# Network Hardening: Security risk assessment report

|  |
| --- |
| **Part 1: Select up to three hardening tools and methods to implement** |
| 1. Firewall maintenance 2. Password policies 3. Multifactor authentication |
|

|  |
| --- |
| **Part 2: Explain your recommendations** |
| Firewall maintenance is essential because the organization currently lacks rules to filter network traffic. Implementing proper firewall rules helps defend against Denial of Service (DoS) attacks. Regular maintenance ensures these rules stay up to date with the latest network traffic anomalies and can be paired with restricting access to only necessary ports.  Password policies are also critical, as employees are sharing passwords, and the admin password for the database is still set to its default. Establishing password requirements with sufficient length, complexity, and incorporating hashing and salting will significantly lower the risk of successful brute force attacks.  In addition, multifactor authentication (MFA) should be mandatory, especially in light of the absence of strong password policies. Enforcing MFA adds an extra layer of protection against brute force attacks and helps ensure confidentiality by limiting access to sensitive information to only those employees who need it. Once implemented, MFA will require minimal upkeep, focusing primarily on activation, deactivation, and device management. |