UNIVERSITY OF CENTRAL FLORIDA

University Standards

Subject:	IT Account Standards
Standards Number:	502
Effective Date:	3/15/2020
Revised Date:	4/12/2025
Responsible Authority:	Information Security Office
Pages:	15

ACCOUNTABILITY/APPLICABILITY

This standard applies to all UCF accounts, the permissions assigned to them and when it is appropriate to use a given account. This includes all stand-alone systems, directory, and domain-based accounts across the university.

PURPOSE AND BACKGROUND

To protect the confidentiality, integrity, and availability of the University of Central Florida's computing systems and the data that resides on those systems, students, employees, and sponsored guests must be granted University IT accounts in accordance with UCF policies and standards (see policy 4-002, Use of Information Technologies and Resources policy).

This standard establishes the criteria for provisioning accounts and associated privileges for all users, as well as de-provisioning criteria for those accounts. Accounts and services are provisioned based upon user affiliation and status, such as whether a student is active, or an employee has retired from the University.

STANDARDS STATEMENT

Establishing different account types based on their purpose, access privileges, and required forms of authentication support the access control process and limit the transactions and functions to only those required. The principles of least privilege and a tiered security model outlined in this standard are to be followed to manage accounts, regardless of domain /directory or system. A defined process to request, approve, monitor, and deactivate an account must also be established to ensure access is restricted to only authorized users and accounts.

Accounts are to be organized in a directory / domain and follow a naming standard. The naming conventions in this standard reflect those in the UCF enterprise domain. For each account type, a brief explanation is given, as well as scenarios in which an account may be activated (provisioned), deactivated (de-provisioned) and used. Naming conventions may vary in other systems but must be documented.

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

DEFINITIONS:

Bastion: Microsoft Bastion is a secure gateway service that allows PAW devices to connect to the Azure and data centers (both on premises and cloud data centers) to manage servers.

Cloud Only (CO) Account: An account that only exists in the cloud directory and not in the on-premises directory. The goal of these accounts is to separate the on premises and cloud management planes and limit the scope of administration (and therefore overall risk).

Domain / Directory: A directory service developed to manage user accounts, permissions, and access rights in a central location. Changes to accounts and permissions are applied across the network.

De-provisioning: The processes designed to adjust or remove access to an organization's resources from an account. The decommissioning of an account's access.

DTC_Atlas Account: A standard user account provisioned to UCF's partner Valencia college users. It provides limited access to actively enrolled students and employees of our partner institutions for the purpose of accessing UCF IT resources in shared learning environments. These accounts follow the partner institution's naming standard.

MFA: The Information Security Office and UCF IT implement the Multi-factor Authentication (MFA) service to protect system access to sensitive information. MFA provides an additional layer of authentication in addition to the account password. A system protected with multi-factor authentication asks users to verify their identity two or more separate ways during the account authentication (sign on) process. For example, myUCF requires users to enter a password (the first factor) and use a second device to respond to an MFA challenge (the second factor).

NID: The Network ID (NID) is a standard account credential provisioned to students, faculty, staff and UCF affiliated individuals (e.g., sponsored accounts and contingent workers) 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/

Non-Paid Appointment: A legacy account affiliation assigned a NID from the student information system. These accounts must be entered into in the system by an employee of the university who is authorized to do so within the student information system.

OID: The "Organizational ID" (OID) is a departmental account used for email and sometimes voice services.

Privileged Access Workstation (PAW): A specialized workstation deployed with the "clean keyboard" methodology. PAWs are used by IT admins and security teams for tasks requiring the highest levels of access within an enterprise network to manage critical systems and cloud services. PAW workstations have a highly restricted attack surface and operate at the same security level as tier zero. They have restricted applications (no productivity applications), restricted web browsing, and are designed for performing sensitive administrative tasks.

Privileged Accounts: Accounts that require additional authorization that are granted special or elevated privileges to control, monitor, or administer a system or device. Privileged accounts

are separate from an individual's standard account credential. "NIDadmin" is the name used to describe privileged administrative accounts, however, there are several diverse types of NIDadmin accounts described in the user account standard.

