# Security risk assessment report

| **Part 1: Select up to three hardening tools and methods to implement** |
| --- |
| The three hardening tools and methods recommended for implementation are password policies, firewall maintenance with port filtering, and multifactor authentication (MFA). These tools directly address the vulnerabilities identified during the inspection and strengthen the overall security posture of the organization. Password policies will eliminate the practice of shared credentials and prevent the use of weak or default passwords. Firewall maintenance with port filtering will ensure that unnecessary network traffic is blocked and only essential services are accessible. Multifactor authentication will add an extra layer of protection beyond passwords, making it more difficult for attackers to gain access even if credentials are compromised. |

| **Part 2: Explain your recommendations** |
| --- |
| Password policies are essential because employees currently share passwords, and the database admin account still uses its default password. Enforcing strong password practices, including unique credentials for each employee and secure storage methods, will reduce the risk of brute force and credential-stuffing attacks. Firewall maintenance with port filtering is equally critical because the current lack of firewall rules leaves the network open to malicious inbound and outbound traffic. By creating and regularly updating firewall policies, the organization can block unnecessary traffic, close unused ports, and reduce the risk of unauthorized access or data exfiltration. Finally, implementing multifactor authentication will address the lack of identity verification controls. MFA requires users to provide two or more forms of authentication, such as a password and a one-time code, which significantly increases account security and prevents unauthorized access even if a password is stolen. Together, these methods provide a strong foundation for preventing future breaches and protecting sensitive customer data. |