[redacted]

Active Directory Naming Conventions
Version 1.0

September 17, 2018

Prepared by Andrew Koski
Approved on October, 1, 2018

For Official Use Only

TABLE OF CONTENTS

Record of Changes

Version Number	Release Date	Summary of Changes	Section Number/ Paragraph Number	Changes Approved by and Date
1	09/17/18	Original		Andrew Koski 10/1/18

Please note: All changes must be approved by a managing member of infrastructure.

1. Background

The Active Directory (AD) Organizational Unit (OU) is governed by policy, procedure, guidelines, and practices. This guidance includes the naming of AD objects (i.e., accounts and resources):

- No two AD accounts shall be named the same; uniqueness enables the use of the user objects across multiple directories and applications.
- Organizations that participate in any AD are required to standardize how they identify their AD network resources (e.g. Workstations, servers, printers, and domain controllers) when registering them in Domain Name System (DNS) and the active directory and to coordinate their standards with the Active Directory Operations Group (ADOG).
- Organizations under contract are expected to adopt a network naming standard that is consistent and relevant to their operations but not infringing on other organizations naming standards.
- Organizations under contract should consistently name AD network resources to reflect the organization they belong to. This is easily accomplished by using the IC acronym as a prefix to the identity of the network name.

The AD Naming Conventions will ensure compliance with technical direction and guidance, create a consistent naming structure across AD accounts and resources, and support the mission.

2. Scope

These practices apply to all Active Directory objects within the client's AD OU and its subordinate OU's. Unless technically impossible, all principle objects should reside within the Active Directory (AD) Organizational Unit (OU).

3. Accounts

All accounts are limited to 256 characters in length and can contain A-Z, a-z, and 0-9 (no special characters allowed).

3.1 Primary User Accounts

User accounts represent an individual person with privileges to access to their specific network resources. User names must be unique within the entire Active Directory namespace. User names will consists of the user's letter of their first name followed by the user's entire surname. For example, for "John Doe" would be: *JDoe*. If that username is taken please resort to spelling out the user's first and last name.

3.2 Secondary User Accounts

Any management position within a client's organization where the secondary account will be utilized may approve the secondary account. He or she may authorize the creation of secondary user accounts in instances where elevated administrative access has been justified. The decision is final.

All secondary accounts will take the form of the letters “aa” followed by the user’s entire primary account. For example, a user with a primary user account of *JDoe* would be issued a secondary account *aaJDoe*.

3.3 Resource Accounts

Resource accounts must be unique within the namespace. Resource accounts must be located under the OU and then a subordinate OU titled “OPS” then “ResourceAccounts”. Resource accounts should denote the purpose of the account. For example, a resource account for Conference Room A might take the form: *XXXConfRoomA or XXXConfA*

3.4 Service Accounts

Service accounts must be unique within the client’s namespace. Service accounts must be located under the OU and then a subordinate OU titled “OPS” then “ServiceAccounts”. Service accounts should denote the purpose of the account. For example, a service account might take the form: *XXXODBackupAcct* or *XXXmonitoring.*

3.5 Training Accounts

Training accounts must be unique within the namespace. Training accounts must be located under the OU and then a subordinate OU titled “OPS” then “TrainingAccounts”. Training accounts should denote the purpose of the account. For example, a training account might take the form: *XXXTraining1* or *XXXABCCStudent01*.

4. Equipment

All equipment registered in the AD OU will follow a standard naming convention to ensure compliance with AD Attribute Data Content and Management: Best Community Practices and create a unique identifier within the AD name space. All equipment names should follow the format:

GroupIdentifier -ClassCode-UniqueIdentifier[-Suffix] where:

ClassCode equals one of:

Code	Description
WS	Workstation or Desktop Computer
NB	Notebook Computer or Portable Device
TC	Thin or Zero Client
PS	Physical Server
VS	Virtual Server
VM	Virtual Machine
NS	Network Attached Storage
SS	Serial Attached Storage
PR	Printer
RT	Router
AP	Wireless Access Point

ES	Ethernet Switch

UniqueIdentifier equals one of:

For ClassCode	Description
Unique Identifier	Property or Asset Number
All Others	Purpose of Device

GroupIdentifier is defined as a registered acronym or designation for an organization. Group identifiers must be consistent across all equipment registered to the group. Group identifier can be found within the vendor and employee directory. The ADWG will ensure uniqueness of group identifiers.

Suffix is any additional text that may help describe or identify the equipment. *Suffix* will traditionally be the user's username.

Examples:

XXX-S-XY-Files01: MS Windows-based Server in Program Area "XY" used primarily as a file server.

XXX-W-S0123456: A workstation with a Property Number S0123456.

XXX-P-S0123456: A network accessible printer a Property Number S0123456.

AD Extended Description Field:

The Asset Tag Number will be included in the AD Extended Description field for all equipment registered in the AD OU.

5. Information and Assistance

Comments, questions, suggestions or requests for further information should be directed to a managing member of infrastructure.

6. References

1. Windows Server Active Directory Best practices;
   http://technet.microsoft.com/en-us/library/cc778219(v=ws.10).aspx