Security Tiers: The Tier model of administration is a security framework designed to protect enterprise environments by segmenting administrative privileges into different tiers. Privileges should never be raised from a lower to higher tier. The Tiers are based on the Bell-LaPadula model which emphasizes data confidentiality and controlled access. UCF's tier model includes:

- **Tier 0**: This is the highest level of privilege, encompassing domain controllers, enterprise admins, and other critical infrastructure components. Administrators at this level have control over the entire environment and can manage identity and permissions enterprise-wide.

- **Tier 1**: This tier includes administrators who manage enterprise member servers and applications. These administrators have significant control over business-critical resources but do not have the same level of access as Tier 0 administrators.

- **Tier 2:** This tier consists of administrators who manage user workstations and devices. They have just enough privilege to achieve their endpoint support objectives and cannot control Tier 0 or Tier 1 resources.

Service Accounts: An account type intended for processes, not users. It is used for non-interactive logon purposes to run administrative background processes.

Guest Accounts: An account type intended for non-employees who are engaged in an official working capacity with the university. Account holders must have a demonstrated business need and be sponsored by an employee. Guest accounts are time-limited.

- **Contingent Worker:** A guest account affiliation assigned a NID from the Workday human resources system granted a specific level of access in the Workday ERP system. This role is suitable for courtesy faculty, contractors, consultants, or other non-employees who are required to use Workday and other UCF systems.

- **External Business to Business (B2B) Guest Collaboration Accounts:** A guest account provisioned from an external identity system. Members of UCF's directory can invite university business partners to collaborate and share applications and services with external B2B guest accounts from within the university's own tenant. This account type uses the account holder's home organization's account and is not provisioned a university NID user account. This role is best suited for research, academic, and business communication collaborations and document sharing.

- **Sponsored Accounts:** A guest account that originates from the sponsored account system. These time-limited accounts must be sponsored by an employee of the university, or their designee provided a memorandum of understanding is in place with the Information Security Office. Employees can request sponsored accounts for individuals such as associates, consultants, contractors, students who perform work in a non-paid capacity, or guests who, for legitimate purposes, require access to technology resources during their temporary affiliation with UCF. Sponsors can request additional access as needed, such as email or other UCF systems (except Workday which requires the contingent worker affiliation).

STANDARDS:

STANDARD ACCOUNTS

Use Case for Standard User Accounts

A standard account is the default and first account type to be issued to an individual based on a defined affiliation with UCF. Standard accounts are to be used for non-security functions. More information is available at: Identities At UCF - UCF Information Security

Assignment of Standard User Accounts

The provisioning and de-provisioning of NID accounts is based on affiliation (e.g., student, employee, guest) and relationship information derived from source systems such as the myUCF student information system (SIS), Workday Human Resources system, and others.

Once a standard account is de-provisioned, any associated privileged accounts must also be de-provisioned.

Authorized Transactions and Functions

- A standard account is designed for routine end-user business tasks such as signing into computers, checking email, accessing applications, web browsing, and basic file management. These accounts should not have administrative (system) privileges, a separate privileged account should be used instead.
- When a standard account (NID) is used to access highly restricted data, MFA must be used. Such access represents a higher risk, and MFA provides an additional layer of protection. The most common cases where MFA is required are:
  - End users accessing highly restricted data within an application.
  - Application user with access to another user or user's data.
  - Application administrators or owners.
  - Developers accessing secure coding environments, Visual Studio, SQL server management server (SSMS), access to code repositories and deployment pipelines, etc.

Requirements for Review and Sustainment of Standard User Accounts

The provisioning of an account is based on affiliation to the university. De-provisioning also follows rules specific to an account's purpose. The common de-provisioning scenarios are:

Employees:
For faculty and staff, de-provisioning starts after the last day of employment (i.e., separation date). Access is removed on the separation date, however former employees can still obtain their electronic W2 for the next tax season.

- **Adjunct, GTA/GRAs:** Those in the adjunct, graduate teaching assistant (GTA), and graduate research assistant (GRA) job families retain access for one year after their separation date.

- **Retired Faculty:** Faculty who retire from the university whose position was represented by the United Faculty of Florida collective bargaining agreement can request access to email (an email only account). Login must occur at least once per year to maintain email access. If no login is detected within the last year, access is de-provisioned.

- **Researchers who separate from the university:** Per agreements with the Office of Research to support ongoing research collaboration, researchers can request a read only email account (email only). Login must occur at least once per year to maintain email access. If no login is detected within the last year, access is de-provisioned.

