# Security risk assessment report

|  |
| --- |
| **Part 1: Select up to three hardening tools and methods to implement** |
| The tools/methods the organization can use to harden their security are:   1. Setting strong password policies 2. Performing firewall maintenance regularly 3. Implementing MFA (Multifactor authentication)   Setting strong password policies can include setting rules for password length, special characters, numbers. Employees must be informed and discouraged to share their passwords with anyone else. An unsuccessful attempt limitation can be added to prevent possible brute force attacks.  Performing regular maintenance to firewalls and updating its configurations regularly can help the organization stay ahead of potential threats.  MFA requires the user to verify their identity in two or more ways to access a system or network. Methods like pin number, badge, one-time password (OTP) and many others in addition to a password. |
|

|  |
| --- |
| **Part 2: Explain your recommendations** |
| First method that should be implemented is making password policies. Creating passwords according to NIST’s recommendations and not allowing the workers to share an identical password is a crucial point in securing the network. Creating unique passwords for each employee and not allowing them share the passwords reduces the risk of unauthorized users and outside traffic from accessing the internal network. This implementation also applies for the admin having the default password instead of a unique one.  Second method is making firewall maintenance regularly. Network firewalls must be checked regularly to keep them up to date and their configurations must be done to block unwanted and potential threat traffic meanwhile allowing the wanted traffic. After each security event, a new set of firewall rules should be applied. This can protect the servers from DoS and DDoS attacks.  The third tool/method is MFA (Multifactor Authentication). By adding an MFA we can make both employees and customers access to the network much more secure since they will be forced to verify their identity in two or more ways. This is an effective way to prevent brute force attacks and similar security events. |