# Security risk assessment report

| **Part 1: Select up to three hardening tools and methods to implement** | |
| --- | --- |
| The recommended methods to implement for avoiding security breaches in the future are:   1. Strict password policies 2. Multifactor Authorization (MFA) 3. Disabling unused ports | |
|

| **Part 2: Explain your recommendations** |
| --- |
| The main security concerns for the organization are:   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.   That is why the aforementioned methods are recommended. A detailed explanation of them follows.  As three of the four security concerns pertain to passwords, the focus should be on implementing measures that harden passwords. First, strict password policies will help in ensuring employees do not share passwords and that passwords are strong, especially the admin password for the database. For this, the NIST (National Institute of Standards and Technology) recommends salting and hashing passwords; that means making passwords unique values that are impossible to decrypt (hashing) and using random characters to hashed passwords like ‘\*’ or ´%’, etc. (salting).  After that, it is imperative to enforce MFA, because it adds more steps to verify a user's identity before granting access to a system. Thus, mitigating the risk of malicious actors accessing the network. This MFA can be Security keys, Safety questions, Captcha or reCaptcha, biometric data, etc.  Finally, the firewall must be configured to filter unwanted network traffic and disable ports that are not used in the company’s daily activities. This makes network traffic more safe and minimizes the attack surface. Thus, limiting the ways that the network can be compromised by a malicious actor. |