



Firewall Management Security Policy

Document Version Number:	2.5
Document Control Number:	ITS.EIS-POL001
Last Updated:	7/22/2025
FOIA Exempt?	No

Process Owner:

- Information Technology Services Enterprise Infrastructure Services

SCOPE:

This policy defines the essential rules regarding the use, management, and maintenance of firewalls at George Mason University. It applies to all firewalls on the university’s networks and Information Technology Services (ITS) employees responsible for managing and maintaining these firewalls.

POLICY STATEMENT:

- All firewalls at George Mason University are managed by the Enterprise Infrastructure Services (EIS) division of ITS. Administrative access to a firewall system is authorized by the EIS Executive Director.
- All firewalls at George Mason shall have a default deny ruleset - traffic is blocked by default and allowed to pass by exception. Exceptions to the default deny ruleset are authorized by the Director of Cybersecurity Operations and the EIS Executive Director.
- Firewall system hardware is maintained and replaced regularly.
- Firewall system software is kept current, and vulnerabilities are addressed immediately.
- Firewall system and security logs shall be collected in a common repository for analysis.
- Firewall configurations must be regularly backed up for system recovery and analysis.
- Administrative authentication shall adhere to the university (University Policy 1311) and ITS authentication and password policies.
- All changes shall be managed in accordance with ITS Change and Configuration Management Policy (ITS.ESD-POL001) and procedures.

RESPONSIBILITIES:

ITS Personnel with Administrative Access to firewalls

- Must abide by this policy.

EIS Executive Director

- Authorizes administrative access to the firewall system.
- Authorizes exceptions to the default deny ruleset.

Titles and department names are subject to organizational changes.



Director of Cybersecurity Operations

- Authorizes exceptions to the default deny ruleset.

Cybersecurity Operations

- Performs vulnerability assessments on all university firewalls.
- Immediately reports discovered vulnerabilities to firewall managers, the Director of Cybersecurity Operations, and EIS Executive Director.

COMPLIANCE:

All ITS employees are required to abide by this policy and follow any applicable standard(s) and processes/procedures. If the conflict is not resolved to the satisfaction of the applicable parties, the matter may be escalated to the VP Information Technology and CIO, Vice President for IT, for further review and action.

Exceptions: Departure from this policy is allowed by documented exceptions approved by the Director of Cybersecurity Operations and the EIS Executive Director.

REVIEW SCHEDULE:

Every 3 years

DEFINITIONS AND ACRONYMS:

Terminology or Acronym	Definition
Firewalls	Firewalls are security systems that control and restrict network traffic and network services. They are essential components of the George Mason University information systems security infrastructure.

APPROVAL:

Title, Department Name	Name	Signature and Date
Executive Director, ITS Enterprise Infrastructure Services	Ben Allen	Signed by: <i>Ben Allen</i> 7/24/2025 02AB20D3D861498...
Interim Director, Director of Cybersecurity Operations	Yu Kuo	Signed by: <i>Yu Kuo</i> 8/29/2025 1037F74D6F864ED...

REVISION HISTORY:

Date	Version Number	Department or Author	Brief Description of Changes
6/19/2018	1.0	ITS Enterprise Infrastructure Services / Ben Allen	Initial release.

Titles and department names are subject to organizational changes.



8/2/2018	2.0	ITS Enterprise Infrastructure Services / Ben Allen IT Process and Planning / Cindy Kim	Major (incorporated recommendations from the Office of University Audits) and minor revisions (changed policy owner, added document control number and related/reference documents)
9/12/2018	2.01	ITS Enterprise Infrastructure Services / Ben Allen	Minor revisions (updated related/referenced documents)
9/18/2019	2.2	ITS Enterprise Infrastructure Services / Ben Allen	Annual review with minor revisions (reformatting, removing references to old university policies, and correcting upper management titles)
3/6/2023	2.3	ITS Enterprise Infrastructure Services / Ben Allen	Annual review with minor revisions (reformatting and updating job titles)
5/9/2024	2.4	ITS Enterprise Infrastructure Services / Ben Allen	Annual review with minor revision (updated document control number for ITS Change and Configuration Management Policy and review cadences, and deleted policy statement #4)
7/22/2025	2.5	ITS Enterprise Infrastructure Services / Ben Allen	Annual review with minor edits (reformatting and updating group name)

RELATED DOCUMENTS/REFERENCES:

- [Information Technology Security Standard 2.1](#)
- [University Policy Number 1311, Information Technology Security Program](#)
- ITS Change and Configuration Management Policy (ITS.ESD-POL001) and procedures
- Firewall Access Standards (ITS.EIS-STD001)
- Firewall Management Standards (ITS.EIS-STD002)
- Firewall Exception Standards (ITS.EIS-STD003)
- Firewall Ruleset Engineering Standard (ITS.EIS-STD005)