Security risk assessment report

Part 1: Select up to three hardening tools and methods to implement
3 hardening tools the organisation can use to address the vulnerabilities include: ● Multi-Factor Authentication (MFA) ● Password Policies ● Port filtering

Part 2: Explain your recommendations
Multi-factor authentication is needed to help protect against any brute force attacks that could occur on the databases' admin password as it is currently set to the default. This is easy to setup and would only need to be setup once but maintained. Password policies need to be implemented aswell to ensure that the database admin password and employee passwords are kept extremely secure and are not shared between employees in the same organisation. Password policies would only need to be setup once but be maintained. Port filtering is needed to control the network traffic and prevent threat actors from taking advantage of an open network. Port filtering needs to be frequently performed to ensure the security of the network.