# Security risk assessment report

| **Part 1: Select up to three hardening tools and methods to implement** | |
| --- | --- |
| **Password Policies**  The organization should adopt password policies recommended by the National Institute of Standards and Technology (NIST) to prevent easy password guessing by attackers. The latest NIST guidelines emphasize salting and hashing passwords over overly complex requirements or frequent password changes. Implementing these password policies consistently can help prevent brute force attacks and maintain robust security.  **MFA - Multi Factor Authentication**  Implementing Multi-Factor Authentication is highly recommended for network security and preventing unauthorized access. MFA requires users to verify their identity using two or more methods, such as a password and a fingerprint, before they can access the system or network. This way, even if an attacker has the user's password, they still can't access the network. Once implemented, MFA needs to be maintained to ensure ongoing security.  **Firewall Maintenance**  Firewalls are the initial barrier protecting networks by blocking unauthorized traffic. Regular maintenance involves checking and updating security settings to stay ahead of potential threats. Firewall rules can be adjusted in response to unusual network activity. Additionally, firewalls should have rules in place to filter incoming and outgoing traffic, which is currently a weak spot in the organization. Implementing port filtering can help by blocking or allowing specific port numbers and limiting unwanted communication. | |
|

| **Part 2: Explain your recommendations** |
| --- |
| MFA is a security measure that requires users to verify their identity through two or more methods before accessing a system or network. It can prevent brute force attacks and similar security incidents. I recommended MFA in this case to address the issue of employees sharing passwords. By requiring multiple authentication methods, it significantly hinders an attacker's ability to access the network, even if they have a password. MFA can be implemented initially and maintained thereafter.  Firewall maintenance involves regularly checking and updating security settings to ensure the network's defenses remain effective against evolving threats. This includes reviewing and modifying firewall rules to block unauthorized access while allowing legitimate traffic. Regularly updating these configurations can help prevent security breaches and maintain optimal network performance. In addition, implementing port filtering can restrict or permit specific port numbers, further securing the network by controlling the flow of data. |