Collin College Technology Services (CC-TS)
Firewall – Information Security Procedure (ISP)

PURPOSE:

External firewalls protect the Collin College (CC) gateways between the Internet and the CC network to establish a secure environment for the College's technology resources. Virtual Local Area Network (VLAN)'s are in place to establish secure communications between different segments of the College's network where different levels of security are warranted. Firewalls are enabled and configured on servers and workstations attached to the College's internal network.

CC's firewalls are vital components of the College's network security architecture. The Firewall ISP governs how the firewalls filter traffic to mitigate the risks and losses associated with security threats to CC's information technology resources. This ISP will attempt to balance risks incurred against the need for access.

This ISP aims to protect CC's information technology resources from hacking and virus attacks by restricting access to information technology resources on the College campus. It is designed to minimize the potential exposure of CC to the loss of sensitive, confidential data, intellectual property, and damage to the public image, which may follow from unauthorized use of CC's information technology resources.

SCOPE:

The Firewall ISP applies to all firewall devices owned and operated by CC.

STATEMENT:

Perimeter Firewalls:

The perimeter firewall permits the following outbound and inbound Internet traffic:

- *Outbound* - All Internet traffic to hosts and services outside CC's networks except those specifically identified and blocked as malicious sites.
- *Inbound* - Allow Internet traffic to support the institution's mission and define the system, application, and service procedures.
- *Outbound/Inbound* – All internet traffic detected as malicious by the College's intrusion prevention system (IPS), and all traffic violating CC firewall policies are dropped.

Reason for filtering ports and applications:

- Protecting CC Internet Users - Certain ports and applications are filtered to protect CC information technology resources. The perimeter firewall protects against certain common worms and dangerous services on CC information technology resources that could allow intruders access.

- Protecting our outbound bandwidth - If CC Internet users overuse their outbound bandwidth by running high-traffic servers or becoming infected with a worm or virus, it can degrade the service of other CC systems.
- Protecting incidental Internet threats – Access Control Lists prevent users from knowingly or unknowingly attacking other computers on the Internet. In addition to being in CC's interests to protect our bandwidth, it is the institution's responsibility to prevent abuse of its network.

ROLES AND RESPONSIBILTIES:

The Chief Information Security Officer is responsible for implementing, configuring, and maintaining CC's firewalls and activities relating to this ISP.

- At a minimum, firewalls must be annually tested and reviewed.
- When significant network requirements change, firewall security policies will be reviewed and may warrant changes.
- Firewalls must have alert capabilities and supporting procedures.
- Auditing must be active to permit analysis of firewall activity.

Related ISP's, References, and Attachments:

An index of approved CC-TS ISPs can be found on the CC Technology Services website at https://www.collin.edu/security

Implementation Information

Review Frequency:	Annually
Responsible Person:	CISO
Approved By:	Abe Johnson, Ed. D.
Approval Date:	02/09/2022

Revision History

Version:	Date:	Description:
1.0	02/09/2022	Initial document
1.1	10/28/2022	Annual Review – No Changes required.
1.2	03/19/2024	Inclusion of “applications” as part of best practices.