**User-Access Control Policy**

# Purpose

<Organization Name> <Insert Organization Mission Here>. This policy establishes the Enterprise Access Control Policy, 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 Name> implement security best practices with regard to logical security, account management, and remote access.

# Scope

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

# Intent

The <Organization Name> Information Security policy serves to be consistent with best practices associated with organizational Information Security management. It is the intention of this policy to establish an access control capability throughout <Organization Name> and its business units to help the organization implement security best practices with regard to logical security, account management, and remote access

# Policy

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

* **AC-1 Access Control Procedures:** All <Organization Name> 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 Name> 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 Name> Business Systems must enforce approved authorizations for logical access to the system in accordance with applicable policy.
* **AC-4 Information Flow Enforcement:** All <Organization Name> Business Systems must enforce approved authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy.
* **AC-5 Separation of Duties:** All <Organization Name> 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 Name> 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 Name> 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 Name> Business Systems must limit the number of concurrent sessions for each system account to **ten** for information assets.
* **AC-10 Session Lock:** All <Organization Name> 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 Name> 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 Name> Business Systems must identify specific user actions that can be performed on the information asset without identification or authentication. In addition, <Organization Name> 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 Name> 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 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 Name> 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 Name> 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 Name> 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 Name> 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.

**Source:** <https://www.google.co.in/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&uact=8&ved=0ahUKEwjXkoqqrrvMAhWi5KYKHY7ZCTsQFggiMAE&url=http%3A%2F%2Fg3ctoolkit.net.s3-website-us-west-2.amazonaws.com%2Fia%2FSecPol%2FwmspDownloads%2FIT_Access_Policy.doc&usg=AFQjCNGJH2eJKwLuXomf9LhBFEYt1NWzRw&bvm=bv.121070826,d.dGY>