# Network Device Security and Configuration Policy

## Overview

Routers and smart switches provide important security functions within a network. Configured correctly, they are one of several hardware and software devices available that help manage and protect a private network from a public one. This document describes a required minimal security configuration for routers and switches connecting to the [LEP] production network or used in a production capacity within [LEP].

## Purpose

Routers and switches physically (and virtually) separate logical networks through configuration and protocol management. Effective management of these important network devices helps to protect internal network resources from external risks. This policy provides policy and protocol standards to minimize security and intrusion risks related to internal resources from outside influences.

## Scope

This policy applies to all [LEP] staff who support network switch and routing technologies.

## Policy

### GENERAL

The following general procedures and protocols shall be applied to all [LEP]-owned switches and routers:

* Every router and switch deployed in the [LEP] network shall be appropriately configured and meet security requirements for their individual purposes (internal, public facing, demilitarized)
* Access control shall be used to provide separate authentication, authorization, and accounting services for network based access
* Configurations shall prohibit direct public access between public networks (e.g. internet) and any internal [LEP] network
* Configurations shall restrict all traffic, inbound and outbound, from untrusted networks (including guest and external wireless connections) and hosts
* Security shall specifically deny all other traffic except for necessary protocols
* No local user accounts shall be configured on the router and all router passwords shall be kept in a secure encrypted form
* All default ACL passwords shall be changed
* Routers and switches shall have centralized, encrypted access passwords set to the current production router password available from the [Insert Appropriate Role]
* Passwords shall follow strong password mechanisms outlined in the [LEP] Access Control and Password Policy
* Access rules shall be added as business needs arise and be approved by the [Insert Appropriate Role] or designee
* All activities and traffic shall be logged and centrally stored using industry standard or vendor specific collection mechanisms (e.g. SNMP)

### CONFIGURATION

Telnet shall not be used to manage or configure a router. When routers are remotely configured, Secure Shell (SSH) is the preferred management protocol. Routers shall minimally be configured to disallow the following communications and transmissions:

* IP directed broadcasts
* Incoming packets at the router sourced with invalid addresses
* TCP small services
* UDP small services
* Source routing
* Web services running on router

Areas where physical network components reside shall be locked and be marked with the following statement posted in clear view: UNAUTHORIZED ACCESS PROHIBITED. Staff shall have explicit permission to access or configure this device granted only by the [Insert Appropriate Role] or [Insert Additional Appropriate Role].

### MANAGEMENT AND ADMINISTRATION

The [Insert Appropriate Role] or their designee shall ensure the following processes and protocols exist for all [LEP]-owned network devices:

* Formal router testing and hardening procedures are in place
* Change management policy is followed for all configuration changes
* All router and switch passwords are long and complex
* Routers and switches are patched and updated on a documented, regular, and timely schedule
* Procedures exist for installing critical security firmware patches
* Routers and switches are under support contract with appropriate response time guarantees and replacement routers are immediately available should a failure occur

## Audit Controls and Management

On-demand documented procedures and evidence of practice should be in place for this operational policy as part of the [LEP]. Satisfactory examples of evidence and compliance include:

* Router and switch configuration guidelines and documentation
* Evidence that regular and critical patching procedures exist
* Archival and historical traffic and configuration logs exist and can be produced
* Change management processes supporting network hardware changes

## Enforcement

Staff members found in policy violation may be subject to disciplinary action, up to and including termination.

## Distribution

This policy is to be distributed to all [LEP] staff responsible for network hardware configuration, engineering, and support.

## Policy Version History

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Description | Approved By |
| 1.0 | 9/30/2016 | Initial Policy Drafted |  |
|  |  |  |  |
|  |  |  |  |