

Education and Workforce Development Cabinet POLICY/PROCEDURE

Policy Number: EDU-03

Effective Date: January 10, 2005
Revision Date: December 20, 2012

Subject: Naming Standards for Workstations and Servers

Policy: This policy supports the Education and Workforce Development Cabinet (EDU) naming standards for workstations/servers to ensure security and also represents a set of standards to be followed. Effective machine names will improve the likelihood that the identification of the machine is correct and that a machines function will not be obvious to an attacker.

All machines must follow these standards prior to being connected to the Kentucky Information Highway (KIH).

Scope: This policy applies to all EDU workstations and servers.

Policy/Procedure Maintenance Responsibility: The EDU Agency Security Contacts (ASC) is responsible for the maintenance of this policy. The Chief Information Officer (CIO) is responsible for the revision of the EDU Policy and Procedures Manual (PPM). The EDU CIO is responsible for authorizing all changes to the PPM.

Applicability: All EDU employees, contract agencies and contractors shall adhere to the following polices and procedures.

Procedure:

Workstation Names (Workstation computer accounts)

Workstation names

1. Must be unique
2. Must not indicate personal ownership, assignment or tied to user logon names (for security purposes)
3. Must depict location information so that workstation and entity affiliation can easily be identified
4. Must begin with character prefixes that denote entity affiliation. DWI, OVR, OFB, CPE, KDLA etc.

Each workstation name, after the prefix, must abide by the following restrictions:

1. Do not use more than 14 characters for the NetBIOS computer name if there are any legacy systems in the NT environment. The older versions of LAN Manager utilities used the 15th character as a special termination character as NT only uses the 16th character as a termination character.
2. Do not create a computer name the same as logon name. This can make the desktop boot order be dependent. If a user logs in on another machine and then tries to boot the original machine, the original machine will fail to log on to the network with a 'duplicate name' error.
3. Do not use the character '-' in the beginning or end of a computer name; as in 'RED-SQL-' or '-RED-SQL'.
4. Do not use the character '_' (underscore) in a computer name. Today this can be used as a valid character because NetBIOS will support it. However, DNS does not support the '_' character. If the computer is supporting FTP or Web connectivity, then DNS cannot resolve names with this character in it. Windows 2000 is DNS-based and does not support the '_' character.
5. Do not start a computer name with a number. Attempt to start the computer name with an alpha character. Applications and different versions of network redirectors assume that when the first character is a number that the computer name being passed is an IP address and not an ASCII computer name. Using a number as the first digit is not supported by DNS.
6. Do not use special characters as in '~' and '{', or such. Applications cannot speak peer to peer with computers that have extended characters in their name. An example of this scenario is PowerPoint conferencing. Presentation broadcasting will not work with these types of computer names. If the presenter has a special character, all desktops can see the show, but the presenter cannot. If one of the desktops has a special character, then the presenter would work, but the desktop could not connect. In addition, these characters are not supported in a DNS environment.

Standard:

The naming convention to be used to uniquely identify all EDU machines may contain up to 14 characters as follows:

- The first characters will identify the Agency or Department. **DWI, OVR, OTR, OET, OTE, OFB, CPE, KDLA**
- The next characters will be the city code. **FK, LX, LV**
- The remaining characters are for the computer inventory tag number.

If the computer is missing the inventory tag then the computer serial number will be used in place of the inventory tag.

An example of a workstation naming convention would be:

OVRFKD123456, Office of Vocation Rehabilitation, Frankfort, inventory tag D123456.

CPEFKX123456, Council Postsecondary Education, Frankfort, inventory tag X123456.

KDLAFKX123456, Kentucky Department Libraries and Archives, Frankfort, inventory tag X123456.

If the computer requires a reload of any type the computer name must be removed from the Domain this prevents duplicate names and prevents the reloaded computer from joining the Domain.

NOTICE:

******A label must be placed on the top or front of all machines identifying the machine name******

Server Names (Member Servers, Global Catalogs, etc.)

