**Switch Security Policy**

* **Purpose**

This document describes a required minimal security configuration for all switches connecting to a production network or used in a production capacity at or on behalf of ***<Company Name>***

* **Scope**

All switches connected to ***<Company Name>*** production networks are affected. Switches within internal, secured labs are not affected. Switches within DMZ areas fall under the Internet DMZ Equipment Policy.

* **Policy**

Every network switch must meet the following configuration standards:

* No user accounts are configured on the switch.
* The enable password on the switch must be kept in a secure encrypted form. The switch must have the enable password set to the current production switch password from the switch's support organization.
* Use department standardized SNMP community strings.
* The switch must be included in the department enterprise management system with a designated point of contact.
* The switch should have MAC level address locking enabled if the option is available
* The switch should generate an SNMP trap if the link drops and is re-established if the feature is available
* The switch should disable a port or group of ports if new or unregistered MAC addresses appear on a port if the feature is available.
* The switch should be placed in a location where physical access is limited to authorized persons only.
* The switch should have any web server software disabled and if required to maintain the switch the server should be started to configure the switch and then re-disabled. All access controls to administrative functions should be enabled (host/login-password/network)
* Each switch must have the following statement posted in clear view: "UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED. You must have explicit permission to access or configure this device. All activities performed on this device may be logged, and violations of this policy may result in disciplinary action, and may be reported to law enforcement. There is no right to privacy on this device."
* **Enforcement**

Any users found to have violated this policy may be subject to disciplinary action.

**Source:** <https://www.cs.stonybrook.edu/sites/default/files/wwwfiles/drupalfiles/basicpage/Router_Security_Policy.pdf>