UNIVERSITY OF CENTRAL FLORIDA

# University Standards

| | |
|---|---|
| **Subject:** | User Account Standards |
| **Standards Number:** | 502 |
| **Effective Date:** | 3/15/2020 |
| **Revised Date:** | 3/7/2021 |
| **Responsible Authority:** | Information Security Office |
| **Pages:** | 5 |

## ACCOUNTABILITY/APPLICABILITY:

This standard applies to UCF enterprise domain accounts, the permissions assigned to them and when it is appropriate to use a given account.

## STANDARDS STATEMENT:

This standard explains the different types of credentials and forms of authentication that may be used by UCF Staff, particularly staff in an IT or technical role on the UCF enterprise domain. For each type of credential, a brief explanation is given, as well as they types of scenarios in which it should be used.

## STANDARDS:

### 1. NID Account

**Use Cases for NID Account:** The NID is for everyday end user activities. The NID account on its own should not be used for most privileged activities or to access highly restricted data. Instead, users should use either NID protected with MFA, or NIDadmin, as described below.

### 2. NID Account, protected with MFA

**Use Cases for Protecting a NID Account with MFA:** Some NID accounts have elevated privileges and/or higher risks associated with their use. These are accounts require MFA to add an additional layer of protection.

- Application Administrators or Owners
- Privileged Users within an Application: Any application users that have access to another user or user's data
- Developers: access to secure coding environments, Visual Studio, SQL server management server (SSMS), access to code push pipelines, etc.
- Any end users accessing highly restricted data within an application



Phone: 407.823.2711 • Fax: 407.882.9006 • Web: infosec.ucf.edu • Email: infosec@ucf.edu

## 3. NIDadmin, protected with MFA

a. **Use Cases for NIDadmin:** These accounts may be responsible for installing, maintaining, configuring, or access control, on systems such as servers and infrastructure. More specifically:

- Server administration, e.g. configuring a web/database/application server
- Database administration: configuring, adding, deleting databases or the elements within them (schemas, tables, etc)
- Endpoint support – configuration, deployment, support, and maintenance of endpoint/client systems such as desktops, laptops, and mobile devices.

Generally, the NIDadmin is intended to provide a dedicated account for the administration of systems, therefore:

- NIDadmins should not be requested and used for the sole purpose of protecting access to data such as Highly Restricted data, such as within an application – use a NID protected with MFA instead.
- NIDadmins should not be requested and used for administrative roles within an application (e.g. software products or web applications) – use a NID protected with MFA instead.
- NIDadmins should not be requested for an end user to make certain applications that require administrator permissions function, or for day-to- day job responsibilities. Other means, such as AppSense, should be used to grant more granular elevated permissions without a dedicated administrator account.

### b. NIDadmin Standards

- NIDadmins are assigned on an as needed basis
- NIDadmins are assigned for each domain the account owner has responsibilities for maintaining (e.g., production/NET and non-production/NETDEV domains)
- NIDadmin accounts provisioned for endpoint support should not be permitted interactive login to servers and other infrastructure. NIDadmins provisioned for the purposes of infrastructure and server administration should not be permitted interactive login to endpoints.
    - Exceptions are permitted to employees with a valid business reason of a mixed role that necessitates access to both desktops and infrastructure (e.g. Endpoint Engineering teams) who typically do not perform direct, tier 1 deskside support.
- NIDadmin accounts must be protected with MFA wherever technically feasible
- NIDadmin accounts should only use mobile-app based push as the MFA second factor.
- NIDadmin accounts are privileged accounts and must follow the Privileged Account Password Standard 501 found here: Infosec.ucf.edu > Policies and Standards > 501 Password Standards



Phone: 407.823.2711 • Fax: 407.882.9006 • Web: infosec.ucf.edu • Email: infosec@ucf.edu

### c. NIDadmin Owner Responsibilities

- Accounts should be returned or disabled if it is no longer needed to complete one's job responsibilities
- NIDadmin account owners should maintain their NIDadmin account password in an approved and industry vetted password safe. Account owners are not expected to memorize their password as the password safe should always store the correct and updated password

## 4. Domain Admins, protected with MFA

### a. Use Cases for Domain Admin accounts

- Domain admins are used exclusively for accessing domain controllers.
- Domain admin accounts should not have access to any other systems or applications.

