PMGS 14-1-3
Cooperative Extension Service
Computer Network Policy

Purpose:

The purpose of this document is to establish policy and procedures to ensure the continuous operation of the
University of Arkansas Cooperative Extension Service's State Office (UAEX-LRSO) computer network.

Scope:

This policy pertains to all employees, contractors, consultants, temporaries, and other workers at UAEX-LRSO, including those workers affiliated with third parties who access UAEX-LRSO information systems and networks. Throughout this policy, the word "worker" will be used to collectively refer to all such individuals. The policy applies to all computer and data communication systems owned by and/or administered by UAEX-LRSO.

General Policies:

All data network access and storage devices, including switches, routers, hubs, access points, servers, NAS (network attached storage) and SAN (storage area network), and printers\print servers, must be set up, configured, and administered by Network Operations. With the exception of wireless access points, printers, and accessories, all such devices must be physically in secure locations accessible only by Network Operations. Any network access device (including any mini-hub in an office or other location) found connected to the network and not administered or already permitted in writing by the IT Director or Network Administrator is subject to disconnection and confiscation by the IT department.

Dial-in modems or private lines (i.e. circuits) on network connected devices must be approved by Network Operations and, if approved, must have authentication procedures and other security-related access parameters conforming to the Network Security Policy before they may be used. All devices which will be attached to the network or use network services must first have their hardware addresses (MAC addresses) registered with Network Operations along with the information of the worker responsible for the device and the location of the device. Devices that are not so registered are subject to disconnection from the network.

Hostnames and Domain Name Services will be administered by Network Operations.

IP addressing of devices:

Servers and other network operations equipment will use IP addresses that are statically assigned. Printers, copiers, and designated workstations will use DHCP to lease an IP address which will be statically assigned based on their mac address. All other workstations and devices will use DHCP to lease an IP address. Any IP addressing conflicts will be resolved according to information found in the Network Operations IP database. Devices found to be using an IP address other than the one they were assigned are subject to disconnection from the network.

Any Network Address Translation devices or procedures must be approved by Network Operations before implementation. Unapproved devices found to be translating addresses will be disconnected from the network.

All network firewalls on the network will be configured, administered and managed by Network Operations. Exceptions must be approved of in writing by the IT Director.

All VPN services being provided must follow a configuration approved by Network Operations and must follow the policies regarding VPN set by the Information Security Administrator.

Wireless Network Access:

Wireless network access at UAEX-LRSO is currently setup to allow for secured (LRSO_WIFI) and unsecured GUEST_WIFI) wireless connections for anyone within the complex. You can set up your wireless device to access either of these networks if you choose.

Downtime:

Scheduled Downtime is necessary for all areas of the network in order to perform maintenance and upgrades on the network devices. Network Operations will notify and work closely with affected users to create reasonable scheduling of the downtimes in order to mitigate the effect of these necessary downtimes on users' operations.

Cabling:

All telecommunications cabling must be approved by Network Operations. Whether the cables are run by a contracted vendor or by the physical plant, they must meet the standards set forth by Network Operations. All cables will be Cat6 compliant and will be terminated by Network Operations in the following manner: office end - Cat6 wall jack, data closet end – next available slot in the punch down panel. Both ends will be clearly labeled in accordance with the numbering scheme set forth by Network Operations.

Data closets, where network devices are connected together through ports on a switch, must be located on the same floor and the same building as those network devices. It is necessary to reserve space in floor designs for those closets when constructing or renovating locations. This requirement exists whether an area uses cabled or wireless network access.

Devices are connected to access switches in data closets using copper Category 6 cabling for all new runs, older runs are still using Category 5 cabling. Data closets are linked together on the premises using multi-mode\single-mode optical fiber (depending on the distance) or Category 6 copper.

Bandwidth Utilization:

No single network-connected device may use network bandwidth for data transmission in a manner that impedes the work of all the other workers. Use of certain sites, such as music\video streaming websites, can slow a network down to a crawl, this is called “bandwidth hog”. Bandwidth hogs impact everybody and therefore require the immediate attention of Network Operations.

Procedure:

When network utilization on a link exceeds 50%, that link may be subjected to a traffic analysis. Any device found in that analysis to be consuming excessive amounts of bandwidth may have its network connectivity suspended (immediately) and the cause of that high network utilization investigated (subsequently). Exceptions to this would be any high bandwidth video conferencing which are deemed to be work related. All instances will be evaluated on a per case basis.

Quarantine Networks:

New Servers and other networked computer equipment which the Information Security Admin may designate shall be set up and configured while connected to special Quarantine Networks. This network is not public and devices connected to it cannot exchange data packets with any other devices on the agency network but can access the internet. Before going into production, devices must move from Quarantine Networks to production networks.

Responsibilities:

The IT Department shall administer the Quarantine Networks. The Information Security Admin shall administer and evaluate the network security testing of servers.

Procedure:

Vendors and server administrators or custodians may only assemble and set up new servers either standing alone (no network connection at all) or connected to a network port on a quarantined network. Quarantined IP addresses should be obtained from Network Operations following the usual procedures for applying for an IP address. The Quarantined network for a given device will be on VLAN 900.

By default, all data processing services which would be delivered via the network are not delivered into a Quarantine network. While setting up and configuring a server, the administrator may need certain services to be brought into the Quarantine network for testing. Requests for these services for testing must be forwarded to the Information Security Admin. The requests must be narrowly defined, noting the source and destination IP addresses and the TCP port number used.

When its administrator believes that the server is ready to go into production, the server will be scanned and tested for known network security vulnerabilities. Any security holes identified by the scan must be fixed before the server may be moved off the quarantined network. The scan also generates warnings. These will be pointed out to the administrator but do not require action. When a scan shows no security holes, the server may be moved to a production network and moved into the server room. The server will also have to pass the requirements for drive imaging and backup operations before being moved to the production network. Refer to the network backup procedures for those requirements.

The server administrator requests a production IP address from Network Operations and gets the port changed from the Quarantine VLAN to a production VLAN. By default, servers will be assigned a private IP address. If the server needs to reach or be reached over the Internet, changes will be made in the firewall to accomplish this.

Immediately after the server has moved onto a production network, it will be scanned again. If this scan turns up security holes for any reason, its network connection will be broken (by disabling the port) until all holes are fixed. This may require moving the server back into quarantine.

Exceptions:

UAEX-LRSO acknowledges that under rare circumstances, certain workers will need to employ systems that are not compliant with this policy. All such instances must be approved in writing and in advance by the Information Security Admin.

Violations:

Violations will be addressed through appropriate disciplinary actions based upon the severity of the infraction and include, but are not limited to, suspension of network accounts, removal of computer equipment, and\or probation and\or termination of employment.