# Security risk assessment report

|  |
| --- |
| **Part 1: Select up to three hardening tools and methods to implement** |
| **Three hardening tools and methods should be implemented:**   1. **Firewall maintenance:** The company have the ability to guard it self by its firewall but it needs first to get maintain and updated in response to an event that allows abnormal network traffic into the network. This measure can be used to protect against various DDoS attacks. 2. **Password policies:** Most of the vulnerabilities gained by human errors and mistakes so the company have to put a restrictions and password policies to guide the employees to make a strong password and reduce it from get it shared with the coworkers. 3. **Multifactor authentication (MFA):** One of the most good practices and methods used today it make shore that the correct person with the correct authority is the only one having the right to access by checking who is he by something he know, something he is and something he have. |
|

|  |
| --- |
| **Part 2: Explain your recommendations** |
| * **Harden systems and accounts:** Remove default passwords and enforce strong passwords plus multi-factor authentication for all admin accounts. Keep servers and web applications patched, run endpoint protection (AV/EDR), and enable perimeter protections such as a web application firewall (WAF) and DNS filtering to block known-malicious domains. * **Verify controls are active:** After applying controls, perform quick audits and tests — check listening ports, confirm firewall/ACL rules, run a vulnerability scan, and test MFA and account lockouts. Keep a simple checklist with dates and responsible persons so you can prove the fixes were applied. * **Train and empower staff:** Give short, practical training sessions that show why default/weak passwords are dangerous, how to spot phishing, and the correct way to handle and report credentials or suspicious links. Provide one-page cheat-sheets and an easy reporting channel so employees act quickly and correctly. * **Maintain and repeat:** Schedule regular checks (patching, audits, and tabletop drills) and refresh training every few months. Security is ongoing — verify, teach, and re-check on a planned cadence. |