### b. Domain Admin account standards

- Domain admin accounts must be protected with MFA.
- Domain admin accounts must only use mobile-app based push or app-generated one time codes as the MFA second factor (not SMS or telephone)

## 5. Other Accounts: Use Cases and Standards

All accounts in the domain should be organized into the appropriate Organizational Unit.
All accounts in the domain should follow a naming standard (see NET domain naming standards).

- **Lab Accounts** - A domain account that should be used in lab environments where the machine is automatically logged on.
  - Lab accounts passwords can be set to not expire, but should be rotated.
- **Test Accounts** - A domain account that is used to test access to systems or settings for troubleshooting purposes
  - To protect end-user support staff NID credentials, End-user support staff should use Test accounts for interactive login to endpoints for initial triage, testing, or troubleshooting purposes, not their personal NID.
  - Test accounts should have extremely limited permissions and access and should not have access to a user's personal files, department shares, etc.
  - Test accounts should have passwords that are different from any users NID or NIDadmin.
  - Test Accounts passwords should expire after 365 days.
- **Service Accounts** - A domain account for non-interactive logon purposes and background processes. This account should be used to run scheduled tasks and services on servers
  - Service accounts passwords are set to not expire.
- **Kiosk Accounts** - A domain account for use in kiosk environments where the machine is automatically logged on in kiosk mode
  - Kiosk account passwords can be set to not expire, but should be rotated.
- **Wireless Accounts** - A domain account for wireless devices to permit access to the UCF_WPA2 wireless network (not VPN). This account may be used for any laptops, tablets, phones, or other wireless that require shared access among users



Phone: 407.823.2711 • Fax: 407.882.9006 • Web: infosec.ucf.edu • Email: infosec@ucf.edu

## DEFINITIONS:

**MFA:** The Information Security Office (ISO) and UCF IT implemented the Multi-factor Authentication (MFA) service to protect systems containing sensitive information. MFA provides an additional layer of authentication on top of the standard NID account.

A system protected with multi-factor authentication asks users to verify their identity two different ways during the sign on process. For example, myUCF requires users to enter a password (the first factor) and use a second device such as their mobile device to click an "approve" button or provide a passcode sent to it (the second factor).

**NID:** The Network ID (NID) is a credential that allows students, faculty, staff and UCF affiliated individuals to sign into the computer labs, myUCF portal, webcourses@UCF and other campus resources. For more information on the uses for the NID, visit https://infosec.ucf.edu/identity-management/identity-details/

**NIDadmin:** NID Administrator accounts are administrative accounts with special or elevated privileges to systems and applications.

## RELATED DOCUMENTS:

1. 4-008 *Data Classification and Protection* policy
2. NET Domain Naming Standards

## CONTACTS:

| | |
|---|---|
| Information Security Office<br>https://infosec.ucf.edu<br>infosec@ucf.edu | Security Incident Response Team (SIRT)<br>https://infosec.ucf.edu/incident-response/<br>sirt@ucf.edu |
| Identity Access Management (IAM)<br>https://infosec.ucf.edu/iam<br>iam@ucf.edu | UCF IT Support Center<br>(407) 823-5117<br>https://ucf.service-now.com/ucfit<br>itsupport@ucf.edu |

| Revision Date | Summary of Change |
|---|---|
| 3/7/2021 | • Changed test account password expiration from 60 days to 365 days. |
| | |
| | |

**INITIATING OFFICE:** Information Security Office

**STANDARDS APPROVAL**
(For use by the Information Security Office)

Standards Number: *502*

Initiating Office: [Information Security Office]

Chief Information Security Officer: *Chris Vakhordjian*

Signature: chrisv chrisv dc=edu, dc=ucf, dc=net, ou=People, cn=chrisv, email=Chris.Vakhordjian@ucf.edu 2021.04.16 16:24:32 -04'00' Date: 4/16/2021



Phone: 407.823.2711 • Fax: 407.882.9006 • Web: infosec.ucf.edu • Email: infosec@ucf.edu