Students:

- **Completed Students:** Any student who completed their academic program will be provided with one-year of email access and keep their account for two years.

- **Discontinued undergraduates:** will remain active for two years giving them the ability to reapply if they choose. If the discontinued student completes any other degree after their discontinued undergraduate career they may be deactivated.

- **UCF Global Students:**
  - J Scholars who reach their DS-2019 end date may be deactivated.
  - J Students or F visa holders will be active for three years after their completion date OR after their OPT ends.

- **Undergraduate and Graduate Studies No-Show Applicants:** Such students may be discontinued and their account de-provisioned 12 months after the admit date.
  - **Undergrad Career** includes those who were admitted, withdrew their application, or had their admission revoked.
  - **Graduate Career** includes those who withdrew their application, or had their admission revoked. Graduate students may also be deactivated if they have discontinued their academic program careers.

- **Monetary or Financial Obligation Holds:** Anyone with an outstanding balance on their university account may have their NID account services suspended until the hold is removed.

- **College of Medicine Students:** Those enrolled in the college of medicine are provided with two years of email access after having completed their last enrolled class and are then de-provisioned.

- **Guest Accounts:** Access is removed immediately following the expiration date.

- **External Business to Business (B2B) Guest Accounts:** Periodically, external B2B guests who have not signed in for 30 days may have their access removed.

Standard User Account Owner Responsibilities

- Follow the 501 Password Standard when setting passwords for standard accounts.
- Safeguard the account as recommended within information security policies and standards.
- Never use the account for security functions or system administrative tasks.
- Safeguard the account with MFA wherever technically feasible.

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

NID ACCOUNTS	
NAMING CONVENTION	**ACCOUNT DESCRIPTION**
NID	The UCF assigned Network ID (NID) is the account name used for standard accounts in the university's enterprise directory.
Standard accounts must meet the requirements listed above and those outlined by the source systems that establish the account.	

LAB ACCOUNTS	
NAMING CONVENTION	**ACCOUNT DESCRIPTION**
LAB_{DEPT}_{LAB_NAME} Example: LAB_IT_TC1	A domain account that should be used in lab environments where the machine is automatically logged on. Lab accounts may also be used for temporary, time-limit (e.g., a week or less but more typically a day) access during special events (e.g., conferences, briefings, etc.) These time limited accounts may use a friendly naming convention and must be set to expire in one week or less.
• Lab accounts passwords can be set to not expire but should be rotated. • Must set long and unguessable passwords per 501 Password Standard for privileged accounts.	

KIOSK ACCOUNTS	
NAMING CONVENTION	**ACCOUNT DESCRIPTION**
KSK_{DEPT}_{SERVICE_NAME} Example: KSK_IT_TC101	An account for use in kiosk environments where the machine is automatically logged on in kiosk (limited access typically for a specific application or website) mode.
• Kiosk account passwords can be set to not expire but should be rotated. • Must set long and unguessable passwords per 501 Password Standard for privileged accounts.	

EXTERNAL BUSINESS TO BUSINESS (B2B) GUEST COLLABORATION ACCOUNTS	
NAMING CONVENTION	**ACCOUNT DESCRIPTION**
None (accounts are based on email address from the guest's identity management system)	**B2B Guest Account** A guest account provisioned from an external identity system. This account type uses the account holder's home organization's account and is not provisioned a university NID user account. Example: {Email of guest@{guest's domain}}.{top level domain}
• Once a UCF account holder invites a guest to collaborate within office 365 or teams, they are responsible for managing that individual's access. Careful attention is needed when providing access to non-academic teams, files, and research. All requirements to access information must also be satisfied prior to providing access (e.g., training, agreements, etc.) • Access should only be granted for the time needed and then removed.	

- External B2B guest accounts should not be used when requirements dictate that a sponsored account or contingent worker account would be more appropriate.
- By using their access, all external B2B guests agree to follow all applicable policies, standards, etc. (e.g., 4-008 the Data Classification and Protection policy).

SHARED MAILBOXES AND OID ACCOUNTS	
NAMING CONVENTION	**ACCOUNT DESCRIPTION**
{Email Address Display Name} Example: Admissions.ucf.edu	**OID.** The "Organizational ID" (OID) is a departmental account used for email and sometimes voice services. Whenever possible, OIDs should be converted to "Shared Mailboxes". Shared Mailboxes are a type of OID account that do not require account passwords.

