3364-65-08   Network and telecommunications.

(A)   Policy statement

The university provides central coordination, design, and planning for all voice, data, and video network and telecommunication needs. Information technology must procure, coordinate, review, and approve all changes and additions to network and telecommunications infrastructure, services, and equipment to university standards before deployment.

(B)   Purpose

This policy establishes requirements for the coordination and management of the university network and telecommunications infrastructure, equipment, and services.

(C)   Scope of policy

The scope of this policy includes university agents, employees, contractors, temporary personnel and other agents of the university who utilize, maintain, or develop requirements for university network and telecommunication capabilities.

(D)   Definitions

    (1)   Network – two or more devices that are connected with one another for the purpose of communicating data electronically.

    (2)   Network segment – portion of a network that is separated from the rest of the network by a device including, but not limited to, a repeater, hub, bridge, switch, or router.

    (3)   Network address – any logical or physical address that uniquely distinguishes a network node or device over a computer or telecommunications network segment.

    (4)   Network equipment – any physical, logical, or virtual device which enables network connectivity.

(E)   Policy

(1)   Network and telecommunication services

Services will be provided to meet university organizational unit needs when approved and authorized by functional management and information technology. Such services include:

(a)   Requests for relocating or changing the features of an existing telephone. An estimate of any cost to the requester will be provided for approval prior to the start of any work.

(b)   Requests for new or modified data or video connections. An estimate of any cost to the requester will be provided prior to the start of any work by the department of facilities and construction management.

Requests for service shall be initiated through the information technology help desk. Information technology will then assess the technical and economic feasibility of the request.

Prioritization of requests will be the responsibility of information technology. Review of the functional and economic feasibility and appropriateness of the request are the responsibility of the requesting university organizational unit.

The vice president, chief information officer/chief technology officer "CIO/CTO," or designee, recommends prioritization of university-wide network and telecommunication executive leadership of the university. When university resources are unavailable or when proprietary programs, unique services, or other services are required, outside supplier-provided services will be considered.

(2)   Network and telecommunications equipment

Except as authorized by the vice president, CIO/CTO, university organizational units are prohibited from installing or operating network or telecommunications equipment, whether physical, logical, or virtual, that specifically performs network service functions on the university network

without first acquiring information technology approval, including but not limited to:

(a)   Hubs, switches, routers, firewalls, or wireless access points;

(b)   Network address distribution or resolution;

(c)   Intrusion detection, packet sniffers, network analyzers, protocol analyzers.

(3)   Supplier and contract services

In addition to the normal determination of the qualifications of suppliers provided by the purchasing department, suppliers and contracts for network and telecommunication services must be approved by information technology as technically qualified prior to authorizing services. Examples of this would include but are not limited to telephony services, leased lines, internet access, or metro ethernet services.

Discussions with outside suppliers to establish new services or to renew existing services will be coordinated through information technology.

(4)   Network and telecommunications standards

Standards for voice, data, and video protocols will be established by information technology to provide system compatibility among functional users and suppliers of communication hardware and software. Equipment to be connected to the campus network must be approved by the vice president, CIO/CTO or designee.

(5)   New construction or renovation projects

All new building construction or renovation projects are to be reviewed by vice president, CIO/CTO, or designee, for impact on the university's voice, data, and video network as well as for conformity to university communication standards.

(6)   Modifications

Any equipment which modifies the university's voice, data, and video network in any way must be approved by vice president, CIO/CTO or

designee, prior to installation. These standards also apply to equipment which extends or otherwise modifies the network in any way.

(7)   Maintenance and monitoring

(a)   Under the direction of the vice president, CIO/CTO, information technology has the authorization to ban, block, disconnect, disable, prevent or remove equipment or terminate connections when any of the following occurs:

(i)   Law enforcement requests such action or illegal activities are suspected;

(ii)   Unauthorized copyrighted or inappropriate material is being accessed or distributed;

(iii)   Institutional members are circumventing safeguards, abusing network access, creating suspicious activities, including spoofing or masking identities, causing major interruptions in network services, or using excessive network resources;

(iv)   Rogue equipment is detected or suspected of distributing network access or services, or interrupting the service of the network;

(v)   Any external force creates a detrimental condition on university operations, either intentionally or unexpectedly;

(vi)   Commercial activities not sponsored by the university are being hosted on the university network.

(b)   Applications which do not support the university's missions or objectives will be disabled or blocked as necessary. Information technology will use a risk management approach to determine which applications may cause a risk to the university's infrastructure or will allow for secure transfer of information.

(c)   Packets that traverse any university network segment may ~~or may not~~ be actively monitored or reviewed by information technology~~, but depending on severity, segments or the entire network may be~~

~~analyzed or monitored periodically~~ to enforce this policy. Only information technology is authorized to perform this activity.

Effective: 12/14/2020

CERTIFIED ELECTRONICALLY
_____

Certification

12/02/2020
_____

Date

Promulgated Under: 111.15
Statutory Authority: 3364
Rule Amplifies: 3364
Prior Effective Dates: 05/28/2018