# Security risk assessment report

|  |
| --- |
| **Part 1: Select up to three hardening tools and methods to implement** |
| 1. Multi-factor Authentication 2. Strong Password Implementation and Frequent Password changes required 3. Firewall for incoming and outgoing traffic |
|

|  |
| --- |
| **Part 2: Explain your recommendations** |
| 1. To prevent users from sharing passwords, and unauthorized logins, MFA is a must 2. Default passwords are vulnerable from breach attacks. Strong password is a must and frequent password changes, at least 2 months can be implemented to prevent any brute force attacks. 3. Since the company has no firewall, I recommend a firewall to filter the incoming and outgoing network traffic. With this, you can monitor malicious traffic, using SIEM tools, you can investigate the source it, and implement countermeasures faster. You can filter your traffic to allow only certain types of protocol, that is need to your network. |