CLOUDAVIZE

Network Security Checklist

✓ Network Perimeter Security :

- □ Are firewalls properly configured and maintained at network boundaries?
- □ Are firewall rules reviewed and updated regularly?
- □ Is intrusion detection/prevention system (IDS/IPS) implemented and monitored?
- □ Is demilitarized zone (DMZ) implemented for public-facing servers?
- □ Are web application firewalls (WAFs) used to protect web applications?

✓ Internal Network Security :

- □ Is network segmentation implemented to isolate critical systems and data?
- □ Are VLANs used to separate network traffic?
- □ Are access control lists (ACLs) used to restrict network traffic?
- □ Is network access control (NAC) implemented to control device access to the network?
- □ Is internal network traffic monitored for suspicious activity?

✓ Wireless Network Security :

- □ Is wireless network security properly configured (e.g., WPA3 encryption)?
- □ Is wireless access point placement optimized for security and coverage?
- □ Is rogue access point detection implemented?
- □ Is guest wireless network separated from the internal network?

✓ Remote Access Security :

- □ Is VPN access used for secure remote access to the network?
- □ Is multi-factor authentication (MFA) required for VPN access?
- □ Are remote access policies and procedures documented and enforced?
- □ Is remote access activity logged and monitored?

✓ Network Device Security :

- □ Are network devices (routers, switches, firewalls) securely configured?
- □ Are default passwords changed on network devices?
- □ Are network device firmware and software updated regularly?
- □ Is remote management access to network devices secured and restricted?
- □ Are unused network ports disabled?

✓ Network Monitoring and Logging :

- □ Is network traffic monitored for security events and anomalies?
- □ Are network logs collected and analyzed for security incidents?
- □ Is network performance monitored for availability and capacity?
- □ Is network vulnerability scanning performed regularly?

✓ DNS and DHCP Security :

- □ Are DNS servers secured and protected from attacks?
- □ Is DNSSEC (Domain Name System Security Extensions) implemented?
- □ Is DHCP snooping used to prevent rogue DHCP servers?

✓ Network Documentation and Management :

- □ Is network documentation up-to-date and accurate?
- □ Is network configuration management implemented?
- □ Are network security policies and procedures documented and reviewed regularly?

You can find this checklist at

https://www.cloudavize.com/network-security-checklist/