# Security risk assessment report

| **Part 1: Select up to three hardening tools and methods to implement** | |
| --- | --- |
| 1. **Password Policies** - The National Institute of Standards and Technology's (NIST) latest recommendations for password policies focuses on using methods to salt and hash passwords, rather than requiring overly complex passwords or enforcing frequent changes to passwords. 2. **Firewall Maintenance**- Firewall maintenance entails checking and updating security configurations regularly to stay ahead of potential threats. 3. **Multi Factor Authentication (MFA)**- A security measure which requires a user to verify their identity in two or more ways to access a system or network. MFA options include a password, pin number, badge, one-time password (OTP) sent to a cell phone, fingerprint, and more. | |
|

| **Part 2: Explain your recommendations** |
| --- |
| 1. Employees of the organization share passwords, which is an unsecure practice in cybersecurity. Implementing NIST’s latest recommendations for password policies with the access privileges implementation will ensure only authorized personnel have the access to certain information. Additionally, changing passwords on a regular basis makes it secure against Brute force attacking. 2. Blocking all the unused ports and allowing only certain types of packets to pass through can help protect against external threats trying to gain access to the secure parts of the network. 3. Currently, there is no multi factor being implemented inside the organization which makes it vulnerable to Brute force attacks. Multi-factor authentication ensures that the person trying to access the information is authorized and genuine by confirming their identity by either using their bio-metrics or an OTP from their personal device. |