

3.4 Firewall Exceptions and Ruleset Procedure

Effective Date: October 27, 2025

Revised Date: July 28, 2026

1. Purpose

This document establishes a standardized procedure for the firewall exceptions and rulesets on the Arkansas State University - Jonesboro (A-State) campus. The goal is to create a clear and consistent procedure for all firewall requests.

2. Scope

These procedures apply to all Arkansas State University - Jonesboro faculty and staff firewall requests.

3. Definitions

- **Firewall** – Network security device that monitors and controls incoming and outgoing traffic on the network based on predetermined rules.
 - **Ruleset** – A collection of rules that act as a security policy to filter network traffic.
 - **Port** – A communication endpoint that identifies a specific process or service on a device.
-

4. Firewall Exception Process

Firewall exceptions added to the A-State firewall must adhere to the following:

- Firewall exceptions (open ports) must be requested in writing via a TDX work order using the [Firewall Policy Change](#) form.
 - Requests must be justified and approved by the Security Division and the Networking Division.
 - Requests must be reapproved annually.
 - ITS may scan devices that can be accessed via open ports for security issues. All issues found must be corrected/justified in five business days or the firewall exception will be closed.
 - ITS may close an open port at any time for security reasons.
 - ITS may, at its discretion, decline to open a port.
-

5. Standards Review

This document will be reviewed and reaffirmed annually, or upon significant changes to university IT governance, systems, or regulatory requirements.

Effective Date: October 27, 2025

Next Review Date: July 28, 2027

Version: 1.1

Revision #4

Created 2025-10-31 02:15:46 UTC by Christopher Boothman

Updated 2026-07-28 19:16:55 UTC by Jacob Weaver