Security risk assessment report

Part 1: Select up to three hardening tools and methods to implement
Password Policies: The organization's employees are currently sharing passwords amongst themselves. This is a very insecure practice and means that if one employee is compromised, there is the potential for further damage. The organization should implement a strong password policy, and make it clear that sharing passwords is prohibited. Passwords should not be shared with anybody, and should also be stored securely. This also related to the company's default admin password, which leaves massive vulnerabilities to disgruntled employees who may be able to access via a brute force attack sensitive information. Port filtering: Currently there are no rules to filter incoming and outgoing traffic. This leaves the company at great risk of an attack. The firewall should have a baseline rule of allowed and disallowed ports, as well as disabling unused ones. Firewalls should also be maintained, checking and updating security configurations regularly so that the organization can stay ahead of threats. MFA: The organization does not use multi-factor authentication. This security measure means users are required to verify at least two means of authentication in order to gain access to something. Without MFA, attackers may have an easier time bypassing security and allowing unauthorized access.

Part 2: Explain your recommendations
There are currently many vulnerabilities within the organization, such as weak password policies and lack of multi-factor authentication. These are massive weak spots in the security of the organization and a strong security policy is needed to address these. The firewall also needs to be configured properly, establishing a baseline for port filtering, as well as disabling unused ports. Overall it seems this case is missing the fundamentals of cybersecurity. Through thorough employee training, and securing the network, the organization can make vast improvements on its defense against threat actors.