# Security risk assessment report

| **Part 1: Select up to three hardening tools and methods to implement** | |
| --- | --- |
| Considering the vulnerabilities found in the network and policies surrounding security, there are some recommendations that will help improve the security posture of the organization. The three recommendations are as follows:   1. Create a strong password policy that employees must recognize and follow. 2. Filter ports in your firewall to limit unnecessary connections. 3. Establish a multifactor authentication (MFA) policy for employees to recognize and follow. | |
|

| **Part 2: Explain your recommendations** |
| --- |
| Following the recommendations above will increase security posture and prevent future incidents. Here are the explanations behind the three recommendations made for the organization’s network and policies.   1. The current standard for passwords indicates that employees share passwords with each other and the admin password was left unchanged from the default setting. Passwords for employees are meant to be private and only known to administrators and the associated employee. This will limit the potential for a password to be leaked to a possible threat actor, sometimes being former employees. Similarly, the default password for the admin of the database is meant to allow for access temporarily and be changed later. The default password is not secure and vulnerable to brute force attacks from threat actors. 2. The firewall’s current state does not filter the traffic that ports receive on the organization’s network. This leaves the attack surface of the network quite wide. The ports that are not being used in everyday work or communication should be blocked through the firewall so that threat actors can not use protocols to plant malware or alter the network in any way. 3. Using MFA is the final security hardening tool that should be implemented in this incident response. MFA ensures that in the event of a password leak or brute force attack from a threat actor, the network is still secure. This adds to the organization's depth of defense and acts as another barrier for malicious actors to cross before any damage can be done. |