# Security risk assessment report

|  |
| --- |
| **Part 1: Select up to three hardening tools and methods to implement** |
| After carefully analyzing the recent data breach incident and the vulnerabilities present in the organization’s network, we recommend implementing the following hardening tools and methods:   1. **Password Management System:** Implementing a robust password management system will help mitigate the risk associated with employees sharing passwords. This system should enforce strong password policies, including requirements for length, complexity, and regular password rotation. Additionally, it should facilitate the secure storage of passwords and enable employees to access accounts without needing to share passwords. 2. **Database Password Policy Enforcement:** To address the vulnerability of having the admin password for the database set to the default, we propose implementing a password policy enforcement mechanism. This system should prevent users from setting weak or default passwords and enforce password complexity requirements. Regular audits should also be conducted to ensure compliance with the password policy. 3. **Firewall Rule Configuration:** To enhance the security of the network, it is imperative to configure the firewalls with stringent rules to filter incoming and outgoing traffic. This involves setting up access control lists (ACLs) and defining rules based on the principle of least privilege. By allowing only necessary traffic and blocking unauthorized or potentially malicious connections, the risk of unauthorized access and data exfiltration can be significantly reduced. |
|

|  |
| --- |
| **Part 2: Explain your recommendations** |
| 1. **Password Management System:** The implementation of a password management system addresses the vulnerability of employees sharing passwords by providing a centralized platform for securely managing and accessing passwords. By enforcing strong password policies and eliminating the need for password sharing, this tool enhances the overall security posture of the organization. Additionally, it simplifies password management for employees, reducing the likelihood of weak or reused passwords. 2. **Database Password Policy Enforcement:** By enforcing a strict password policy for database access, the organization can mitigate the risk of unauthorized access resulting from default or weak passwords. Regular audits ensure that passwords adhere to the established policy, reducing the likelihood of successful brute-force attacks or unauthorized database access. This measure enhances the security of sensitive data stored within the database, safeguarding it against potential breaches. 3. **Firewall Rule Configuration:** Configuring the firewalls with proper rules to filter traffic enhances the organization’s network security by controlling the flow of data both into and out of the network. By implementing access control measures based on the principle of least privilege, the organization can limit exposure to potential threats and prevent unauthorized access to network resources. This proactive approach to network security helps mitigate the risk of data breaches and other cyberattacks by effectively controlling network traffic.   In conclusion, the implementation of these hardening tools and methods will significantly strengthen the organization’s network security posture, reducing the likelihood of future data breaches or other attacks. By addressing the identified vulnerabilities and proactively mitigating associated risks, the organization can better protect its assets and uphold the confidentiality, integrity, and availability of its systems and data. |