# Security risk assessment report

|  |
| --- |
| **Part 1: Select up to three hardening tools and methods to implement** |
| 1. **Enforce Strong Password Policies and Use a Password Manager:** Implementing a strong password policy that includes the use of unique and complex passwords is crucial. This should be coupled with the use of a password manager to generate, store, and manage passwords securely for all employees.  2. **Change Default Credentials and Regularly Update Passwords:** Immediately change all default credentials, especially for high-privilege accounts like the admin password for the database. Set up a regular schedule for updating passwords to ensure ongoing security.  3. **Implement Multifactor Authentication (MFA):** Adding MFA provides an additional layer of security beyond just passwords. MFA requires users to provide two or more verification factors to gain access to a resource, such as a one-time code sent to their phone or biometric verification. |
|

|  |
| --- |
| **Part 2: Explain your recommendations** |
| 1.**Enforce Strong Password Policies and Use a Password Manager:**  Create a policy that mandates the use of strong, unique passwords with a minimum length of 12 characters, including a mix of letters, numbers, and special characters. Deploy a password manager across the organization and provide training on its use to all employees.  2. **Change Default Credentials and Regularly Update Passwords:**  Implementation: Immediately change the admin password for all systems, particularly databases and network devices. Develop a policy for regular password changes and ensure that all passwords are updated every 60–90 days. Use unique, strong passwords for all administrative accounts and avoid reuse across systems.  3. **Implement Multifactor Authentication (MFA):**  Implementation: Deploy MFA across all critical systems and user accounts, including email, internal tools, and databases. Choose an MFA method that is user-friendly and secure, such as a mobile app authenticator or biometric verification. Provide training to all employees on how to use MFA and explain the importance of this security measure.  By implementing these three security hardening tools and methods, the organization can address the identified vulnerabilities effectively. These actions will significantly strengthen the network's security posture, reduce the risk of future breaches, and protect sensitive customer information. |