CLOUDAVIZE

Endpoint Security Audit Checklist

✓ Endpoint Security Policies and Management :

- □ Are endpoint security policies documented and enforced?
- □ Is there a centralized endpoint management system in place?
- □ Are endpoint security configurations standardized and managed?
- □ Is endpoint compliance monitored and enforced?

✓ Anti-Malware and Threat Protection :

- □ Is anti-malware software deployed and updated on all endpoints?
- □ Is real-time scanning enabled for anti-malware software?
- □ Are anti-malware definitions updated regularly?
- □ Is endpoint detection and response (EDR) solution implemented?
- □ Is threat intelligence integrated into endpoint security?

✓ Operating System and Application Security :

- □ Are operating systems patched regularly with security updates?
- □ Are applications patched regularly with security updates?
- □ Is unnecessary software removed from endpoints?
- □ Is application whitelisting or blacklisting implemented?
- □ Are default accounts disabled or secured on endpoints?

✓ Data Protection on Endpoints :

- □ Is full disk encryption enabled on laptops and portable devices?
- □ Are data loss prevention (DLP) measures implemented on endpoints?
- □ Are removable media (USB drives) controlled and restricted?
- □ Are data backup and recovery procedures in place for endpoints?

✓ Access Control and Authentication :

- □ Are strong password policies enforced on endpoints?
- □ Is multi-factor authentication (MFA) implemented for endpoint access where appropriate?
- □ Are local administrator rights restricted on endpoints?
- □ Is screen lock enabled with appropriate timeout settings?

Endpoint Network Security :

- □ Is personal firewall enabled on endpoints?
- □ Is network access control (NAC) used to control endpoint access to the network?
- □ Is VPN used for secure remote access from endpoints?

Mobile Device Security (if applicable) :

- □ Are mobile device management (MDM) solutions implemented?
- □ Are mobile device security policies enforced (passcodes, encryption, remote wipe)?
- □ Are mobile apps vetted for security before deployment?
- □ Is mobile device data secured and backed up?

Endpoint Security Monitoring and Incident Response :

- □ Are endpoint security logs monitored for security events?
- □ Is there an incident response plan for endpoint security incidents?
- □ Are security alerts and incidents handled effectively on endpoints?
- □ Are endpoint security vulnerabilities and incidents tracked and remediated?

You can find this checklist at

https://www.cloudavize.com/endpoint-security-audit-checklist