29.01.99.X0.03 | AgriLife Extension Network Procedures

Approved: April 20, 2012
Revised: September 12, 2014

Next Scheduled Review: September 12, 2019

PROCEDURE STATEMENT

This procedure establishes data network standard operating procedures for all Texas A&M AgriLife Extension Service (AgriLife Extension) facilities.

REASON FOR PROCEDURE

AgriLife Extension currently operates regional facilities that include data network services. The purpose of this document is to outline features and service levels, and to establish formal guidelines and procedures related to the use of the service. These procedures are established to achieve the following:

- ensure compliance with applicable statutes, regulations, and rules regarding data network use;
- define required practices regarding the use and optimization of the data network; and
- educate individuals who may use the data network with respect to their responsibilities associated with such use.

PROCEDURES AND RESPONSIBILITIES

1.0 GENERAL

1.1 Terms of use:

Electronic data network equipment located in AgriLife Extension facilities are under the management and control of AgriLife Extension except where expressly stated otherwise via approved formal agreements. All use of the data network shall be in compliance with all electronic computing and network rules and procedures published by AgriLife Extension, as well as any applicable state or federal regulations.

1.2 Individuals may be subject to loss of access privileges for AgriLife Extension information resources.

1.3 Any exceptions to the procedures outlined must be preapproved by the directors of AgriLife Extension and Texas A&M AgriLife Research (AgriLife Research).

2.0 RESPONSIBILITIES

2.1 Personal Use of Network Bandwidth

Network bandwidth is limited and should be primarily used for business purposes. While incidental personal use is accepted, the following uses can consume most or all available bandwidth within a regional facility and should be minimized.

A. use of streaming music/audio sites;

B. use of streaming video sites; or

C. use of supervisor–approved peer–to–peer data sharing service sites.

Degradation in network service through continued misuse may require the application of bandwidth restrictions per review by the center director and AgriLife Information Technology (AIT).

Consult with AIT and the center director before using any of the above types of online services or any other high bandwidth classified services for personal use.

2.2 Wired Network Data Jack Connections

The following apply to the use of wired network connections within each facility with the purpose to maintain wiring certifications and service level standards:

A. Existing drops shall not be moved or altered without authorization from AIT.

B. New network drop requests shall be requested through AIT, and will be funded by each regional center location.

C. New network drops can only be added by certified wiring contractors authorized by AIT.

D. Port security is enabled on all network data jacks such that only one device can be connected at a time per data jack.

2.3 Network Wiring Closet Switching Equipment and Wireless Access Equipment

The following apply to the maintenance and management of all network wiring and switching equipment:

A. Under no circumstances shall alteration of the physical configuration of any network wiring or switching equipment be made unless authorized by AIT.

B. Wireless access points and their antennas shall not be altered or changed in any manner.

C. All network wiring closets shall remain secured at all times. An access log shall be maintained for any closet being used for multiple purposes (i.e. storage).

2.4 Installation of Network Equipment

A. Network equipment may only be installed by AIT or any entity authorized and under the direction of AIT. Examples include hubs, switches, or any type of network routing device.

B. Addition of wireless access points via individual hardware or activation of computer–based wireless access points for the purpose of extending or exposing network access is not allowed.

2.5 Wireless Network Use and Guest Access

In each regional facility a wireless network has been deployed with both guest and employee network access. The following shall be adhered to relative to use of these wireless networks:

A. Employees shall always connect to the AGNET wireless network whereas guests can only connect to the AGNET-GUEST network.

B. Guest users of any Texas A&M AgriLife (AgriLife) facility are required to complete the *Guest Network Terms of Use and Authorization* form prior to accessing the network.

C. The *Guest Network Terms of Use and Authorization* form shall be retained electronically per state records retention policies.

2.6 Network Planning, Voice over IP, and Security Systems

Bandwidth usage within the regional centers is very critical to the day–to–day operations of business. The following are designed to maintain service level quality and stability:

A. Any planning with outside vendors or service providers, including Texas A&M University (TAMU) Telecom, with regard to the use or augmentation of the data network shall be coordinated through AIT.

B. Implementation of center wide Voice over IP (VOIP) services shall be facilitated via separate data switching equipment—unless approved otherwise by AIT—in order to preserve or guarantee 911 service functionality is fully facilitated.

C. Implementation of center security systems shall be facilitated via separate data cabling and switching equipment—unless approved otherwise by AIT.

D. Any new business initiatives that would require the ongoing transmission of large quantities of data to and from the regional center facility shall be coordinated with the AIT network operations team in order to conduct an impact analysis.

2.7 Network Server Deployment

A. Installation or deployment of a network server (i.e. file server, video server, or web server) shall be coordinated with AIT prior to procurement and installation for purposes of conducting a virtual server, bandwidth, and security impact analysis.

B. An annual security assessment of each network server within the facility must be documented. This shall be developed in coordination with AIT, and filed with the office of the Information Security Officer (ISO).

C. Designated network server resource managers of any facility based network server are required to participate in monthly information system security (ISS) reviews conducted by the ISO to meet state guidelines regarding timely application and documentation of system operation management requirements.

2.8 Firewall and Network Traffic Blocking

A border firewall has been installed at each regional facility. The following apply to the operation and use of the firewall:

A. All outbound network ports are by default open through the firewall with the exception of those that are blocked as per authority of the center director or related to the use of peer–to–peer file sharing.

B. Network traffic may be blocked upon notification of any system penetration event, illegal use of the network per agency, system, or state guidelines. Owners of computer resources that have been blocked will be notified along with the center director.

C. Network traffic may be limited in the event that system use is consuming quantities of bandwidth that impact the work of other center employees. Owners of computer resources that have been limited will be notified along with the center director.

D. Employees of facilities requiring access to local machines or file services from remote locations will be required to use Virtual Private Networking (VPN) software. For activation, send requests to AIT via the service desk.

RELATED STATUTES, POLICIES, OR REQUIREMENTS

AgriLife Extension Procedure 29.01.03.X0.01 *Information Resource Procedures*

Guest Network Terms of Use and Authorization Form

CONTACT OFFICE

For questions, contact AIT at 979-845-9689 or first-call@tamu.edu.