# Security risk assessment report

|  |
| --- |
| **Part 1: Select up to three hardening tools and methods to implement** |
| 1. Create and implement a policy for disabling unused ports in firewalls. Include scheduled for firewall configuration review (example annual\biannual)  2. Create and implement a policy for Administrator passwords to include complexity rules, age and role access. Use The National Institute of Standards and Technology's (NIST) latest recommendations for password policy  3. Create and implement a policy for employee accounts and password include complexity rules and age. Use The National Institute of Standards and Technology's (NIST) latest recommendations for password policy  4. Set a schedule to review NIST standards against the password policy developed by the company. |
|

|  |
| --- |
| **Part 2: Explain your recommendations** |
| The areas of hardening the organizations technology assets and data based on the discovery of the four vulnerabilities discovered.   1. The organization’s employees' share passwords. 2. The admin password for the database is set to the default. 3. The firewalls do not have rules in place to filter traffic coming in and out of the network. 4. Multifactor authentication (MFA) is not used.   This is not an exhaustive list of hardening that can be done, but it will secure the areas that where discovered in the data breach review.  1. Disabling the unused ports in firewalls will reduce the footprint of the organization, make it more difficult for threats to attack company assets.  2. Using NIST standards as a guide for password policy within the company improve security for assets and data employees access as part of there job functions. |