# Security risk assessment report

Nela-officer

Date: 06/12/2024.

|  |
| --- |
| **Part 1: Select up to three hardening tools and methods to implement** |
| Considering the major vulnerabilities detected during the recent data breach in the network, we recommend implementing the following measures:   * Review the current password policy to guarantee that covers all the elements needed, such as disallowing previous passwords from being used. Update the policy and reinforce it for all the employees. * Firewall rules must be created and periodically updated, create a calendar maintenance for the firewall to guarantee the review. * Implement MFA * The latest standard of Encryption considers the safety of the customers’ personal information. |
|

|  |
| --- |
| **Part 2: Explain your recommendations** |
| The measures recommend will minimize the risk of the four vulnerabilities detected and protect for the future:   1. The organization’s employees' share passwords therefore a strong password policy widespread to reinforce the best practice to all the employees will reduce the risk. 2. The admin password for the database is set to the default, therefore the disallowing of previous passwords as part of the password policy will be effective. 3. The firewalls do not have rules in place to filter traffic coming in and out of the network. Creation of rules and proper maintenance will reduce significant the risk. 4. Multifactor authentication (MFA) implementation, currently not in place, will guarantee additional check to validate the User’s ID. |