- Enterprise directory service accounts must be requested through ITSM request processes.
- Must have at least one owner and up to a maximum of three owners.
- Sometimes referred to as "Organizational ID" or "Departmental Accounts" are email and/or voice enabled accounts issued explicitly for the purposes of unified communications. They provide colleges and departments with a single point of contact that multiple employees can check and maintain. They are not intended for any other purposes.
- OIDs should never be used as service accounts

WIRELESS ACCOUNTS	
NAMING CONVENTION	**ACCOUNT DESCRIPTION**
WLS_{Dept}_Purpose Example: WLS_IT_FrontDeskiPad	**Wireless Service Account.** A domain account for wireless devices to permit access to the UCF_WPA2 wireless network (not VPN). Wireless service accounts may also be used for temporary, time-limit (e.g., a week or less but more typically a day) access during special events (e.g., conferences, briefings, etc.) where wireless network conductivity will be provided. These time limited accounts may use a friendly naming convention.

- This account may be used for any laptops, tablets, phones, or other wireless that require shared access among users.
- Should not be assigned any other services.
- With approval from the information security office, accounts may be temporarily used as a conference ID for on campus affiliated and hosted conferences.

PRIVILEGED ACCOUNTS

Use Case for Privileged Accounts

A privileged account is separate from an individual's standard user account and is used to control, monitor, or perform management and system administrator activities such as modifying an operating system (OS) or application settings.

Assignment of Privileged Accounts

Privileged accounts are assigned on an as needed basis where there is demonstrated need to perform an individual's job responsibilities. Privileged accounts are only to be issued (or renewed) for individuals affirmed to meet all applicable account requirements.

Authorized Transactions and Functions:

Privileged account owners must respect their functional access authority limits, the rights of system users, and comply with relevant university policies, standards, and guidelines.

- A privileged account is to be used only when performing system administrative duties or other elevated functions, tasks defined for standard accounts (e.g., routine business productivity activities, accessing email, browsing internet) are not to be performed.
- Privileged accounts must not be used for unauthorized viewing, modification, copying, or destruction of system or user data.

Requirements for Review and Sustainment of Privileged Accounts

- User identity is known to the university, there is a demonstrated need for the account to perform the individual's role, function, or job responsibilities, and access is endorsed by applicable parties for the specific privileged account type.
- Personnel Screening(s) has been conducted. Privileged accounts minimally require a standard background check (see UCF Policy 3-011 Background Checks) and may include affirmation of U.S. Person status if export controlled technical data is involved. Accounts issued to manage a single endpoint may not require a background check.
- University required Security Awareness, Privileged User, and any applicable role-based training must be complete and current upon initial issue and renewal. Link in references.
- Accounts must be formally reviewed on an annual basis and de-provisioned when the need to perform administrative or privileged duties for which the account is used no longer exists (e.g., a transfer of job, change of responsibilities, or termination of employment).
- Privileged accounts must be de-provisioned when the standard account is de-provisioned.

Privileged Account Owner Responsibilities

- Inform IT when account is no longer required.
- Adhere to security policies and exclusively use privileged account for its intended purpose.
- Set long and unguessable passwords per 501 Password Standard for highly privileged accounts. Account owners are not expected to memorize their password as the password safe should always store the correct and current password.
- Exercise the utmost care when managing their FIDO2 token. Always store the FIDO2 token in a secure location when not in use. Avoid leaving it unattended or in easily accessible areas. Never share the FIDO2 token with others. It is a personal security device and should only be used by the designated administrator. Account owners must immediately report lost or stolen FIDO2 tokens to the UCF Information Security Office's Identity and Access Management Team and Security Incident Response Team.

Privileged Account Types by Tier:

ENDPOINT ADMINISTRATORS (TIER 2)		
These accounts are privileged account types used exclusively for accessing and administering endpoint systems and workstations. Tier 2 administration accounts may be assigned for each domain where the account owner has responsibilities for maintaining (e.g., production/NET, and non-production/NETDEV domains and clouds) and are most commonly assigned in production.		
NAMING CONVENTION	**ACCOUNT DESCRIPTION**	**TIER 2**
NIDadmin_T2	**On Premises Endpoint Administrator.** These accounts used exclusively for accessing and administering on premises domain joined (hybrid joined) endpoint systems and workstations that require administrators to MFA when using elevated privileges. • NIDadmin_T2 accounts must be protected with MFA authentication methods e.g., FIDO2 methods with SCRIL (Smart Card Required for Interactive Login) enabled – (no SMS or telephone) and configured for Passwordless sign in to administer domain/hybrid joined endpoints. ○ Note: Some T2 accounts may be used with SCRIL disabled and is based on technical requirements provided the configuration is not in conflict with a compliance requirement. Accounts in this category will be placed in a named Active Directory group: “UCF IT - Tier 2 SCRIL Exclusions". • NIDadmin_T2 accounts must be provisioned in the on-premises directory only. They must never be provisioned any tier one or zero privileges. If possible, the accounts should not be synchronized to the cloud directory.	
NIDadmin_COT2	**Cloud Only Endpoint Administrator.** These accounts are used exclusively for accessing and administering cloud only (CO) based tier two (T2) endpoint systems and workstations (e.g., a cloud joined device deployed with Microsoft Intune). • NIDadmin_COT2 accounts must be protected with MFA and can be configured for Passwordless sign in. • NIDadmin_COT2 accounts must be provisioned in the cloud directory only and never be synchronized to an on-premises directory service. • NIDadmin_COT2 accounts can only access certain specialized or enterprise workstations for the specific purposes of temporary elevation to achieve an objective the standard user account cannot. They may require privileged elevation to perform certain assigned functions. Privileged elevation or escalation may require administrators to request privileged role use at the time of need (just in time) and submit an explanation for the elevation (e.g., processing a service request, installing approved software, or troubleshooting).	

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

	Additional NIDadmin_COT2 Owner Responsibilities • Adhere to security policies and exclusively use the COT2 accounts for approved cloud joined endpoint management (never on-premises administration). • Account owners should only elevate to the lowest level privileged roles that allow them to perform the task needed and for the least amount of time that the role might be needed (up to 12 hours).

MEMBER SERVER / APPLICATION ADMINISTRATOR (TIER 1)

A privileged account type used exclusively for accessing and administering tier one (T1) member servers and applications.

- Provisioning and de-provisioning procedures require additional scrutiny with endorsement from the supervisor and the Information Security Office.
- Tier 1 accounts should not be used for tier two or tier zero administration.
- May be assigned for each domain the account owner has responsibilities to maintain (e.g., production/NET and non-production/NETDEV domains), and are most commonly assigned in production (as production can access non-production systems).
- May require a specialized workstation (dependent on the requirements).
- **Accounts must be protected with MFA and only use strong authentication methods** such as mobile-app based push, FIDO2 options, or app-generated one-time codes as the MFA second factor (no SMS or telephone call back).

NAMING CONVENTION	ACCOUNT DESCRIPTION	TIER 1
NIDadmin_T1	**Directory Joined Member Server or Application Administrator.** Used exclusively for accessing and administering tier one (T1) servers and applications (web/database/application) that reside within the network and/or data center. • Must be provisioned in the on-premises directory only and never provisioned any cloud-based tier zero privileges. If possible, the accounts should not be synchronized to the cloud directory.	
NIDadmin_COT1	**Cloud Only Application Administrator.** Used for accessing and administering cloud only (CO) based tier one (T1) applications and administration functions by IT operations, security teams, and users of specialized workstations. • Can be configured for Passwordless sign in. • Accounts must be provisioned in the cloud directory *only* and never synchronized to an on-premises directory service. NIDadmin_COT1 accounts may use certain specialized or enterprise workstations for the specific purposes of temporary elevation to achieve an objective the standard user account cannot. They may require privileged elevation to perform certain assigned functions. Privileged elevation or escalation may require administrators to request privileged role use at the time of need (just in time) and submit an explanation for the elevation (e.g., processing a service request, installing approved software, or adjusting network settings.)	

