# Security risk assessment report

| **Part 1: Select up to three hardening tools and methods to implement** | |
| --- | --- |
| After the discovery of four (4) major vulnerabilities, these are the recommended tools and methods to be implemented to address the vulnerabilities.   1. Password Policies 2. Firewall maintenance 3. Multifactor authentication(MFA) | |
|

| **Part 2: Explain your recommendations** |
| --- |
| Password policies are recommended because the organization’s employees’ share passwords and the admin password for the database is set to the default password. These policies will help more secure accounts and will prevent attackers from easily guessing user passwords.  Because the current firewall does not have rules in place to filter traffic coming in and out of the network, it is recommended to have Firewall Maintenance. Firewall maintenance entails checking and updating security configurations regularly to stay ahead of potential threats.  The use of MFA will further secure accounts in the organization by having two or more ways to identify the user. MFA will help protect against brute force attacks and similar security events. |