Security risk assessment report

Part 1: Select up to three hardening tools and methods to implement
The organization needs to configure a firewall with rules and disable unused ports and enable port filtering. There should be maintenance to ensure the firewall is configured and functioning correctly. There should be NIST standard password policies enforced, and multi-factor authentication should be enforced. There should also be network access privileges implemented since the employees' all share the same password.

Part 2: Explain your recommendations
The organization needs to implement a firewall to filter outgoing and incoming traffic. Any ports that are not necessary should be disabled to lower the attack surface and port filtering should be implemented in order to control network traffic. There should also be password policies implemented that meet the standards of the NIST. This will help prevent password attacks, support least access, and limit the threat of internal activities. Alongside this, multifactor authentication such as a one-time password and a face scan should be implemented to further secure credentials especially the admin login. The admin login needs to be changed immediately to a strong password. Network access privileges should be implemented to prevent unauthorized employees and threat actors from accessing network data. Each of these hardening methods should be regularly maintained and testing to ensure rules and policies do not need to be updated and are secure.