

## **29.01.99.N0.05 Network Configuration and Wiring**

Approved: February 3, 2012

Revised: March 22, 2018

Revised: July 7, 2023

Next Scheduled Review: July 7, 2028

### **Summary**

The purpose of this SAP is to establish the rules for the maintenance, expansion, and use of the network infrastructure. These rules are necessary to preserve the integrity, availability, and confidentiality of TEEX information. The TEEX Network Configuration SAP applies equally to all individuals with access to any TEEX Information Resource. The TEEX network infrastructure is provided as a central utility for all users of TEEX Information Resources. It is important that the infrastructure, which includes cabling and the associated equipment such as routers and switches, continues to develop with sufficient flexibility to meet user demands while at the same time remaining capable of exploiting anticipated developments in high-speed networking technology to allow the future provision of enhanced user services.

### **Definitions**

Information resources as defined in Texas Government Code § 2054.003(7) means the procedures, equipment, and software that are employed, designed, built, operated, and maintained to collect, record, process, store, retrieve, display, and transmit information, and associated personnel including consultants and contractors.

### **Requirements**

1. TEEX Network Information Services (NIS) owns and is responsible for the TEEX network infrastructure and will continue to manage further developments and enhancements to this infrastructure.
2. To provide a consistent TEEX network infrastructure capable of exploiting new networking developments, all network wiring projects in TEEX-owned or leased space shall be requested through NIS to ensure standardization within TEEX and compliance with the Texas Administrative Code (TAC) and TEEX security control catalog.
3. All network connected equipment must be configured to a specification approved by TEEX NIS and consistent with the Security Controls Catalog linked from the [NIS Security page](#).
4. All hardware connected to the TEEX network is subject to TEEX NIS management and monitoring standards.

5. Changes to the configuration of active network management devices must not be made without the approval of TEEX NIS Security.
6. The TEEX network infrastructure supports a well-defined set of approved networking protocols. Any use of non-sanctioned protocols must be discussed with [NIS Security](#) before authorization and documented by TEEX NIS prior to implementation using the [NIS Security Exception Form](#).
7. The networking addresses for the supported protocols are allocated, registered, and managed centrally by TEEX NIS.
8. All connections of the network infrastructure to external third-party networks are the responsibility of TEEX NIS. This includes connections to external telephone networks.
9. TEEX NIS must authorize and coordinate the installation and operation of all network infrastructure and security devices.
10. The use of departmental firewalls is not permitted without the written authorization from TEEX NIS as well as documented using the NIS Security Exception Form.
11. Users are not permitted to extend or re-transmit network services in any way. This means you must not install a router, switch, hub, or wireless access point to the TEEX network without TEEX NIS approval.
12. Users are not permitted to install network hardware or software that provides network services without TEEX NIS approval.
13. Users are not permitted to alter network hardware in any way.

## **Quality Assurance Measures**

NIS will conduct a periodic review and scanning of network connected devices, the wireless network signals, and the security exceptions.

## **Related Statutes, Policies, and Requirements**

[System Policy 29.01, Information Resources](#)

## **Office of Responsibility**

Network & Information Services  
(979) 458-6868