Information Technology Services

# WSU Standard for Boundary Devices

Author(s): Steven Conover
Keela Ruppenthall

Date: 06/12/2020

Washington State University

## Revision History

| Version No. | Date | Description | Author |
|---|---|---|---|
| 1.0 | 06/12/2020 | Initial Release | Steven Conover<br>Keela Ruppenthall |

## Contents

## Standards References

**Washington State OCIO 141.10.**
3.1, 5.1.2 (1, 2), 5.5, 5.6 (2,3), 6.1.2 (7, 12), 6.4 (1, 4, 5, 6, 7), 7.1 (1), 7.3 (1)

**NIST 800-53 (rev4):**
AC (2, 6, 7), AU (2), CM (1, 2, 3, 4, 5, 6, 7, 8, 9), CP (8), PE (3), SI (1, 2)

# Standard for Boundary Devices

## Boundary Device Standard

### Purpose:

This standard contains the Washington State University (WSU) Standard for Boundary Devices. The purpose of this standard is to establish the specific recommendations for the configuration and administration of WSU boundary devices.

### Scope:

This policy applies to all Institutional business units, workforce members, and institutional information systems that collect, store, process, share, or transmit Institutional Data

# Standard:

## Boundary Status Meetings

Communication is a crucial component of security posture. WSU has a very large footprint, both physically and logically. WSU contains multiple ingress/egress points that are maintained by multiple administrators. WSU also contains multiple high-level security zones, such as data centers, research units, etc., that are logically separate and distinct from the lower level zones of the common access network. Due to this large scale, it is important to ensure that boundary defenses are secured to the same level in accordance with the mission of the University.

- WSU shall hold Boundary Status meetings as required to assess the state of boundary defenses. Attendees of these meetings shall be any persons who are responsible for any ingress/egress points on the WSU network that constitutes a boundary as defined in this document.
    - Topics for meetings may include, but are not limited to:
    - Revisions to the WSU Standard for Boundary Devices document
    - New firmware versions for ingress/egress points
    - Point of contact updates

## System

### Operating System Version Control

- Boundary devices across all WSU networks shall be provided regular firmware updates while in operation. Firmware versions shall be reviewed biannually, emergency firmware updates shall be installed within 36 hours. All firmware updates shall be acquired directly from the vendor through the vendor-approved channels.
- When choosing a firmware version, vendor support may be required. Vendors often have a recommended firmware version; recommended firmware versions shall be used when available, if applicable.
    - Firmware shall be verified as valid before installation on boundary devices.
- All boundary devices for WSU shall maintain the same firmware code version. Stakeholders may discuss firmware versions at the Boundary Status meetings.

- New device firmware will be tested at the Pullman and Spokane campuses for no more than 30 days. If the testing is successful, the firmware to be considered valid. All other boundary devices shall be upgraded within 7 days.

### Threat (Dynamic) Updates

- Threat (dynamic) updates shall be monitored and applied in a timely manner. To ensure timely installation, automatic updates, if available, shall be configured. If automatic updates are not available, updates shall be applied no later than 7 days after release.

## System Access

### Physical Access

- Physical access to any location that houses a boundary device shall be secured with access limited to employees with a valid need to know.
- Boundary devices shall be restricted from physical contact and secured with multi-factor authentication (MFA). The factors are defined as: (i) something you know; (ii) something you have; or (iii) something you are.
- Inside the secured location, the boundary devices shall be placed in locked enclosures.
- Physical access points to locations securing boundary devices shall be monitored 24 hours a day, 7 days a week. This access data shall be retained for no less than 6 months.

### Interactive Access

- Administrator accounts shall only be issued on an as-needed basis. When this access is no longer required, administrator accounts shall be removed. Boundary devices shall be audited quarterly to ensure that all active administrator accounts are valid.
- Credentials for administrative access to boundary devices shall not be shared with any other devices. Unique administration credentials shall be assigned to each person.
- MFA is required when available.
- Access to boundary devices is limited to specific Tier 1 source IPs.
- All changes made by administrator accounts shall be logged, on both the local device and a remote logging server. The security operations department will monitor all changes. Atypical use of accounts shall be reported.
- Unsuccessful login attempts to boundary devices shall be limited to five attempts. After five unsuccessful login attempts, the account shall be locked for a minimum of 60 minutes.

- Unsuccessful login attempts will be recorded, both on the device and to a remote logging server. The security operations department will monitor this log data.

## System Configuration

### Standardized Baseline Configurations

- Standardized baseline configurations are required to be used on all WSU boundary devices on all campuses.
    - Campus requests for exemptions to standardized baseline configuration element(s) must be submitted through Change Control with justification(s) and approved by Campus CIO.
- Standardized baseline configurations are to be reviewed and updated quarterly.
- Three previous baseline configurations (current version minus 3) are to be retained in a configuration archive.
- When technically feasible, ingress filtering shall be applied to boundary devices to protect against Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks.
    - Network ingress filtering practices should employ guidance from Best Current Practice No. 38, put forth by the Internet Engineering Taskforce (IETF) and be included in Standardized Baseline Hardening configurations.

**Standardized Baseline Hardening:**

- WSU System Naming Conventions
    - Standardized naming conventions are to be used across all WSU campuses to easily identify Campus, Zone, Device, and Node Number.
        - Example 1: PUL-00-OR-01 for Pullman-Transport Zone-Border Router-01
        - Example 2: SPO-01-DR-02 for Spokane-Distribution Zone – Distribution Router-02
- A centralized event logging location is needed to enable continuous monitoring.
- Baseline hardening should be incorporated into every configuration change.
- After a boundary device configuration change, baseline hardening scripts shall be re-applied to the device and the configuration will be reviewed for accuracy before the maintenance process for that device is closed.

