STANDARD ADMINISTRATIVE PROCEDURE

29.01.03.M0.08 Information Resources – Network Access

Approved July 28, 2005
Revised May 28, 2010
Revised February 10, 2012
Revised August 14, 2013
Next Scheduled Review: August 14, 2018

Standard Administrative Procedure Statement

The information resources network infrastructure in Bryan/College Station is provided by Texas A&M University for users of University facilities. It is important that the infrastructure, which includes media, active electronic equipment (e.g., switchers, routers, access points) and supporting software, be able to meet current performance requirements while retaining the flexibility to allow emerging developments in high speed networking technology and enhanced user services.

Reason for SAP

The purpose of this Texas A&M University network access standard administrative procedure is to establish the process for user access to the University's network infrastructure.

Definitions

Anonymous proxies – tools that attempt to make activity on the Internet untraceable.

Backhaul – transmitting data beyond its normal destination point and back again to utilize network equipment not available at the destination location. It is typically used to mask the location of the point of origin.

Information Resources (IR) – the procedures, equipment, and software that are designed, employed, operated, and maintained to collect, record, process, store, retrieve, display, or transmit information or data.

Official Procedure/ Responsibilities/ Process

1. APPLICABILITY

This Standard Administrative Procedure (SAP) applies to all University network information resources and users of those resources. This SAP is intended to provide a set of measures that will mitigate information security risks associated with network access.

2. PROCEDURES

2.1 Network aggregation devices (e.g., hubs, switches, routers) shall not be connected to network infrastructure without prior approval by Texas A&M IT security team. Contact Texas A&M IT security team through Help Desk Central at hdc@tamu.edu or (979) 845-8300.

2.2 Management of network addresses and name space may be delegated to system administrators. Users are permitted to use only those network addresses issued to them by their designated system administrator.

2.3 Individuals that control right-to-use privileges for systems attached to the University network infrastructure will ensure that only authorized persons are granted access.

2.4 Texas A&M University information resources may not be accessed using any means, such as anonymous proxies, that circumvents the University's ability to identify users by geographic location.

2.5 Most VPN implementers that are not managed by Texas A&M IT services, and which backhaul data from a location to a central site thus masking its true location, are not allowable on the Texas A&M IT network. Contact Texas A&M IT security team for allowable uses through Help Desk Central at hdc@tamu.edu.

2.6 Users shall not alter University owned network hardware in any way.

Related Statutes, Policies, or Requirements

System Policy *29.01 Information Resources*

University SAP *29.01.03.M0.01 Security of Electronic Information Resources*

Contact Office

CONTACT: Office of the Chief Information Security Officer

OFFICE OF RESPONSIBILITY: Associate Vice President for Information Technology & Chief Information Officer