

Network Configuration Standard

Revision Date:

1. Purpose: The purpose of the EPCC Network Configuration Security Standard 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 EPCC information.

2. Scope: The EPCC Network Configuration Standard applies equally to all individuals with access to any EPCC Information Resource.

3. Description: The EPCC network infrastructure is provided as a central utility for all users of EPCC 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.

- EPCC Information Technology (IT) owns and is responsible for the EPCC network infrastructure and will continue to manage further developments and enhancements to this infrastructure.
- To provide a consistent EPCC network infrastructure capable of exploiting new networking developments, all cabling must be installed by EPCC IT or an approved contractor.
- All network connected equipment must be configured to a specification approved by EPCC IT.
- All hardware connected to the EPCC network is subject to EPCC IT management and monitoring standards.
- Changes to the configuration of active network management devices must not be made without the approval of EPCC IT.
- The EPCC network infrastructure supports a well-defined set of approved networking protocols. Any use of non-sanctioned protocols must be approved by EPCC IT.
- The networking addresses for the supported protocols are allocated, registered and managed centrally by EPCC IT.
- All connections of the network infrastructure to external third party networks is the responsibility of EPCC IT. This includes connections to external synchronous optical (SONET) and telephone networks.
- EPCC IT firewalls must be installed and configured following the EPCC Firewall Implementation Standard documentation.
- The use of departmental firewalls is not permitted without the written authorization from EPCC IT.
- Users must not 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 EPCC network without EPCC IT approval.
- Users are not permitted to alter network hardware in any way.

- Users must not install network hardware or software that provides network services without EPCC IT approval.
- IT reserves the right to remove any network device that does not comply with standards or is not considered to be adequately secure.

4. Enforcement: Violation of this standard may result in disciplinary action in accordance with El Paso Community College policy and procedures. If you need clarification of this standard, call or e-mail Richard Buller, 831-6312, richardb@epcc.edu, from the Vice President for Information Technology/Chief Information Officer.

References

Copyright Act of 1976
Foreign Corrupt Practices Act of 1977
Computer Fraud and Abuse Act of 1986
Computer Security Act of 1987
The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
The State of Texas Information Act
Texas Government Code, Section 441
Texas Administrative Code, Chapter 202
IRM Act, 2054.075(b)
The State of Texas Penal Code, Chapters 33 and 33A
EPCC Computer Security - 2.05.01.30
EPCC Information Security – 2.05.08.