Network Documentation Policy

1.0 Overview

This Network Documentation Policy defines the minimum documentation required to properly operate the network in an efficient manner. This Network Documentation Policy defines the level of network documentation required such as documentation of which switch ports connect to which switches. It defines who will have access to read network documentation and who will have access to change it. It also defines who will be notified when changes are made to the network.

2.0 Purpose

This Network Documentation Policy is designed to increase network efficiency and protect the network since administrators will be able to more quickly troubleshoot problems and disconnect systems that are operating malware or other unauthorized software. This Network Documentation Policy is designed to provide network stability by ensuring that network documentation is complete and current. This policy should complement disaster management and recovery by ensuring that documentation is available in the event that systems should need to be rebuilt. This policy will help reduce troubleshooting time by ensuring that appropriate personnel are notified when changes are made to the network.

3.0 Scope

This Network Documentation Policy applies to the Information Technology Department.

4.0 Documentation

The network structure and configuration shall be documented and provide the following information:

1. Physical locations of of all devices on the network especially networking devices and the connected jack numbers for client connections with associated room numbers or names.
2. IP addresses of all server and networking appliances on the network with static IP addresses.
3. Network drawings showing:
    1. The locations and IP addresses of all hubs, switches, routers, and firewalls on the network.
    2. The various security zones on the network and devices that control access between them.
    3. The locations of every network drop and the associated switch and port on the switch supplying that connection.
    4. The interrelationship between all network devices showing lines running between the network devices.

   5. All subnets on the network and their relationships including the range of IP addresses on all subnets and netmask information.
   6. All wide area network (WAN) or metropolitan area network (MAN) information including network devices connecting them and IP addresses of connecting devices.
4. Configuration information on all network devices including:
   1. Switches
   2. Routers
   3. Firewalls
5. Configuration shall include but not be limited to:
   1. IP Address
   2. Netmask
   3. Default gateway
   4. DNS server IP addresses for primary and secondary DNS servers.
6. Network connection information including:
   1. Type of connection to the internet or other WAN/MAN including T1,T3, frame relay.
   2. Provider of internet/WAN/MAN connection and contact information for sales and support.
   3. Configuration information including netmask, network ID, and gateway.
   4. Physical location of where the cabling enters the building and circuit number.
7. DHCP server settings showing:
   1. Range of IP addresses assigned by all DHCP servers on all subnets.
   2. Subnet mask, default gateway, DNS server settings, WINS server settings assigned by all DHCP servers on all subnets.
   3. Lease duration time.

5.0 Access

The IT networking and some enterprise security staff shall have full access to all network documentation. The IT networking staff shall have the ability to read and modify network documentation. Designated enterprise security staff shall have access to read and change network documentation but those not designated with change access cannot change it. Help desk staff shall have read access to network documentation.

6.0 Change Notification

The help desk staff, server administration staff, application developer staff, and IT management shall be notified when network changes are made. A log shall be used to log these activities. Activities include:

1. Reboot of a network device including switches, routers, and firewalls.
2. Changes of rules or configuration of a network device including switches, routers, and firewalls.
3. Upgrades to any software on any network device.

4. Additions of any software on any network device.
5. Changes to any servers which perform significant network functions whether configuration or upgrade changes are made. These servers include:
    1. DHCP
    2. DNS
    3. Domain controllers
6. Notification shall be through email to designated groups of people or through a logging tool which notifies people using email.

7.0 Documentation Review

The network or IT manager shall ensure that network documentation is kept current by performing a monthly review of documentation or designating a staff member to perform a review. The remedy or help desk requests within the last month should be reviewed to help determine whether any network changes were made. Also any current or completed projects affecting network settings should be reviewed to determine whether there were any network changes made to support the project.

8.0 Storage Locations

Network documentation shall be kept either in written form or electronic form in a minimum of two places. It should be kept in two facilities at least two miles apart so that if one facility is destroyed, information from the other facility may be used to help construct the IT infrastructure. Information in both facilities should be updated monthly at the time of the documentation review.

9.0 Enforcement

Since proper network documentation is important to the operation and maintenance of the network employees that do not adhere to this policy may be subject to disciplinary action up to and including lock of account.

LAST PRINTED 6/2/16