SALT LAKE COUNTY
COUNTYWIDE INFORMATION TECHNOLOGY STANDARD
ON
ACTIVE DIRECTORY STRUCTURE AND OBJECT NAMING

Purpose –

The purpose of this standard is to offer guidance for the proper structure of Active Directory and the naming of objects in Salt Lake County Active Directory domains.

Employees of Salt Lake County are expected to follow the *Active Directory Structure and Object Naming Standard* established by the Information Technology Division. The Information Technology Division will monitor and enforce compliance with this standard.

Reference –

The standards set forth herein are provided in accordance with Countywide Policy 1400, which directs the Salt Lake County Information Technology Division to provide information technology standards. Also referencing the following:

All Countywide Information Technology Security Policies in the 1400 series
All Countywide Human Resource Policies

1.0 Scope

All Salt Lake County employees shall adhere to this Countywide information technology standard.

2.0 Definitions

Information Technology Resource(s) and/or System(s)
Computers, hardware, software, data, storage media, electronic communications (including, but not limited to, email, fax, phones, phone systems, and voice mail), networks, operational procedures and processes used in the collection, processing, storage, sharing or distribution of information within, or with any access beyond ordinary public access to, the County's shared computing and network infrastructure.

Active Directory
Active Directory (AD) is a Microsoft product consisting of several services that run on Windows Server to manage permissions and access to networked resources.

Active Directory Object
Active Directory stores data as objects. An object is a single element, such as a user, group, computer, application, or device, such as a printer.

3.0 Standard Guidance

Revision History
AUGUST 2021 - MLE

All Salt Lake County Employees will follow the County's *Active Directory Object Naming Standard* as defined in appendix A of this document.

4.0 Exceptions

Any exceptions to this standard must be explicitly approved in writing by the Salt Lake County Chief Information Officer or their designee.

5.0 Enforcement

Anyone found to have knowingly violated this standard shall be subject to disciplinary action by County disciplinary policies.

Revision History
AUGUST 2021 - MLE

Appendix A
Active Directory Object Naming Standard

Workstations Object Names

We must follow a standard in naming computer objects in Active Directory. Many automated processes have been put in place that relies on the department code section being correct. Therefore, it is important that only approved department codes be used here. Approved department codes can be found in the next section of this IT standard. New department codes may not be used until they have been discussed and approved by the IT Governance process.

Workstation object naming standard:

- There are 15-characters available to use.
- The first 2-4 characters are reserved for the department code. (See approved table below)
- The character following the department code must be a hyphen.
- The remaining 12-characters can be any string that is meaningful to the agency that owns the workstation.
- Workstation names should be in ALL CAPS for the sake of consistency.

Examples:
Workstation object name referencing the assigned user:

- A computer for a user named John Smith [Logon ID: JSmith] in Aging Services would be: AG-JSMITH
- If the complete logon ID is too long, truncate from the end of the logon ID.
- Use a "dash" or hyphen character to separate the department and username.
- DO NOT use the underline character.

Workstation object name referencing a serial number

- A computer with the serial number 123456 in Aging Services would be AG-123456.
- If the complete logon ID is too long, truncate from the end of the serial number.
- Use a "dash" or hyphen character to separate the department and username.
- DO NOT use the underline character.

Please do not use ANY spaces or special characters, such as: * & $ # ‘ [apostrophe] , [comma] or . [period]. These and other characters can cause problems with scripted or automated tools and processes. The use of numbers is acceptable, where appropriate.

Computer names are not case-sensitive, but it is preferred to use ALL CAPS for the sake of consistency.

Other options:

- If space allows, you can indicate the operating system of the computer: AG-JSMITH-10
- If a user has more than one computer, you may add a number after the logon ID: AG-JSMITH02
- For a laptop computer, add [–LT] to the end of the computer name: AG-JSMITH-LT
- For a tablet computer, add [–TAB] to the end of the computer name: AG-JSMITH-TAB
- For an MS Surface, add [–SUR] to the end of the computer name: AG-JSMITH-SUR
- Or use a combination of descriptors: AG-JSMITH-LT10

Department Codes

Revision History
AUGUST 2021 - MLE

The following department codes have been approved for use in our naming convention. Therefore, you may only use these approved department codes.