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

NIDAdmin *NOTE: While this account naming convention is still valid, its use will be phased out over time in favor of the modern Tier model of privileged account provisioning.*	This is a legacy "general use" privileged administrator account that may be responsible for installing, maintaining, configuring, or access control, on systems such as servers, infrastructure, and sometimes cloud management. More specifically: • Server administration within a data center (on premises or cloud data center), e.g., configuring a web, database, or application server. • Database administration: configuring, adding, deleting databases or the elements within them (schemas, tables, etc.) • Endpoint support for domain joined / hybrid joined systems– configuration, deployment, support, and maintenance of endpoint/client systems such as desktops, laptops, and mobile devices. These accounts should follow the same standards for both T1 and COT1 accounts. Additionally, the account owner's responsibilities for T1 and COT1 apply to NIDadmins. • NIDadmins should not be requested and used for the sole purpose of protecting access to data such as Highly Restricted data (e.g., within an application), use a NID with MFA instead. • NIDadmins are assigned for each domain the account owner has responsibilities for maintaining (e.g., production/NET, and non-production/NETDEV domains) NIDadmins should be protected with MFA whenever technically feasible. • NIDadmins may require privileged elevation to perform certain assigned functions. Privileged elevation or escalation may require administrators to request privileged role use at the time of need (just in time) and submit an explanation for the elevation (e.g., processing a service request or implementation a project).

Additional Responsibilities for Tier 1 Account Owners:

- If a specialized workstation is assigned, use the account only from this workstation including tasks such as MFA registration, password reset, etc.)

TIER ZERO ADMINISTRATORS (TIER 0)

A Tier 0 administrator account is a highly privileged account used exclusively to administer the enterprise directories and cloud portals. Tier zero administrator accounts are strictly controlled and only authorized for the minimum number required to provide appropriate service levels and reasonable redundancy.

- Provisioning and de-provisioning procedures require additional scrutiny with endorsement from the supervisor, the Director of Enterprise Infrastructure, and the Information Security Office.
- Tier zero accounts are not to be used to access any other systems or applications or used for any standard user or business productivity activities. Accounts are intended for privileged domain or cloud administration only by IT operations and security teams.

- Must be configured to follow the 501 Password Standard for Privileged Accounts.
- Must be protected with MFA and only use strong authentication methods such as mobile-app based push, FIDO2 options, or app-generated one-time codes as the MFA second factor (no SMS or telephone call back).
- May be assigned for each domain the account owner has responsibilities to maintain (e.g., production/NET and non-production/NETDEV domains), and are most commonly assigned in production (as production can access non-production systems).
- Tier zero administrative accounts can only access tier zero from privileged access workstations (PAW).
  - NOTE: Modern PAW device implementations intended to administer sensitive cloud roles should only allow "cloud only" NIDadmin_COT0 accounts to sign in but can also permit access to on premises tier zero resources by signing into the bastion service with a tier zero account.

NAMING CONVENTION	ACCOUNT DESCRIPTION	TIER 0
NETadmin	NETadmins are privileged account types added to the domain and/or enterprise administrators' group and used exclusively for accessing and administering domain controllers. • Must be provisioned in the on-premises directory only and never provisioned any cloud-based tier zero privileges. If possible, the accounts should not be synchronized to the cloud directory. • Domain administration account group members are kept to the lowest number of provisioned accounts needed to provide appropriate service levels and reasonable redundancy.	
NIDadmin_T0	Used exclusively for accessing and administering tier zero (T0) servers and applications that reside within the data center or physical network. • Must be provisioned in the on-premises directory only and never provisioned any cloud-based tier zero privileges. If possible, the accounts should not be synchronized to the cloud directory.	
NIDadmin_COT0	**Cloud Only Tier Zero Administrator.** Used exclusively for accessing and administering cloud only (CO) based tier zero (T0) management applications such as Entra ID, Azure and cloud-based data centers, Unified Communications Services, Intune management consoles, and security focused management consoles. They are also used to sign into cloud-only privileged access workstations (PAW). • Must be provisioned in the cloud directory only and never be synchronized to an on-premises directory service. • Must be protected with strong MFA authentication methods (e.g., Windows Hello for Business and other FIDO2 methods – no SMS or telephone call back) and configured for Passwordless sign in. NOTE: Preapproval of using device exclusions may be granted in a limited capacity to accommodate some applications and procedures that require COT0 accounts to sign in. • May require privileged elevation to perform certain assigned functions. Privileged elevation or escalation may require administrators to request privileged role use at the time of need (just in time) and submit	

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

	an explanation for the elevation (e.g., processing a service request or implementation a project). • Account owners should only elevate to the lowest level privileged roles that allow them to perform the task needed and for the least amount of time that the role might be needed (up to 12 hours).

