OIS 23 – Standard for Network Configuration

I. STANDARD STATEMENT

The UTSA Standard for Network Configuration establishes the rules for the maintenance, expansion and use of the network infrastructure. These rules are necessary to preserve the integrity, availability and confidentiality of UTSA information.

II. RATIONALE

This standard supports HOP Policy 8-12 Information Resources Use and Security Policy

III. SCOPE

This standard applies to all UTSA faculty, staff, and students.

IV. CONTACTS

The Office of Information Security
informationsecurity@utsa.edu

V. PROCEDURES

A. The UTSA Standard for Network Configuration applies equally to all individuals with access to any UTSA information resource.
   1. UTSA University Technology Solutions (UTS) is the custodian of and is responsible for the UTSA network infrastructure and will continue to manage further developments and enhancements to this infrastructure.
   2. To provide a consistent UTSA network infrastructure capable of exploiting new networking developments, all cabling must be installed by UTS or an approved contractor under management by UTS.
   3. All equipment that is connected to the network must be configured to specifications approved by UTS.
   4. All hardware connected to the UTSA network is subject to UTS management and monitoring standards.
   5. Changes to the configuration of active network management devices must have the prior approval of UTS.
   6. The UTSA network infrastructure supports a well-defined set of approved networking protocols. Any use of non-sanctioned protocols must be approved by

UTS. The networking addresses for the supported protocols are allocated, registered and managed centrally by UTS.

7. All connections of the network infrastructure to external third party networks will be the responsibility of UTS. This includes connections to external telephone networks.
8. The use of departmental firewalls is not permitted without prior written authorization from UTS.
9. Users must not extend or re-transmit network services in any way. Users must not install a router, switch, hub or wireless access point to the UTSA network without UTS approval.
10. Users must not install network hardware or software that provides network services without UTS approval.
11. Users are not permitted to alter network hardware in any way.

Title: OIS 23 – Standard for Network Configuration
Last Revised: September 21, 2017
Last Reviewed: August 5, 2020