# Security risk assessment report

|  |
| --- |
| **Part 1: Select up to three hardening tools and methods to implement** |
| Password policies  MFA  Firewall maintenance |
|

|  |
| --- |
| **Part 2: Explain your recommendations** |
| Taking a deep look at the scenerio, The organization’s employees' share passwords and The admin password for the database is set to the default.This shows that the best pratices have not been put in place as regards their password policies.The more the characters of a password the harder it is to crack. The password should contain Upper letter, lower letters and special characters and it must not be less than 12 characters. Passwords should also not be related to anyone or anything in the organization to avoid brute attack  Multi -factor authentication should also be put in place . It provides an additional layer of authentication .  There should be frequent firewall maintenenace This can happen regularly. Firewall rules can be updated in response to an event that allows abnormal network traffic into the network. This measure can be used to protect against various DDoS attacks. |