# Security risk assessment report

| **Part 1: Select up to three hardening tools and methods to implement** |
| --- |
| The following are three hardening tools an organization can choose to implement to address known vulnerabilities:<br><br>1. Password policies with stronger requirements.<br>2. Maintain and update firewalls regularly.<br>3. Implement MFA for all users.<br><br>Password requirements can include a certain length, addition of numbers, addition of upper and lower case letters, and the addition of symbols (@#$%&*). Also the discouragement of sharing passwords amongst the organization's employees. Also, the addition of rules regarding unsuccessful login attempts, locking the user out.<br><br>Firewall maintenance/management to check for incoming and outgoing traffic. The addition of port filtering rules to allow/disallow traffic through certain ports, along with updating security configurations.<br><br>MFA requires additional authentication and verification of credentials to access sensitive information. This extra layer of security can be easy to implement and can prevent a multitude of malicious actions. |

| **Part 2: Explain your recommendations** |
| --- |
| Implementing and enforcing a stricter password policy with stricter requirements will mitigate the potential for malicious actors to gain access to the network. Locking a user out of their account after unsuccessful login attempts can prevent brute force attacks. Increasing the complexity of passwords can prevent dictionary attacks.<br><br>Implementing regular firewall maintenance will mitigate risks associated with flooding attacks such as DoS or DDoS attacks. Updating security configurations can help to stay ahead of known/upcoming vulnerabilities. |

Implementing MFA is an extra layer of security that can be easy to implement and can prevent a multitude of malicious actions. It reduces the potential for malicious actors to conduct a brute force or dictionary attack. This will also mitigate the risk associated with employees sharing passwords. The shared password alone will not grant access if MFA is implemented.