Office of Information Technology

IT Standard
NETWORK FIREWALLS AND ROUTERS

Standard:	IT10003
Original Effective Date:	09/21/2010
Last Revised:	08/06/2021
Last Reviewed:	08/06/2021
Next Scheduled Review Date:	08/01/2022
Version No.:	2.2
Administrative Owner:	Director of Information Security Services

PURPOSE

The Montgomery College ("College") Office of Information Technology (OIT) is responsible for controls that administer secured access to College information and technology resources while mitigating risks to their confidentiality, integrity and availability. This is a multi-layered security control system and includes the use of network-based firewalls. This document provides the minimum standards by which the College manages network-based firewalls.

SCOPE

This standard applies to all network-based firewalls and routers. The scope does not include host-based firewalls.

STANDARD

A. General

1. The IT Security Group (ITSG) is responsible for managing all network-based firewalls.
2. The Network Engineering Group (NE) is responsible for managing all network routers
3. All network-based firewalls must restrict inbound and outbound traffic to that which is necessary for the environment.
4. For perimeter firewalls, any packets entering the College's network that have a source address of an internal host should be denied.
5. No traffic should be allowed to leave the College's network that does not have an internal source address.

B. Network Location

1. A network-based perimeter firewall must be installed at each Internet connection and between any DMZ and the internal network zone.

C. Management

1. All changes to network-based firewalls and routers must be documented via the College's Change Management Process.
2. Requests to modify network-based firewalls must include business justification and list all services, protocols, ports and direction of traffic.
3. Firewalls and routers must be secured from unauthorized access

D. Maintenance

1. Firewall rule sets for systems and applications in scope for PCI compliance must be reviewed at least every six months. The review should include ensuring rules are needed and contain accurate, current information.
2. The firewall and router configurations must be backed up periodically.
3. Firewall logs must be retained for at least three months and for no more than one year per the Logging Standard.
4. Firewalls and routers must be monitored in terms of physical health and system processes.

E. Network Diagrams

1. NE shall maintain network diagrams that reflect the current network design
2. NE shall update network diagrams whenever changes are made to the network layout

EXCEPTIONS

Exceptions to this standard will be considered on a case-by-case basis in accordance with the IT Exception Request Form.

COMPLIANCE AND RECOURSE FOR NON-COMPLIANCE

Montgomery College has established College Policies/Procedures and the OIT has established IT Standards and Processes and associated guiding documents to provide appropriate protection of technology resources, to assure protection of personally identifiable and sensitive information and to promote privacy. Any faculty, staff, contractor, vendor or other agent found to have violated any part of College Policies, Procedures or IT Standards or Processes may be subject to disciplinary action and/or legal action.

RELATED DOCUMENTS

Acceptable Use Policy and the accompanying Procedure/Guidelines Statement

WEB SITE ADDRESS FOR THIS STANDARD

APPROVALS / REVISION HISTORY

DATE	VERSION / REVISION / NOTES	APPROVER
September 21, 2010	Original roll-out of this Network Firewalls and Routers document.	Patrick Feehan, Information Security and Privacy Director/ITPA
January 26, 2018	Revised.	Patrick Feehan, Information Security and Privacy Director/ITPA
September 30, 2020	Decided upon and added review cycle dates.	Nell Feldman / Keith Wilson
August 6, 2021	Slight update to firewall logs retention period (min. 3 months instead of 6).	Nell Feldman, Director of Information Security Services