# Security risk assessment report

|  |
| --- |
| **Part 1: Select up to three hardening tools and methods to implement** |
| There are several major vulnerabilities that needs to be addressed after inspecting the organization’s network. It is necessary to implement hardening tools and methods, and these are my 3 suggestions:   1. Password policies. 2. Multi-factor authentication. 3. Port filtering. |
|

|  |
| --- |
| **Part 2: Explain your recommendations** |
| PASSWORD POLICIES  We found that the administrator password for the database is still set to the default. Following the latest recommendations of the National Institute of Standards and Technology (NIST) will help to prevent attackers from guessing the passwords used by the organization.  MULTI-FACTOR AUTHENTICATION  It is currently not used, and we also found that the organization’s employees are sharing passwords to access to system or network. Making this method mandatory will help protect against brute force attacks and similar security events. Options include using badge, one-time password (OTP) sent to a cellphone, fingerprint, etc. It only needs to be set up once, and then maintained.  PORT FILTERING  Currently it doesn’t have rules in place to filter traffic coming in and out of the network. Additionally, a firewall maintenance can happen regularly to stay ahead of potential threats and protect against various DoS attacks. |