|  |  |
| --- | --- |
| **Access Control Procedure** | **No. [Organization]** **IS-1** |
|  | **Effective Date:** Sept 27, 2023 |

# Overview

This procedure establishes the [Organization] Access Control Procedure, for managing risks from user account management, access enforcement and monitoring, separation of duties, and remote access through the establishment of an Access Control program. The access control program helps [Organization] implement security best practices regarding logical security, account management, and remote access.

# Purpose

The [Organization] Information Security procedure serves to be consistent with best practices associated with organizational Information Security management. It is the intention of this procedure to establish an access control capability throughout [Organization] to help the organization implement security best practices about logical security, account management, and remote access.

# Scope

The scope of this procedure is applicable to all Information Technology (IT) resources owned or operated by [Organization]. Any information not specifically identified as the property of other parties, that is transmitted or stored on [Organization] IT resources (including e-mail, messages, and files) is the property of [Organization]. All users (employees, contractors, vendors, or others) of IT resources are responsible for adhering to this procedure.

# Procedure

**Access Control**

[Organization] has chosen to adopt the Access Controlprinciples established in NIST SP 800-53 “Access Control,” Control Family guidelines, as the official procedure for this domain. The following subsections outline the Access Controlstandards that constitute [Organization] procedure. Each [Organization] Information Security System is then bound to this procedure and must develop or adhere to a program plan which demonstrates compliance with the procedure related the standards documented.

* AC-1 Access Control Procedures: All [Organization] Business Systems must develop, adopt or adhere to a formal, documented access control procedure that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.
* AC-2 Account Management: All [Organization] Business Systems must:
  + Identify account types (i.e., individual, group, system, application, guest/anonymous, and temporary).
  + Establish conditions for group membership.
  + Identify authorized users of the information asset and specifying access privileges.
  + Require appropriate approvals for requests to establish accounts.
  + Establish, activate, modify, disable, and remove accounts.
  + Specifically authorize and monitor the use of guest/anonymous and temporary accounts.
  + Notify account managers when temporary accounts are no longer required and when information asset users are terminated, transferred, or information assets usage or need-to-know/need-to-share changes.
  + Deactivate temporary accounts that are no longer required and accounts of terminated or transferred users.
  + Grant access to the system based on (1) valid access authorization, (2) intended system usage, and (3) other attributes as required by the organization or associated missions/business functions.
  + Review accounts on a periodic basis or at least annually.
* AC-3 Access Enforcement: All [Organization] Business Systems must enforce approved authorizations for logical access to the system in accordance with applicable procedure.
* AC-4 Information Flow Enforcement: All [Organization] Business Systems must enforce approved authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable procedure.
* AC-5 Separation of Duties: All [Organization] Business Systems must:
  + Separates duties of individuals as necessary, to prevent malevolent activity without collusion.
  + Document separation of duties.
  + Implements separation of duties through assigned information asset access authorizations.
* AC-6 Least Privilege: All [Organization] Business Systems must employ the concept of least privilege, allowing only authorized accesses for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.
* AC-7 System Use Notification: All [Organization] Business Systems must:
  + Display an approved system use notification message or banner before granting access to the system that provides privacy and security notices consistent with regulations, standards, and policies.
  + Retain the notification message or banner on the screen until users take explicit actions to log on to or further access the information asset.
* AC-9 Concurrent Session Control: All [Organization] Business Systems must limit the number of concurrent sessions for each system account to ten for information assets.
* AC-10 Session Lock: All [Organization] Business Systems must prevent further access to the information asset by initiating a session lock after 120 minutes of inactivity or upon receiving a request from a user. In addition, [Organization] Business Systems must retain the session lock until the user reestablishes access using established identification and authentication procedures.
* AC-11 Permitted Actions without Identification or Authentication: All [Organization] Business Systems must identify specific user actions that can be performed on the information asset without identification or authentication. In addition, [Organization] Business Systems must document and provide supporting rationale in the security plan for the information asset, user actions not requiring identification and authentication.
* AC-12 Remote Access: All [Organization] Business Systems must:
  + Document allowed methods of remote access to the information assets.
  + Establish usage restrictions and implementation guidance for each allowed remote access method.
  + Monitor for unauthorized remote access software as well as remote access traffic to the information asset.
  + Authorize remote access to the information asset prior to connection.
  + Enforce requirements for remote connections to the information asset.
* AC-13 Wireless Access: All [Organization] Business Systems must:
  + Establish usage restrictions and implementation guidance wireless access.
  + Monitor for unauthorized wireless access to the information asset.
  + Authorize wireless access to the information asset prior to connection.
  + Enforce requirements for wireless connections for the information asset.
* AC-14 Access Control for Mobile Devices: All [Organization] Business Systems must:
  + Establish usage restrictions and implementation guidance for organization-controlled mobile devices.
  + Authorize connection of mobile devices meeting organizational usage restrictions and implementation guidance to organizational information assets.
  + Monitor for unauthorized connections of mobile devices to organizational information assets.
  + Enforce requirements for the connection of mobile devices to organizational information assets.
  + Disable information asset functionality that provides the capability for automatic execution of code on mobile devices without user direction.
  + Issue specially configured mobile devices to individuals traveling to locations (international locations which are considered sensitive by the Department of State) that the organization deems to be of significant risk in accordance with organizational policies and procedures.
* AC-15 Use of External Information Systems: All [Organization] Business Systems must establish terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information assets, allowing authorized individuals to:
  + Access the information asset from the external information systems.
  + Process, store, and/or transmit organization-controlled information using the external information systems.
* AC-16 Publicly Accessible Content: All [Organization] Business Systems must:
  + Designate individuals authorized to post information onto an organizational information system that is publicly accessible.
  + Train authorized individuals to ensure that publicly accessible information does not contain nonpublic information.
  + Review the proposed content of publicly accessible information for nonpublic information prior to posting onto the organizational information system.
  + Review the content on the publicly accessible organizational information system for nonpublic information.
  + Removes nonpublic information from the publicly accessible organizational information system, if discovered.

