questions or concerns if they believe an information-security risk or leak is present.

# Disclaimers

COMPANY retains the right to:

* Restrict or revoke any User’s privileges to information, equipment or systems
* Inspect, copy, remove or otherwise alter any information, program, or other system resource that may undermine these objectives
* Take any other steps deemed necessary to protect COMPANY information or information systems

This right may be exercised with or without notice to the involved users. COMPANY disclaims any responsibility for loss or damage to information or software that results from COMPANY exercising its rights under Information Security Policies.

All documents, computing assets, and communications systems assets, including the email and phone systems, physically located at or pertaining to COMPANY are the property of COMPANY. COMPANY reserves the right to examine all information stored in or transmitted by these systems, subject to applicable law. Users should have no expectation of privacy associated with personal information and information stored in, created on, or sent through the COMPANY computer and communication systems.

# Definitions

The following terms are related to this Information Security Policy:

* **Access Control**: The application of technical controls and procedures as preventive measures or countermeasures against the threat of unauthorized access to resources and data.
* **Authentication**: To verify the identity of a user, device, or other entity in a computer system, often as a prerequisite to allowing access to resources in a system.
* **Authorization**: The granting of access rights (or privileges) to a user, program, or process.
* **Credentials**: Detailed information, acquired during authentication, that describes the user, any group associations, and other security-related identity attributes. Credentials can be used to perform a multitude of services, such as authorization, auditing, and delegation.
* **Credential Management**: The act of managing the assignment, use, monitoring, protection, and revocation of credentials.
* **Identification**: The process that enables recognition of an entity by a system, generally by the use of unique machine-readable user names.
* **Least Privilege**: The principle that requires that each subject be granted the most restrictive set of permissions (or access) needed for the performance of authorized tasks.
* **Privilege**: Authorization / permission to perform a specific function usually restricted to a limited set of individuals or elements.