Henry Post

ITMS 428

Access Controls

Contents

[[AC-2]: Account Management 1](#_Toc525914170)

[2. Removal of temporary/emergency accounts 1](#_Toc525914171)

[3. Disable inactive accounts 1](#_Toc525914172)

[5. Inactivity logout 1](#_Toc525914173)

[6. Dynamic Privilege Management 1](#_Toc525914174)

[8. Dynamic Account Creation 1](#_Toc525914175)

[11. Usage Conditions 1](#_Toc525914176)

[12. Account Monitoring / Atypical Usage 2](#_Toc525914177)

[[AC-3]: Access Enforcement 2](#_Toc525914178)

[2. Dual Authorization 2](#_Toc525914179)

[3. Mandatory Access Control 2](#_Toc525914180)

[a. Uniform enforcement of access control policy over all subjects and objects 2](#_Toc525914181)

[b. A subject that has been granted access to information is constrained from doing any of the following: 2](#_Toc525914182)

[5. Security-Relevant Information 3](#_Toc525914183)

[[AC-5]: Separation of Duties 3](#_Toc525914184)

[a. Separates [**Assignment: organization-defined duties of individuals**] 3](#_Toc525914185)

[b. Documents separation of duties of individuals 3](#_Toc525914186)

[[AC-6] Least Privilege 4](#_Toc525914187)

[[AC-7] Unsuccessful logon attempts 4](#_Toc525914188)

[2. Purge / Wipe mobile device 4](#_Toc525914189)

[References and citations 5](#_Toc525914190)

# [AC-2]: Account Management

## 2. Removal of temporary/emergency accounts

All automatic or temporary accounts, especially those with high privileges, shall be terminated after [**Assignment: organization-defined frequency**] of inactivity.

## 3. Disable inactive accounts

All accounts inactive for more than [**Assignment: organization-defined frequency**] shall be automatically disabled until the user who owns the account logs in.

## 5. Inactivity logout

All currently active login sessions bound to a user that are inactive for longer than [**Assignment: organization-defined frequency**] shall be invalidated.

## 6. Dynamic Privilege Management

All modes of authentication that are password or encrypted-key based shall be changed or rotated every [**Assignment: organization-defined frequency**].

## 8. Dynamic Account Creation

All account creation, except for emergency or temporary accounts, shall be automated.

In addition to this, the priviledges granted for these accounts shall be generated dynamically and of appropriate scope for the type of entity causing them to be generated.

Example: New hires who work on the user interface of the Organization’s website shall have a user associated with their person which can access, modify, delete, and update the resources required to change how the user interface presents data and arranges it for users.

They shall not, however, be able to perform manipulations on systems that are outside of the scope of their tasks, such as modifying how authentication is handled or APIs that the site may provide to developers.

## 11. Usage Conditions

The usage of user accounts shall be restricted to times that the user is normally expected to be using that account.

This can be described on a per-user basis, by the group(s) they belong to, and/or by an organization-wide policy.

## 12. Account Monitoring / Atypical Usage

If, at any time, a login is attempted outside of normal operating times, especially at a time when few people are monitoring the system, that event shall be captured, along with as much information about the source of the login attempt.

It is up to the discretion of the organization to decide which events shall warrant an audit, but it is recommended for events similar to those described in the example below.

Example: A user who normally works 9am-5pm on Monday to Friday at a Los Angeles location attempts to log in at 1AM on a Sunday, from Sri Lanka.  
  
That login attempt shall be recorded, and an audit shall be performed on the user and/or any groups that the user in question belongs to.

All login attempts, session lengths, locations, IP addresses, and (esp.) suspicious connection attempts shall be monitored.

# [AC-3]: Access Enforcement

## 2. Dual Authorization

Dual authorization shall be implemented in the following forms:

* All users shall implement as many of the procedures listed below as possible:
* All users shall carry with them a key fob (NOT RFID or any system susceptible to radio snooping)
  + All key fobs shall generate rotating codes each [**Assignment: organization-defined frequency**], synchronized with a key server which keeps track of each key fob’s ‘seed’ used to generate a code.
* All users shall carry with them a USB key containing a private key they receive every [**Assignment: organization-defined frequency**], which will be rotated as needed.
  + This private key will be used to verify the user by generating a signature whenever the user needs access to a system.

## 3. Mandatory Access Control

### a. Uniform enforcement of access control policy over all subjects and objects

All users shall be subject to the access control policy over the jurisdiction of the information system.

### b. A subject that has been granted access to information is constrained from doing any of the following:

* Divulging information to users or objects which do not have the permissions to access such information on their own
* Performing modifications to the information system that is either:
  + Outside of their jurisdiction (*in which case, they should not have the privileges to perform the modification in the first place*), or
  + Not immediately necessary for them to do to accomplish their assigned tasks.

## 5. Security-Relevant Information

Access to all secure operations (i.e. generation of keys, verification of keys, the code that controls credential rotation) shall be forbidden when the system is operating business-related processing.

# [AC-5]: Separation of Duties

## Separates [**Assignment: organization-defined duties of individuals**]

Organizations shall decide which privileges users need to perform assigned tasks.

In addition to this, for groups of users with similar tasks, the privileges shall be as uniform as possible.

Maintenance done on the information system that involves different systems shall be split across different people and tasks will be delegated based on what subsystem an individual is tasked with maintaining.

## Documents separation of duties of individuals

Per-group privileges will be documented in a living document, and disseminated to all users who belong to the group.

All users shall only be permitted to know their privileges and the privileges of those with less sensitive access than them.

1. Defines information system access authorizations to support separation of duties

Organization shall configure separate access levels, groups, and/or accounts to enforce the separation of duties across different individuals and classes of individuals.

In addition to this, safeguards protecting different subsystems from each other shall be implemented such that if one subsystem is totally compromised, it cannot perform unauthorized operations on another subsystem.

Example: The MySQL server for forum threads is entirely compromised, with attackers remotely accessing it. However, with their current credentials and all other things found on that server, they are unable to penetrate the MariaDB server for user credentials, or any other server.

# [AC-6] Least Privilege

Organizations shall employ the principle of ‘least privilege’, giving only the necessary privileges to users that are required to accomplish tasks they have been assigned.

In addition to this, each [**Assignment: organization-defined frequency**], audits shall be performed to determine whether or not a user or group of users still require their current privileges, or if they can be reduced.

# [AC-7] Unsuccessful logon attempts

A limit of [**Assignment: organization-defined number**] unsuccessful login attempts shall invalidate whatever credentials a user is using to login.

In addition to this, a full audit shall be performed upon the user whose account is accessed.

If this occurs repeatedly, an audit against a larger system, subsystem, or group of users may be performed.

## 2. Purge / Wipe mobile device

If [**Assignment: organization-defined number**] unsuccessful login/decryption/authentication attempts are made on any mobile device containing sensitive data, its data shall be irrecoverably wiped from it using a sufficiently strong data wiping technique.

# References and citations

“NVD – Rev4.” *NVD - CVE-2017-5638*, <https://nvd.nist.gov/800-53/Rev4>