# Security risk assessment report

| **Part 1: Select up to three hardening tools and methods to implement** | |
| --- | --- |
| The organization should implement the following methods to reduce risk of another security event.   1. Stronger and more stringent password policies/guidelines for employees. 2. Use of Multi-Factor Authentication (MFA) to verify a user's login credentials. 3. Properly setup and maintain a firewall and set rules to detect malicious traffic. | |
|

| **Part 2: Explain your recommendations** |
| --- |
| First employee’s should be educated on the risks of weak passwords and of password sharing. More strict guidelines should be introduced for acceptable passwords including the overall length and use of special characters.  Using Multi-Factor Authentication (MFA) will help reduce the risk of malicious attacks on the network and threats gaining access who should not. Using fingerprints, pins, or email to verify login credentials will strengthen the overall security of the network.  The firewall should be properly set with rules to block unwanted and malicious traffic from the network. This firewall should also be updated regularly for new threats and after any security events and maintained often. |