# Security risk assessment report

| **Part 1: Select up to three hardening tools and methods to implement** | |
| --- | --- |
| To bolster network security, three essential hardening methods should be implemented. Firstly, enforcing stringent password policies and conducting regular cybersecurity training for employees can prevent password sharing and promote stronger password practices, reducing the risk of unauthorized access. Secondly, enhancing database security by changing the default admin password, implementing role-based access control, and maintaining vigilant access logs can safeguard sensitive data from potential breaches. Lastly, configuring firewalls with rigorous traffic filtering rules and considering the deployment of network intrusion detection/prevention systems (NIDS/NIPS) for real-time monitoring can fortify the network against unauthorized or malicious activities. | |
|

| **Part 2: Explain your recommendations** |
| --- |
| The recommended hardening measures aim to significantly improve network security. Strengthening password policies and conducting training will mitigate the vulnerability associated with password sharing, instilling a security-conscious culture among employees. Altering the default admin password, instituting role-based access controls, and closely monitoring access logs will collectively bolster database security, minimizing the likelihood of unauthorized data access or tampering. The suggested firewall configuration, featuring stringent traffic filtering and potential NIDS/NIPS deployment, serves as a robust defense mechanism against unauthorized network access and suspicious activities, providing a comprehensive and proactive approach to safeguarding the network against future breaches or attacks. |