NETWORK DEVICE SECURITY POLICY

Purpose: The purpose of this policy is to establish security requirements for network devices connected to the state network and/or administered by the Department of Information Technology (DoIT).

Policy: This security policy applies to all network devices including but not limited to firewalls, routers, and switches.

Access

1. Devices should be placed in limited access, environmentally controlled areas and be placed on a building or stand-alone uninterruptible power supply (UPS) where possible.
2. Only authorized personnel (as designated by the Director of Operations) shall have administrative privileges to install, modify or remove network devices.
3. Administrator accounts shall be unique to each authorized personnel and meet the administrator account policy and maintenance procedure including a required password change after first use and after account reset. Passwords are changed every 90 days.
4. Remote administration shall be secured as specified in the device configurations standards; authentication must use TACACS and all activities shall be logged.
5. Authorized personnel must have a signed Network Administrative Privileges Use Agreement on file at the Human Resources (HR) office; this agreement shall be updated annually.
6. One local account is permitted for emergency access; it must meet the administrator policy and maintenance procedure.
7. The local account must be changed when any administrator ceases to have administrative responsibilities or terminates employment.
8. Physical access ports not needed must be disabled.
9. Authorized personnel must accompany any unauthorized personnel such as vendors providing on-site support and/or hardware maintenance services.

Configuration

1. Devices shall be configured in compliance with configuration standards.
2. IOS upgrades and configuration changes shall have an internal review and be approved via an Infrastructure Change Request (ICR) process prior to implementation.
3. Inbound and outbound traffic not specifically allowed based on provided business requirements shall be denied.
4. Services and interfaces not required shall be disabled.
5. Access lists shall allow only required protocols, ports and IP addresses based on provided business requirements.

Maintenance

1. All configuration changes must be approved via an Infrastructure Change Request (ICR).
2. Configuration backups shall be kept in sync with actively running configurations.
3. Vulnerability scans shall be run routinely on all core devices and network device types.
4. A recovery procedure must be in place and routinely exercised.
5. Logs will be retained based on disk storage capacity and be reviewed as needed.
6. In the event of a suspected compromise, the Security Incident Response Procedure shall be followed.
7. Device configuration standards shall be reviewed annually at a minimum.
8. Modifications to this policy or the device configuration standards must be submitted to the IT Security Group (ITSG) for review and approval by the Security Response Team.

NETWORK DEVICE SECURITY POLICY

Accountability: This policy applies to all network devices administered by the DoIT. It is the responsibility of each DoIT Division Director and Bureau Chief or their designee to enforce this policy.

Employees who do not comply with this policy shall be subject to disciplinary action as outlined in the Administrative Rules of the Division of Personnel.

Description: This policy ensures the uniform and secure policy requirements for router devices.

Reference: Router Configuration Standards
Firewall Configuration Standards
Administrator Account and Password Policy
Administrator Account Maintenance Procedure
Network Administrative Privileges Use Agreement
Login Warning Banner Policy
Security Incident Response Procedure