UTEP Standard 19: Server and Device Configuration and Management

19.1 Network Infrastructure Configuration. The UTEP Telecommunications Infrastructure (TI) group is solely responsible for the UTEP network infrastructure and will continue to manage further developments and enhancements to this infrastructure and include:

(a) configuring and managing the resource in accordance with U.T. System and UTEP Information Resources Use and Security Policy, Standards, Guidelines, and Procedures by:

i. segmenting the UTEP network either physically or logically to reduce the scope of exposure of Information Resources commensurate with the Risk and value of the Information Resource and Data;

ii. separating Internet-facing applications from internal applications; and

iii. managing, registering and allocating network addresses for the supported protocols.

(b) maintaining appropriate access to the Network Infrastructure in accordance with U.T. System and UTEP Information Resources Use and Security Policy, Standards, Guidelines, and Procedures;

(c) managing, testing and installing updates to operating systems and applications for network equipment under their responsibility;

(d) all cabling must be installed by UTEP TI or an approved contractor;

(e) all hardware connected to the network may be subject to management and monitoring standards, and must be configured to specifications approved by UTEP TI. Changes to the configuration of active network management devices must not be made without the approval of the UTEP TI. Use of non-sanctioned protocols must be approved by UTEP TI.

19.2 Server Hardening. To protect against malicious attack, all Servers and Devices on UTEP networks will be security hardened based on Risk and must be administered according to UTEP Policies, Standards, Guidelines, and Procedures prescribed by UTEP and U.T. System, as applicable, and incorporates the following procedures:

(a) identify and assign appropriately trained administrators for all Mission Critical Devices, or Servers supporting Information Systems containing Confidential Data;

(b) Minimum Security Standards for Systems as well as other UTEP Guidelines provide the detailed information required to harden a Server or computing Device and must be implemented for UTEP Information Security Office (ISO) accreditation; and

(c) manage the test and installation of service packs, hot fixes, and security patches for equipment under their responsibility.

For more information and additional requirements please refer to The University of Texas at El Paso Information Resources Use and Security Policy, The University of Texas at El Paso Minimum Security Standards for Systems, and The University of Texas at El Paso Payment Card Industry (PCI) Data Security Standard (DSS).

19.3 Device Configuration. All Devices, including but not limited to routers, laptops, tablets, desktops, and handheld devices, on UTEP networks must be protected against malicious attack. The ISO shall establish and communicate security configurations based on Risk and incorporate the following procedures:

(a) set baseline security "hardened" configuration Standards for common operating system platforms and devices;

(b) establish and make available minimum security standards for University-owned and Non-University Owned Portable Computing Devices; and

(c) ISO or other approved team will test security patches against Information Security core resources before release where practical, and not more than 30 days from release date for PCI systems. The only exception being when immediate application would interfere with business requirements. Security patches must be implemented within the specified timeframe of notification from the ISO or other approved team.

19.4 Device Management. Departments and/or Colleges shall ensure that devices are administered by professionally trained staff in accordance with Policies, Standards, Guidelines, and Procedures prescribed by the Institution.

19.5 Access to Information Security Information and Devices. All Owners and Custodians of University owned, leased, or controlled Information Resources must provide the ISO with direct access to detailed security status Information including, but not restricted to, the following:

(a) firewall rules;

(b) IPS/IDS rules;

(c) security configurations and patch status; and

(d) sufficient access rights to Servers and Devices to independently and effectively execute ISO monitoring duties.

19.6 System Disclaimer/Warning Banner. All systems that store Confidential Information must display the following banner, or similar CISO approved banner(s):

System Disclaimers

Use of computer and network facilities owned or operated by The University of Texas at El Paso requires prior authorization.

Unauthorized access is prohibited. Usage may be subject to security testing and monitoring, and affords no privacy guarantees or expectations except as otherwise provided by applicable privacy laws. Abuse is subject to criminal prosecution.

Use of these facilities implies agreement to comply with the policies of The University of Texas at El Paso.

OR

This system is for the use of authorized users only. Individuals using this computer system without authority, or in excess of their authority, are subject to having all of the activities on this system monitored and recorded by system personnel.

In the course of monitoring individuals improperly using this system, or in the course of system maintenance, the activities of authorized users may also be monitored. Users (authorized or unauthorized) have no expectation of privacy except as otherwise provided by applicable privacy laws.

Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence of such monitoring to campus officials or law enforcement agencies. By continuing to use this system you indicate your awareness of and consent to these terms and conditions of use.

19.7 Miscellaneous

(a) Owners of Devices and Servers housing Confidential Information will perform periodic audits to ensure that all outlined security measures are in place.

(b) Any system or hard drive that contained Confidential Information and that is transferred to Surplus must be wiped of all data in accordance with the Electronic Data Destruction Guidelines.

(c) Any system that contained Confidential Information must have the electronic media wiped of all data in accordance with the Electronic Data Destruction Guidelines prior to transferring or reallocation of the system.

(d) Confidential Information must not be displayed in any public way (e.g., in posted lists, mailing labels, system screen in public areas, web pages, etc.)

19.8 All systems providing commodity services to University affiliates (e.g., web servers, mail servers, file servers, database servers, directory servers, etc.) must either be physically co-located within the University Data Centers or be virtualized within the IT Virtualization service.

(a) The Information Security Office will work with Colleges, Schools, and Departments to proactively identify all such qualifying systems.

(b) Exceptions must be submitted for approval by the CISO via a Security Exception Request Form in cases where business, technical, or research needs require the system to be locally hosted. All exceptions must identify the business need for the exception and the compensating controls that will be implemented to offset the risks associated with locally hosting the system. A single exception may be filed for a number of devices as long as the devices can be uniquely identified (e.g., UTEP Inventory Tag, Service Tag/Serial Number, MAC address). For more information please refer to the Security Exception Reporting Process.

19.9 All Units are required to have their local Information Resources Custodian(s) participate in processing (e.g., inventory, standards verification, configuration) of all IT procurements (e.g., network-capable computing devices and large dollar or high risk software). This includes but is not limited to any University-owned devices that have the ability to store University data or use the University wired or wireless networks. Example of these types of computing devices include but are not limited to laptops, desktops, computers, tablet devices, and servers.

(a) For Units where Central IT support contracts exist, the contracting entity will be required to provide the local Information Resources Custodian(s) with a complete inventory of computing devices for the contracted Unit. The Information Resources Custodian(s) will perform these tasks in a timely manner so as not to delay distribution of the device to the end user.

(b) All Units creating Purchase Orders or ProCard transactions for IT Procurements (e.g., network-capable computing devices and large

dollar or high risk software) will ensure the Information Resources Custodian(s) are aware of the delivery destination.

i. The local Information Resources Custodian(s) will ensure the device is properly tagged for UTEP inventory and accounted for.

ii. The local Information Resources Custodian(s) submit a System Information Form to the CISO which contains the computing device information and will configure it per policy requirements. All University and specific Unit procedures for configuration will be applied including but not limited to encryption, system management tools, and strong user account passwords.

(c) Department Heads or their designate may submit a Security Exception Request Form to the CISO to this operational procedure in the event it would unnecessarily burden their Unit. Please refer to the Security Exception Reporting Process for more information.

19.10 Revision History

Complete Rewrite: May 31, 2017 (align with UTS165)
Approved: June 9, 2017
Gerard D. Cochrane Jr., Chief Information Security Officer