**4.1 Strong Password Requirements**

Strong passwords are long, the more characters you have the stronger the password. The [Organization] recommends a minimum of 14 characters in your password. In addition, we highly encourage the use of passphrases, passwords made up of multiple words. Examples include “*It’s time for vacation*” or “*block-curious-sunny-leaves*”. Passphrases are both easy to remember and type yet meet the strength requirements.

* 14 characters minimum
* Contain at least one capitalize letter, at least one lower case letter, at least one number and at least one special character
* Use of passphrases

Do not use poor, or weak, passwords have the following characteristics:

* Contain eight characters or less.
* Contain personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters.
* Contain number patterns such as aaabbb, qwerty, zyxwvuts, or 123321.
* Is some version of “Welcome123” “Password123” or “Changeme123”.

# In addition, every work account should have a different, unique password. To enable users to maintain multiple passwords, we highly encourage the use of ‘password manager’ software that is authorized and provided by the organization. Whenever possible, also enable the use of multi-factor authentication.

# Users must use a separate, unique password for each of their work-related accounts. Users may not use any work-related passwords for their own, personal accounts.

# User accounts that have system-level privileges granted through group memberships or programs such as Sudo must have a unique password from all other accounts held by that user to access system-level privileges. In addition, it is highly recommended that some form of multi-factor authentication is used for any privileged accounts

# Password Change

# Passwords should be changed only when there is reason to believe a password has been compromised.

# Password cracking or guessing may be performed on a periodic or random basis by the [Organization] Infosec Team or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it to be in compliance with the Password Construction Guidelines.

# Password Protection

# Passwords must not be shared with anyone, including supervisors and coworkers. All passwords are to be treated as sensitive, confidential [Organization] information. Corporate Information Security recognizes that legacy applications do not support proxy systems in place. Please refer to the technical reference for additional details.

# Passwords must not be inserted into email messages, Alliance cases or other forms of electronic communication, nor revealed over the phone to anyone.

# Passwords may be stored only in “password managers” authorized by the organization.

# Do not use the "Remember Password" feature of applications (for example, web browsers).

# Any user suspecting that his/her password may have been compromised must report the incident and change all passwords.

# Application Development

Application developers must ensure that their programs contain the following security precautions:

* + 1. Applications must support authentication of individual users, not groups.
    2. Applications must not store passwords in clear text or in any easily reversible form.
    3. Applications must not transmit passwords in clear text over the network.
    4. Applications must provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.

# Multi-Factor Authentication

# Multi-factor authentication is highly encouraged and should be used whenever possible, not only for work related accounts but personal accounts also.

