# Security risk assessment report

| **Part 1: Select up to three hardening tools and methods to implement** | |
| --- | --- |
| 1. Multifactor Authentication 2. Password Policies 3. Firewall Maintenance | |
|

| **Part 2: Explain your recommendations** |
| --- |
| The major vulnerabilities the organization has currently is default passwords and password sharing, and an unconfigured firewall. Password policies makes it so that default passwords will not be used and further that passwords that are used will be difficult to guess or brute force for a threat actor. Multifactor Authentication adds at least a second requirement to logging in that is known or only useable by the individual who owns the account, this will make password or account sharing difficult if not impossible and prevent threat actors from being able to social engineer their way into an account used by a group of individuals. Finally firewall maintenance will ensure many kinds of attacks will be stymied, most importantly it can be useful as a tool that can be updated during an attack to slow down attackers or after an attack to rebuff any repeated attempts. Firewall maintenance is most useful against DoS attacks which can bring down networks and halt business operations. |