| **Sr. No.** | **Audit Questionnaire** | **Company A (Yes/No)** | **Company B (Yes/No)** | **Remarks** |
| --- | --- | --- | --- | --- |
| **Step 1 – Define the Scope of the Audit** |  |  |  |  |
| 1 | Security cameras installed to monitor the data center? | Yes | No | A: CCTV with 30-day retention, B: Not installed |
| 2 | Are devices, OS, and access layers clearly listed for audit? | Yes | Yes | Both maintain asset documentation |
| 3 | Is there a record of network topology diagrams? | Yes | No | B lacks updated topology diagram |
| **Step 2 – Determine Threats** |  |  |  |  |
| 4 | Is a list of potential cybersecurity threats documented? | Yes | No | A uses threat modeling tools |
| 5 | Do you conduct risk assessments regularly? | Yes | Yes | Annually for A; only post-incident for B |
| 6 | Is there protection against DDoS and malware? | Yes | Partial | B lacks advanced DDoS protection |
| **Step 3 – Review and Edit Internal Policies** |  |  |  |  |
| 7 | Do you have a network security policy? | Yes | Yes | A reviews quarterly; B yearly |
| 8 | Do you have a remote access policy? | Yes | No | B lacks VPN-based remote policy |
| 9 | Do you have a documented data backup policy? | Yes | Yes | Daily incremental backups for A |
| **Step 4 – Ensure Safety of Sensitive Data** |  |  |  |  |
| 10 | Is access to sensitive data role-based? | Yes | Yes | Both follow RBAC principle |
| 11 | Is sensitive data encrypted at rest and in transit? | Yes | No | B lacks TLS encryption in some APIs |
| 12 | Is sensitive data stored separately from general data? | Yes | Yes | Segregated database servers in both |
| **Step 5 – Inspect the Servers** |  |  |  |  |
| 13 | Are server configurations reviewed regularly? | Yes | No | B has outdated configuration records |
| 14 | Are DNS/WINS and static IP settings properly configured? | Yes | Yes | Verified in both |
| 15 | Are all servers updated with latest patches? | Yes | Partial | B delayed updates by 2 months |
| **Step 6 – Examine Training Logs and Use Log Monitoring** |  |  |  |  |
| 16 | Are staff trained regularly on cybersecurity practices? | Yes | Yes | A: quarterly; B: yearly |
| 17 | Are logs monitored automatically for suspicious activity? | Yes | No | B relies on manual checks |
| 18 | Are inactive devices removed from the network promptly? | Yes | No | B lacks de-provisioning protocol |
| **Step 7 – Safe Internet Access** |  |  |  |  |
| 19 | Are firewalls and malware scanners in place? | Yes | Yes | Both use enterprise-grade firewalls |
| 20 | Is internet traffic encrypted and filtered? | Yes | Partial | B lacks HTTPS enforcement |
| 21 | Are bandwidth and port restrictions applied? | Yes | Yes | Optimized for internal networks |
| **Step 8 – Penetration Testing** |  |  |  |  |
| 22 | Is penetration testing performed regularly? | Yes | No | B only performs internal vulnerability scans |
| 23 | Are vulnerabilities tracked and remediated? | Yes | Partial | B delays patch closure |
| 24 | Are unauthorized access points identified and removed? | Yes | Yes | Both follow MAC filtering |
| **Step 9 – Share the Network Security Audit with the Team** |  |  |  |  |
| 25 | Are audit findings shared with the IT/security team? | Yes | Yes | A uses internal dashboard |
| 26 | Is employee feedback collected post-audit? | Yes | No | B does not conduct audit meetings |
| 27 | Are improvement plans created based on audit results? | Yes | Yes | Both document corrective actions |
| **Step 10 – Regular Network Security Audits** |  |  |  |  |
| 28 | Is audit frequency defined (once/twice per year)? | Yes | No | B has no fixed audit schedule |
| 29 | Is there an audit report repository maintained? | Yes | Yes | Maintained in internal portal |
| 30 | Are audits used to improve security policies? | Yes | Yes | Periodic updates in both firms |