Security risk assessment report

Part 1: Select up to three hardening tools and methods to implement
Employees must not share passwords with each other. Sharing passwords increases the likelihood of a malicious actor gaining access to secure systems more easily. Password policies: more complex password rules need to be implemented for accounts that have access to critical data/assets. Firewalls need to at the very least have port filtering enabled. . MFA is a less expensive method to increase password security.

Part 2: Explain your recommendations
MFA would require a token sent to a user's email or phone in addition to their password. In case of an attack where the threat actor guesses a password correctly, they would be unable to gain access due to MFA. This security would only need to be implemented once. Password policies are vital to enhancing account security and ensuring threat actors cannot easily guess passwords using brute force attacks. Regular updates to passwords would need to be enforced. Port filtering will limit the amount and types of traffic that are allowed into the organization's network by disallowing traffic through unused ports. Unused ports that are open are vulnerable to malicious actors attempting access through these open ports. Firewalls would only need to be implemented a single time. Malicious actors will have a harder time accessing important data if access to ports requires privileged credentials. As added security an IPS, IDS, SIEM tool, or any combination of the three would drastically improve the network's security.