**WSU System - Information Boundaries**

- WSU information boundaries are to be classified by Trust Level. Appropriate controls shall be in place to reduce the risk associated with the Trust Level of that boundary.

- **Boundary 1 (B1):** WSU boundary to the Internet - Trust Level: Untrusted
  - Baseline “in/out” policies, security profiles, access control lists, etc. explicitly permit only those applications and packet flows required to conduct WSU business.
    - Implicit Deny for all traffic flows not associated to WSU business
  - Ensure all data flows are mapped to specific user identities
    - Require known User-ID for traffic originating in user zones
    - Prevent unauthenticated devices from reaching the Internet
  - Unknown Devices
    - Captive Portal with fewest applications required for initial configuration
      - Use strong authentication techniques (i.e., Kerberos) with captive portal
  - Incorporate user groups in policy to tune for best practices
    - Establish Employee vs. non-employee distinction (e.g. decryption, blocking tunneling apps)
    - Create Quality of Service (QoS) policies by user group

- **Boundary 2 (B2):** WSU boundary between communities of interest (COIs) exchanging WSU Non-Public and/or WSU Confidential data – Trust Level: Based on data sensitivity.

    - Reference COI Trust Table

## COI Trust Table

| | Group Policy | Virtual LAN<br>(VLAN) | Shared VPN Gateway | Dedicated VPN Gateway | Intrusion Prevention | Firewall |
|---|---|---|---|---|---|---|
| Non-Public<br>(CIO A) | X1 | X1 | | | | |
| Confidential (CIO B) | X1 | X1 | X1 | X 2 | | |
| Confidential<br>Co-Located<br>(CIO C) | X1 | X1 | | | X 3 | X 3 |

Notes: X1: Limits network access to a private server
X2. Protects private server with its own LAN
X3. If required

COI type A: enforced group policies, and potentially a VLAN, will be used to control access to the server.

COI type B: VLAN and policy-based routing shall segregate the COI from WSU. VPNs and group policy will provide confidentiality and access to distributed members of the group.

COI type C: the server resides within the responsible WSU information unit and segregated from other units by boundary devices. Group policy and VLAN control the access to the server. Intrusion prevention and a firewall may be deployed to improve the segregation of the group from WSU.

## Change Control

### Change Management

- Configuration Changes to WSU boundary devices are governed by WSU BPPM: Configuration Management Policy.
  - In order to minimize the number and impact of any related incidents, a change management process shall be followed for all changes to ensure that standardized methods and procedures are used for efficient and prompt handling of all changes associated with the University's Technology infrastructure and services.
  - Changes are defined as the addition, modification, or removal of a configuration setting, service, or service component, to include its associated elements.

## Documentation

### WSU Boundary Components Workbook

- Boundary Components Workbooks will contain:
  - Device Name
  - Device Location
  - Device Interface IP addresses
  - VLANs Used & Reserved

  - Network Diagrams
  - Vulnerability Scan Results
  - Security Audit Results
  - User Access List
  - How to Access
  - Points Of Contact (POCs)

- Workbook sections shall be created and updated by group responsible for that portion of the workbook.

  Example:

  - Network group creates/updates network drawings
  - Security group creates/updates security documents
    - Example: WSU Border Configuration Workbook, scans, audits, etc.

- Workbooks shall be maintained in a central repository with all other campuses' workbooks.

  - Access shall be defined by Role / Permissions
    Example:
    - Network Engineers
    - Network Analysts
    - Security Engineers
    - Security Analysts
    - Managers

- Workbooks shall be updated annually

## Business Continuity / Disaster Recovery

- An established business continuity/disaster recovery plan shall be developed and followed that identifies boundary devices as critical information system assets supporting essential WSU missions and business functions
- Business Continuity/Disaster Recovery Plan shall be documented and developed using WSU policies and guidelines.
- Alternate telecommunication services (for data and voice) shall be established including necessary agreements to permit the resumption of essential WSU missions and business

functions within 48 hours when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.

  - Agreements shall contain priority-of-service provisions in accordance with availability requirements of essential WSU missions and business functions; and,
  - Reduce the likelihood of sharing a single point of failure with primary telecommunications services.

- Information System backup information, including user-level and system-level information, together with security-related documentation shall be protected to ensure the confidentiality, integrity, and availability of backup information at storage locations.

  - Information System backup information shall be tested semi-annually to verify media reliability and information integrity.

- The Business Continuity / Disaster Recovery plan shall provide for the recovery and reconstitution of the boundary device to a known state after disruption, compromise, or failure.

**Administration Point of Contact**

- Primary and secondary contacts for each boundary device shall be documented. These contacts shall be updated biannually at a minimum.
- Primary and secondary contacts shall be used for all events and incidents involving boundary devices. These contacts shall be engaged via a support ticket.

## Administrative:

The Office of the Chief Information Officer is responsible for the administration of, and the enforcement of compliance with this standard.

## Definitions:

For further clarification on the terminology and definition of terms used within this document, please refer to this organization's published glossary of terms associated with this document.

## Exceptions:

Exceptions to this policy shall be managed and maintained by the Office of the CIO, following the processes outlined by WSU BPPM: Configuration Management Policy and ITS Exceptions Process.

## Review Cycle:

This standard is to be reviewed every three years or on an as-needed basis due to changes to technology environments, business operations, or regulatory environments.