Server names

- The first characters will identify agency (CPE), (KDLA) (KCDHH), (OVR), (OFB), (OET)
- The next characters will be city code.
- If the agency has multiple servers in one location then the next characters will be a numeric designation i.e. 01, 02 etc.

An example of a member server naming convention would be:

OETFK01, Office of Employment and Training, Frankfort, server number one (1)

OVRSS, Office of Vocational Rehabilitation, Somerset

OFBLV, Office For the Blind, Louisville

CPEFK, Council Postsecondary Education, Frankfort

For security purposes, and to mask the server's functionality from hackers, server names must not reflect *specific* functionality. For example, if a server is running SQL the word 'SQL' should not specifically be used in the name. It would be acceptable, however, to use more generic terms, such as 'MSG' for 'Messaging'. If a hacker were out to cripple a DHCP server, then it would be very easy to locate on the network if the letters 'DHCP' were in the server's name. Since DHCP is an infrastructure service, it might be more feasible to name the server with the letters 'INFSTR' (abbreviation for 'infrastructure' in the name rather than DHCP. There are many possibilities for server names. These examples are offered for illustration purposes only.

The simplest scheme that is commonly adopted in many organizations is based on the combination of Entity affiliation (represented via a very generic Location specifier), type of service and instance. An example of this would be 'EDUFKFS1'; this name stands for Education Cabinet, located in Frankfort and is a File Server. With this naming scheme, the server can move from location to location within the entity without having to change the name whenever the physical location of the server changes. It is unlikely that physical machines move from campus to campus or change entity affiliations, so this scheme is generally acceptable.

If, for some reason, the server does move, then the ownership and/or function have typically changed and the machine should be renamed as part of the move. Domain Controllers and Global Catalog servers should not follow the same rule, however, as Domain Controller and Global Catalog functions can be transitive, and the roles are not considered to be permanent. In this case, it would be best naming

the servers based on location or entity affiliation, along with a generic 'Server XX' identifier, especially if multiple services are to be offered by the same machine.

If a server is to be dedicated to a specific role, such as DHCP, WINS, Messaging, etc., then naming the server after the service provided can be acceptable. Be advised that if this model is followed, the name will not represent the server offerings if more responsibilities are assigned to the server and the name is not subsequently changed. Only consider this option if there is no perceived change in the server's present and future roles. Also be advised that by naming the server after the function that it performs can make it easier for hackers to locate. Be aware that future name changes can wreak havoc on clients and necessitate client software reconfiguration.

A few more popular naming conventions are naming servers with proper names, such as mythical people, animals, planets, and galaxies. Even though this naming scheme has appeal from several levels, it generally is not acceptable for corporate-facing servers.

Below are several more naming standard recommendations to consider:

1. Do not use special characters. Two characters that are popular today are the '_' and the '-'. The '_' is not a valid DNS name so in a conversion to Windows 2000, it will break. The '-' character also breaks database products like SQL Server, Oracle and Sybase.
2. Do not use a period. This will be resolved as a DNS name. If the computer is connected to the Internet, the operating system will generate a DNS query against the ROOT DNS servers.
3. It is generally recommended that the server not be named for the applications that run on it, as in 'SRVSQLEXCHXX'. This name is derived from the role of the machine: NT member Server, SQL Server and Exchange server XX. Time makes the unavoidable chore of moving services around more difficult because the server names are tied to the software that runs on them. This is especially true when there are multiple services on the same physical server. If, however, only one service runs on the physical server, it is dedicated to one specific function, and there is a small probability that the physical server will ever serve any other functions, this can be acceptable.
4. If possible, avoid naming the servers with proper names, such as a city or person. By using a proper name, such as a city, support staff and end-users can get confused as to actual server location, name and function.

Policy Number: EDU-03
Subject: Naming Standards for Workstations and Servers Policy

Review Cycle:
Annually

Timeline:
Review Date: November 29, 2012
Reviewed By: EDU Agency Security Contacts

Enterprise Security and Policies
Cross Reference:

OTS Standards
Cross Reference: