# Security risk assessment report

| **Part 1: Select up to three hardening tools and methods to implement** | |
| --- | --- |
| Firewall Maintenance, Password Policies, and MFA.  Password policies can be implemented by mandating that secure passwords must be used and updated regularly, as well as mandating that nobody can share passwords. Firewall Maintenance can be mandated by ensuring that the policies is adhered to. MFA can be implemented by mandating it’s use because it is already in the system but isn’t being put to use. | |
|

| **Part 2: Explain your recommendations** |
| --- |
| Password Policies need to be implemented because users are sharing passwords among each other and the admin password is set to the default which is a high risk. Implementing these policies will help in the case of brute force attacks. Multi factor Authentication needs to be implemented fully and used appropriately in order to authenticate users properly within the system. This also prevents threat actors from gaining access to sensitive accounts and information. And Firewall Maintenance needs to take place because the firewall rules need to be updated to prevent potential threat actors from gaining access to sensitive areas of the system. MFA can be set up once and then maintained, Firewall maintenance needs to be regular and updated in response to an event that allows abnormal network traffic into the network. Passwords need to be updated once a month and the policy only needs to be implemented once and maintained. |