# 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:** Regular firewall maintenance is essential because the organization currently lacks proper rules to filter network traffic. Implementing well-defined firewall rules helps safeguard against Denial of Service (DoS) attacks. This process should be performed consistently to keep up with emerging threats and ensure only necessary ports remain open, enhancing overall network security.  **Password Policies:** Establishing strong password policies is crucial, as employees currently share passwords, and the database’s admin password still uses the default setting. Enforcing guidelines that require longer passwords with varied characters, along with incorporating hashing and salting techniques, can significantly reduce the risk of successful brute force attacks.  **Multifactor Authentication (MFA):** Requiring multifactor authentication is a necessary step, especially given the absence of proper password protocols. MFA adds an extra layer of protection against brute force attacks and ensures sensitive information is only accessible to authorized personnel. Implementation is a one-time process, with ongoing maintenance focused on managing device activation and deactivation. |