# Remote Access Requirements

# Secure remote access must be strictly controlled with encryption (i.e., Virtual Private Networks (VPNs)) and strong pass-phrases. For further information see the Encryption Procedure and the Password Procedure.

# Authorized Users shall protect their login and password, even from family members.

# While using a [Organization]-owned computer to remotely connect to [Organization]'s [Organization] network, Authorized Users shall ensure the remote host is not connected to any other network at the same time, with the exception of personal networks that are under their complete control or under the complete control of an Authorized User or Third Party.

# Use of external resources to conduct [Organization] business must be approved in advance by the [Organization] CISO or Zone IT manager.

# All hosts that are connected to [Organization] internal networks via remote access technologies must use the most up-to-date anti-virus software, this includes personal computers. Third party connections must comply with all the requirements as stated in [Organization] IS policies.

# Personal equipment used to connect to [Organization]'s networks must meet the requirements of [Organization]-owned equipment for remote access as stated in the Hardware and Software Configuration Standards for Remote Access to [Organization] Networks.

# VPN Procedure Procedure

Approved employees and authorized third parties (customers, vendors, etc.) may utilize the benefits of VPNs, which are a "user managed" service. This means that the user is responsible for selecting an Internet Service Provider (ISP), coordinating installation, installing any required software, and paying associated fees. Further details may be found in the Remote Access Procedure in this procedure.

# It is the responsibility of employees with VPN privileges to ensure that unauthorized users are not allowed access to [Organization] internal networks.

# VPN use is to be controlled using either a one-time password authentication such as a token device or a public/private key system with a strong passphrase.

# When actively connected to the [Organization] network, VPNs will force all traffic to and from the PC over the VPN tunnel: all other traffic will be dropped.

# Dual (split) tunneling is NOT permitted; only one network connection is allowed.

# VPN gateways will be set up and managed by [Organization] network operational groups.

# All computers connected to [Organization] internal networks via VPN or any other technology must use the most up-to-date anti-virus software that is the corporate standard (provide URL to this software); this includes personal computers.

# VPN users will be automatically disconnected from [Organization]'s network after thirty minutes of inactivity. The user must then logon again to reconnect to the network. Pings or other artificial network processes are not to be used to keep the connection open.

# The VPN concentrator is limited to an absolute connection time of 24 hours.

# Users of computers that are not [Organization]-owned equipment must configure the equipment to comply with [Organization]'s VPN and Network policies.

# Only Infosec-approved VPN clients may be used.

# By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of [Organization]'s network, and as such are subject to the same rules and regulations that apply to [Organization]-owned equipment, i.e., their machines must be configured to comply with Infosec's Security Policies.

# Third Party Procedures

# Pre-Requisites Security Review

All new extranet connectivity will go through a security review with the [Organization] CISO. The reviews are to ensure that all access matches the business requirements in a best possible way, and that the principle of least access is followed.

# Third Party Connection Agreement

All new connection requests between third parties and the [Organization] require that the third party and representatives agree to and sign the Third-Party Agreement. This agreement must be signed by the [Organization] CISO as well as a representative from the third party who is legally empowered to sign on behalf of the third party.  By signing this agreement, the third party agrees to abide by all referenced policies. The signed document is to be kept on file with the relevant extranet group.  All non-publicly accessible information is the sole property of the [Organization].

# Business Case

All extranet connections or network resource access must be accompanied by a valid business justification, in writing, that is approved by both the third party and the [Organization] CISO. Typically, this function is handled as part of the Third-Party Agreement.

# Point of Contact

The [Organization] CISO contracting authority must designate a person to be the Point of Contact (POC) for the third-party connection. The POC acts on behalf of the [Organization] CISO contracting authority and is responsible for those portions of this procedure and the “Third Party Agreement” that pertain to it. If the POC changes, the relevant third-party person or organization, must be informed promptly.

