# Security risk assessment report

|  |
| --- |
| **Part 1: Select up to three hardening tools and methods to implement** |
| 1. Updating password policies: Every user will be required to change their passwords immediately. These new passwords will require an at least 1 uppercase character, a number and a special character. The new passwords cannot be any default password or previous passwords used. MFA will also be introduced to further harden the security around passwords. 2. Firewalls: Firewalls will be implemented around the network to block incoming traffic from unknown sources 3. Intrusion detection system (IDS): will be introduced to provide alerts to security analysts about potential threats |
|

|  |
| --- |
| **Part 2: Explain your recommendations** |
| Password policies need to be updated to prevent any brute force attacks from happening or at least make it more difficult for malicious actors. Users sharing passwords and admins using default passwords are major vulnerabilities in the networks security. Requiring all users to change their passwords at their next login attempts and also implementing MFA will help alleviate any threats against a brute force attack.  Adding functionality for firewalls to be able to filter unknown sources from entering the network will prevent malicious actors from unknown sources from penetrating the network and gaining access to sensitive data.  Finally, adding an IDS will generate even more alerts against threats if used alongside a SIEM tool allowing security analysts to react to and fight against threats earlier  These hardening tools should be updated often to stay steps ahead of malicious actors. |