Addressing	AD	Health Department	HL
Administrative Services	ADM	Human Resources	HR
Aging & Adult Services	AG	Human Services	HS
Animal Services	AN, MDT	Information Technology	IS
Archives	AR	Jail	JL
Assessor	AS	Justice Courts	JC
Auditor	AU	Landfill	LF
Behavioral Health Services	BH	Library	LI
Center for the Arts	FA	Mayor	MA
Children's Justice Center	CJC	Mayor Finance	MF
Clark Planetarium	PL	Parks & Recreation	PR
Clerk	CL	Municipal Services District	MSD
Community Services	CS	Public Works	PW
Contracts & Procurement	CP	PW Operations	OP
County Council	CC	Recorder	RE
Criminal Justice Advisory Council	CJAC	Regional Development	RD
Criminal Justice Services	CJ	Sheriff	SH, MDT
District Attorney	DA	Surveyor	SV
Elections	EL	Tax Administration	TA
Emergency Services	ES	Treasurer	TR
Engineering	ENG	Unified Police Department	UPD, MDT
Flood Control	FC	USU Extension Services	UE
Facilities Management	FM	WFWRD	WF
Fleet Management	FL	Youth Services	YS

Server Object Names

- Server names should use the following convention: [SLC][Department Code][Function or Location][Environment]
- Server names should be in ALL CAPS for the sake of consistency except in the case of Linux servers.
- For example, a server in the Aging Services department that provides printing services might be SLCAGPRINT.
- A general-purpose server at a Parks & Recreation facility in Herriman might be SLCPRHERRIMAN.
- Any test or development server should be appended with a –T or –D respectively to identify the environment. A server will be assumed to be in the production environment otherwise.
- All database servers should be identified by including the letters "DB" after the "Function or Location" section, such as SLCISSIGMADB or SLCISSIGMADB-T.
- The maximum server name length is 15 characters and should not use underlines or special characters for the same reasons described for workstations above.

Printer Object Names

- Printer names can be long and descriptive. The printer "share names" are shorter and should make use of the abbreviations described herein. These guidelines cover printer names and printer share names alike.

- Both names should use the following convention. Share names should be abbreviated versions of the printer name: [Department Code]-[Campus/Building]-[Room/Location]-[Manufacturer][Model Number]-[Printer Number*]
- For example, a Canon iR9000 printer in the Aging Services area of the government center might be named:
  Name: AG GC S1500 Canon iR9000
  Share Name: AG-GC-S1500-CiR9000
- If this were the third Canon iR9000 to be installed in this location, it might be named:
  Name: AG GC S1500 Canon iR9000 Southwest
  Share Name: AG-GC-S1500-CiR9000-3

- A Hewlett-Packard OfficeJet 7400 located in the booking area of the ADC might be named:
  Name: SH ADC Booking Counter HP OfficeJet 7400
  Share Name: SH-ADC-BK-HPOJ7400
- It is acceptable to use the abbreviated "Share Name" as the "Printer Name" if it is clear enough for end-users to interpret.

Printer names and share names CAN be longer than 15 characters and often will be. Longer names may cause DOS-based programs that need direct access to printers, but these programs are rare and becoming less common with time. In most cases, if a department or office uses a legacy program that requires special printer considerations, they should be able to tell you.

Printer Manufacturer Codes

For internal consistency, please use the following manufacturer codes when naming printers. If you encounter a printer manufacturer that is not on this list, please determine an appropriate 1- or 2-character abbreviation for it and add it to this list:

B	Brother	O	Okidata
C	Canon	S	Sharp
E	Epson	X	Xerox
HP	Hewlett-Packard		

Users

- **User Directory Names**
  - Directory Names should use the following convention: [First Name] [Last Name] (ex: PSmith) (redundant – specified in the "Regular and Service Account Standard)
  - For duplicate accounts, add the user's middle initial or one or more additional letters from the user's first name to the account name (ex: PLSmithe or PeSmith) (redundant – specified in the "Regular and Service Account Standard)
  - Directory names must be unique within the Domain; this means unique within the County network system – not just within the user's department.
  - Directory names can be up to 64 characters in length, so practically any name can be accommodated by this system.
  - Directory Names should be entered with appropriate capitalization; names are generally case-aware (meaning they will be saved in the same case they were entered) but are not case-sensitive.
  - Directory names may include spaces and hyphens but should not contain any other special characters. This is because special characters can cause problems with scripted or automated tools and processes.

- **User Display (Common) Names**
  - The Display Name corresponds with the "Name" field in ADU&C.
  - Display Names should use the following convention: [First Name] [Last Name]

- Display Names are not unique within the Domain and can be modified by the user.
- Display names can be up to 64 characters in length, as with Directory Names.
- Display Names should be entered with appropriate capitalization, as with Directory Names.
- Display names may include spaces and hyphens but should not contain any other special characters, as with Directory Names.

Typically, a Display Name should match the corresponding Directory Name. Exceptions MAY include the addition of such information as rank or office held, but the use of this information is discouraged as it may change at any time. In most cases, only service accounts or other non-real user accounts will have specific Display Name information.

Regular, Vendor and Service accounts will follow the standards specified in the "Regular and Service Accounts" Countywide Information Technology Standard document.

Accounts with Privileged access will follow the standards specified in the "Privileged Access Management Standard" Countywide Information Technology Standard document.

User accounts for email resources will follow conventions specific to them described under the Exchange Related Objects section in this document.