Additional Responsibilities for Tier 0 Account Owners:

- Use a PAW for all Tier Zero administrator work (MFA registration, password reset, etc.)

SYSTEM ACCOUNTS

- All "other accounts" acting on behalf of authorized users should be identified per the naming standards above and have an appropriate description listed in the directory. The description field for all other accounts should identify the purpose of the account.
- All "other accounts" should be enabled to act on behalf of designated authorized users who shall be listed as the owner of these accounts. Up to three users can be listed as the owner of an "other account" and at least one must be present for the account to persist.
- Account owners may be asked to review and attest that accounts are still required on an annual basis. Account owners who do not respond or whose accounts have not signed in for over a year may be disabled and deleted.
- Some "other accounts" may require special approvals.

SERVICE ACCOUNTS	
NAMING CONVENTION	**ACCOUNT DESCRIPTION**
SVC_{DEPT}_{SERVICE_NAME} Example: SVC_IT_SQL1	**Service Account.** This account should be used to run non-interactive background and integration services such as scheduled tasks and services on servers and/or other services.
• Enterprise directory service accounts must be requested through ITSM request processes. • Must have at least one owner and up to a maximum of three owners. • Service accounts passwords can be set to not expire and should be rotated when a compromise is suspected. • Must set long and unguessable passwords per 501 Password Standard for highly privileged accounts. • Use principles of least privilege as well as vendor guidance to provision service accounts. Consider creating accounts that encourage logical separation of systems and networks and use alternatives to service accounts if available (e.g., Service Principles, etc.) • On premises service accounts should not be granted cloud permissions and cloud-based service accounts should not be granted permissions on premises.	

TEST ACCOUNTS	
NAMING CONVENTION	**ACCOUNT DESCRIPTION**
TST_{DEPT}_{NAME} Example: TST_IT_Bob1	**Test Account.** 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 can 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 randomly generated passwords that are different from any user's NID or privileged account.
- Must set long and unguessable passwords per 501 Password Standard for standard accounts.
- Test accounts should expire after 60 days.
- Test accounts for standard accounts should follow all standard account requirements. Privileged test accounts should follow all privileged account requirements and not be used in production when alternatives exist such as testing in non-production.
- Nonproduction should be used for testing, validating, proof of concept, etc. whenever technically feasible.

RELATED DOCUMENTS:

- 4-008 *Data Classification and Protection* policy
- NET Domain Naming Standards
- 501 [UCF] Password Standards
  NOTE: You must be signed in and have an employee attribute to view these forms:
- Request Form: Privileged Endpoint Access Request
- Request Form: Add, Remove, or Reset a Privileged Administrator Account
- UCF Sponsored Account | UCF request system

CONTACTS:

Information Security Office	infosec@ucf.edu https://infosec.ucf.edu
Security Incident Response Team (SIRT)	sirt@ucf.edu https://infosec.ucf.edu/incident-response/
Identity Access Management (IAM)	iam@ucf.edu https://infosec.ucf.edu/iam
Research Cyber Risk Management (RCRM)	ResearchCyberRisk@ucf.edu https://rcrm.infosec.ucf.edu
UCF IT Support Center	itsupport@ucf.edu (407) 823-5117 https://ucf.service-now.com/ucfit

Revision Date	Summary of Change
08/30/2022	Changed test account password expiration from 60 days to 365 days.
04/12/2025	The document title was changed from User Account Standards to IT Account Standards. The applicability was updated to include all accounts, regardless of domain, directory, or system. Account management practices were added for each account type. The transactions and functions authorized by account type were enhanced. The document structure was organized to differentiate between standard, privileged, and system account types. New account types were introduced to represent the tiered security model and the separation of on-premises and cloud accounts. The process to request, approve, and retain privileged accounts was expanded. Established screening and training requirements for privileged accounts and the requirement to renew annually.

INITIATING OFFICE: Information Security Office

STANDARDS APPROVAL

(For use by the Information Security Office)

Standards Number: 502

Initiating Office: Information Security Office

Interim Chief Information Security Officer: *Tammie McClellan*

Signature: Tammie McClellan Digitally signed by Tammie McClellan Date: 2025.05.01 15:40:25 -04'00' Date: 5/01/2025

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