# Security risk assessment report

| **Part 1: Select up to three hardening tools and methods to implement** | |
| --- | --- |
| After reviewing the vulnerability in our organizations I selected three important hardening tools and methods that should be implemented urgently.   * Set up a Password policy. * Reconfigure the firewall rules and port filtering. * Implement MFA . | |
|

| **Part 2: Explain your recommendations** |
| --- |
| Our organization needs a password policy that don’t tolerate the share of passwords, and that oblige the employees to changes their passwords every three months and to have a rule of passwords as well (eg : the password should atleast have 8 characters, no consecutive numbers , at least one special character ), and admin passwords should never be set to default. Which will discourage malicious actors from trying to penetrate our network.  We should configure our firewall rules and maintain it regularly because it’s our first line of defense that filters traffic coming in and out of the network, and implements port filtering which can help protect against various attack like DOS or DDOS attacks which can be fatal to an organization if not stoped.  As well as implement MFA which help mitigate the risk of identity theft because in order to connect using MFA even if the malicious actor has the username and password, they’ll be asked to use biometrics (like fingerprints, palmprint) or enter random generated number by the MFA application in order to connect. |