- **User Logon IDs**
  - Logon IDs should use the following convention whenever possible: [Initial of First Name] [Last Name]
  - For example, a user named Michael G. Doe might ideally have the following Logon ID (i.e., MDoe)
  - If a chosen Logon ID already exists, add a middle initial if possible: [Initial of First Name] [Initial of Middle Name] [Last Name] (i.e., MGDoe)
  - If this Logon ID also exists, or if the user has no middle name, add successive characters from the first name until a unique combination has been reached (i.e., MiDoe)
  - Logon IDs must be unique within the Domain; this means unique within the County network system – not just within the user's department.
  - Logon IDs should be entered with appropriate capitalization, as with Directory Names.
  - Logon IDs may include hyphens but should not contain spaces or special characters, as with Directory Names.

A Login ID can be abbreviated at the user's discretion if the name is so long that it makes it inconvenient. However, for identification purposes, the email address and Display Name should match how the user is referenced in Human Resources or how the user is commonly known.

Contacts

- Contacts are generally used for including non-county contact information in the directory.
- Contacts should have the following fields populated: First Name, Last Name, Display Name, Email. Other information is optional.
- The Name attribute must be unique to the Contact objects.
- The Display Name does not have to be unique. However, care should be taken to make sure it does not conflict with the Display Name of other objects.
- Information is visible in the directory, only include personal email and phone numbers with permission from the individual.

Groups

- Group names should be short and be descriptive of their purpose. For example, those specific to a division will begin with the division code, followed by the abbreviated description.
- Groups should be appropriately located in the AD hierarchy for management.
- Group scope will be defined as Global and type as Local unless another definition is necessary.
- Groups will be used for specific access to resources.
- The Description field will include information specific to the group's purpose; the Notes field will be used for further explanation as necessary.

Groups for Role-Based Access Control (RBAC) will follow the standards specified in the "Role Based Access Control" Countywide Information Technology Standard document.

Organizational Objects (OUs)

- OUs will be placed in the AD hierarchy for proper management and inheritance
- The OU hierarchy for divisions will be created under the "Department" OU. It will reflect the division name, with sub-OUs as needed for Computers, Groups, Member Servers, and Users following these conventions. Sub-OUs below these levels will be created following these standards:
    - Computers (this may be further divided for locations)
        - Remote (Laptops – for VPN access)
    - Groups
    - Member Servers
        - Server OS group (separate group for each OS)
    - Users (this may be further divided for locations)
        - Disabled Accounts
        - Holds (disabled accounts with litigation holds)
        - Limited Accounts (accounts with no file or email access)
        - Special Accounts
            - Alias Accounts (accounts for privileged access)
            - Application Accounts
            - Email Resource Accounts
            - Vendors (vendor accounts)
            - Windows Service Accounts
- The "Computers-New" OU is the default container for newly joined computers. Computers should be immediately moved to the proper location for the object in the sponsoring department's hierarchy.
- The "PageCenter" OU will contain only PageCenter related group objects.
- The "SharePoint" OU will contain only SharePoint-related groups and user objects.
- The "Locations" OU is for directory items specific to Buildings, Departments, Organizations, and Rooms. Although the contents of these OUs are self-explanatory, naming conventions should follow existing items.

Exchange Related Objects

- Email Resource Accounts are used mainly for scheduling resources such as conference rooms. Therefore, the following attributes should be configured for these accounts:
    - Directory Name (details match those for User Directory Names specified earlier in this document)
    - Display Name (usually matches the Directory Name).
    - Description (references the resource, include the Division, resource type, and location).
    - The account should be disabled.
- Distribution lists.
    - Stored in the "Distribution Lists" container in Active Directory
    - The name should be descriptive and end with "DL."

    - Associated Email account should follow format [Organization code]-[abbreviated purpose/description]DL@slco.org
    - Scope and type set to "Universal" and "Distribution," respectively.
    - The description should reference the purpose, include other details as necessary.
- Exchange servers.
- Stored in the Information Services/Member Servers/Exchange 2013 Servers container
- Information specific to

Group Policy Objects

- Group Policy names will use the convention of [Organization code (if applicable)] [environment] [purpose].
- The Comments field will include information regarding the purpose of the policy.

Managed Service Account Resources

- Managed Service Accounts are stored in the "Managed Service Accounts" container in Active Directory.
- Group Managed Service Account names will use the convention of gMSA[SQL or Web][description][environment] Ex: gMSAsql2016Prod or gMSAwebAuPort
- Managed Service Account names will use the convention of MSA[description]
- Resources associated with Group Managed Service Accounts, including the associated servers and groups, are stored in the "Information Services/Member Servers/SQL GMSA" and "Information Services/Member Servers/Web GMSA" OUs. A separate OU at these locations will be configured for the resources associated with each GMSA and named [SQL or Web] [description] [environment]

Revision History
FEB 2020 - MLE