Network Configuration Policy

The purpose of this policy is to establish standards for the secure configuration of network devices to protect the integrity, confidentiality, and availability of network resources.

This policy applies to all network infrastructure devices, including but not limited to routers, switches, firewalls, and wireless access points.

Password Management

- All network devices must use strong passwords with a minimum length of 12 characters.
- Passwords must include a combination of uppercase letters, lowercase letters, numbers, and special characters.
- Default passwords on all network devices must be changed before deployment.
- Passwords must be changed at least every 90 days.
- Password history must be maintained to prevent reuse of the last 5 passwords.

Access Control

- Telnet must be disabled on all network devices. Only SSH version 2 is permitted for remote access.
- Access to network devices must be restricted to authorized personnel only.
- Role-based access control (RBAC) should be implemented where possible to limit access based on user roles.

Port Security

- Unused ports on switches and routers must be administratively disabled.
- Port security features should be enabled to limit the number of devices that can connect to a single port.
- MAC address filtering should be implemented to prevent unauthorized devices from connecting to the network.

Network Services

- Unnecessary network services and protocols must be disabled to reduce the attack surface.
- SNMP should be configured to use the most secure version available (preferably SNMPv3) and community strings should be changed from the default.
- NTP should be configured to synchronize time from reliable and secure sources.

VLAN Configuration

- All VLANs must be configured with a description in the format `department-lan` or `department-guest`.
- VLAN descriptions must accurately reflect the department or usage to facilitate network management and troubleshooting.
    - Examples:
        - VLAN 10: `marketing-lan`
        - VLAN 15: `marketing-guest`
        - VLAN 20: `hr-lan`
        - VLAN 30: `it-guest`
        - VLAN 40: `finance-guest`