# Security risk assessment report

|  |
| --- |
| **Part 1: Select up to three hardening tools and methods to implement** |
| To rectify the security vulnerabilities found within the organization (sharing passwords; using a default admin password; no firewall rules to filter incoming/outgoing network traffic; no MFA used), I suggest that the organization implement firewall maintenance, multifactor authentication, and setting and enforcing strong password policies. |
|

|  |
| --- |
| **Part 2: Explain your recommendations** |
| To address the issue of not having firewall rules in place, I suggested that we implement firewall maintenance to monitor network traffic and investigate suspicious activity earlier to prevent attacks and large-scale data breaches. This will help to secure the network and keep out unauthorized users/programs from accessing sensitive information.  Multifactor authentication will help to provide better security measures for the organization, as employees will have to verify their identity in two or more ways, decreasing the risk that brute force attacks or other security events present. MFA also makes it much more difficult for users to share passwords. Identifying and verifying credentials is imperative for employees with admin privileges. MFA can be set up once, and then maintained as needed.  Setting and enforcing strong password policies will make it more challenging for malicious actors to obtain employee credentials and access the network. NIST recommends using methods to salt and hash passwords rather than requiring overly complex passwords or enforcing frequent changes to passwords. The new rules in the password policy will need to be enforced regularly within the organization to help increaser user security. |