# Establishing Connectivity

All contracting authorities within that wish to establish connectivity or network resource access to a third party are to file an Extranet connectivity request with the [Organization] CISO accompanied by a “Third Party Agreement” signed by the third party person, organization, or rightful designee.  The [Organization] CISO will then engage the third party to address security issues inherent in the project. The sponsoring contract authority must provide full and complete information as to the nature of the proposed access to the [Organization] CISO, as requested. All connectivity established must be based on the least-access principle, in accordance with the approved business requirements and the security review. All connectivity requests will have a specific beginning and ending date.  In no case will rely upon the third party to protect network or resources.  The [Organization] CISO will grant access to all approved resources and reserves the right to refuse access since legitimate security concern as decided by the [Organization] CISO**.**

# Modifying or Changing Connectivity and Access

All changes in access must be accompanied by a valid business justification and are subject to security review.  The sponsoring contracting authority is responsible for notifying the third-party person or organization and the [Organization] CISO when there is a material change in their originally provided information so that security and connectivity evolve accordingly.  Extensions will be granted on a case by case basis and must be requested in writing by the sponsoring contracting authority.

# Terminating Access

When access is no longer required, the sponsoring contracting authority within the [Organization] must notify the [Organization] CISO, who will then terminate the access. This may mean a modification of existing permissions up to terminating the circuit, as appropriate. IT security teams must conduct an audit of their respective connections on an annual basis to ensure that all existing connections are still needed, and that the access provided meets the needs of the connection. Connections that are found to be deprecated, and/or are no longer being used to conduct business or other approved business transactions will be terminated immediately. Should a security incident or a finding that a circuit has been deprecated and is no longer being used to conduct business or other approved business transactions necessitate a modification of existing permissions, or termination of connectivity, the [Organization] CISO will notify the POC of the sponsoring contracting authority of the change prior to taking any action.

# Documentation

The documentation shall consist of software installation Procedure, and related procedures and guidelines. The Compliance Procedure document and all other referenced documents shall be controlled. Version control shall be to preserve the latest release and the previous version of any document. However, the previous version of the documents shall be retained only for a period of two years for legal and knowledge preservation purpose.

# Records

Records being generated as part of this Procedure shall be retained for a period of two years. Records shall be in hard copy or electronic media. The records shall be owned by the respective system administrators and shall be audited once a year.

# Procedure Compliance

* 1. **Compliance Measurement**

The [Organization] management team will verify compliance to this procedure through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the procedure owner.

* 1. **Exceptions**

Any exception to the procedure must be approved by the [Organization] IT team in advance.

* 1. **Non-Compliance**

An end user found to have violated this procedure may be subject to disciplinary action, up to and including termination of appointment to the [Organization].

# Related Standards, Policies and Processes

The following references illustrate public laws which have been issued on the subject of cyber security and should be used to demonstrate [Organization] responsibilities associated with protection of its cyber assets.

1. United States Department of Commerce National Institute for Standards and Technology (NIST) Special Publication 800-53 Recommended Security Controls for Federal Information Systems Revision 3, Technical Controls, Access Control Family, August 2009.
2. United States Department of Commerce National Institute for Standards and Technology (NIST) Special Publication 800-100 “Information Security Handbook: A Guide for Manager” October 2006.
3. United States Department of Commerce National Institute for Standards and Technology (NIST) Special Publication 800-46 “Guide to Enterprise Telework and Remote Access Security” June 2009.
4. United States Department of Commerce National Institute for Standards and Technology (NIST) Special Publication 800-113 “Guide to SSL VPNs” July 2008.
5. United States Department of Commerce National Institute for Standards and Technology (NIST) Special Publication 800-114 “User’s Guide to Securing External Devices for Telework and Remote Access” November 2007.
6. United States Department of Commerce National Institute for Standards and Technology (NIST) Special Publication 800-121 “Guide to Bluetooth Security” September 2008.
7. United States Department of Commerce National Institute for Standards and Technology (NIST) Special Publication 800-48 “Guide to Securing Legacy IEEE 802.11 Wireless Networks” July 2008.
8. United States Department of Commerce National Institute for Standards and Technology (NIST) Special Publication 800-94 “Guide to Intrusion Detection and Prevention Systems (IDPS)” February 2007.
9. United States Department of Commerce National Institute for Standards and Technology (NIST) Special Publication 800-97 “Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i” February 2007.
10. United States Department of Commerce National Institute for Standards and Technology (NIST) Special Publication 800-124 “Guidelines on Cell Phone and PDA Security” October 2008.
11. United States Department of Commerce National Institute for Standards and Technology (NIST) Special Publication 800-77 “Guide to IPsec VPNs” December 2005.

# Definitions and Terms

# Revision History

|  |  |  |
| --- | --- | --- |
| **Date of Change** | **Responsible** | **Summary of Change** |
| Sept 27, 2023 | [Organization] | Created initial draft |
|  |  |  |