# Security risk assessment report

| **Part 1: Select up to three hardening tools and methods to implement** | |
| --- | --- |
| Password Manager: This tool will help address the vulnerability of employees sharing passwords by securely storing and generating unique complex passwords for each user.  Database Password Reset: Changing the admin password for the database from the default setting will enhance security and prevent unauthorized access.  Firewall Rule Configuration: Implementing proper rules in the organization's firewalls to filter incoming and outgoing traffic will help restrict access to authorized sources and reduce the risk of unauthorized network access. | |
|

| **Part 2: Explain your recommendations** |
| --- |
| Password Manager: The recommended use of a password manager is effective because it promotes the use of strong, unique passwords for each user. By eliminating password sharing and encouraging complex passwords, it significantly reduces the risk of unauthorized access to user accounts. Password managers also provide an additional layer of security through encryption and secure password storage. This practice should be implemented immediately and consistently for all employees.  Database Password Reset: Changing the admin password from the default setting is essential for securing the organization's database. Default passwords are often widely known and can be easily exploited by attackers. By setting a strong, unique password, the organization significantly mitigates the risk of unauthorized access to the database. This should be a one-time action and followed by a policy of regular password updates to ensure continued security.  Firewall Rule Configuration: Configuring firewall rules to filter traffic is an effective method for securing the network. By specifying which types of traffic are allowed and blocking all others, the organization can minimize the attack surface and prevent unauthorized access. Regular review and updates to firewall rules are recommended to adapt to changing threats and network requirements. This practice should be performed periodically, such as on a monthly or quarterly basis, to ensure ongoing protection. |