Security risk assessment report

Part 1: Select up to three hardening tools and methods to implement
1. Password Policies 2. Firewall Maintenance 3. Multifactor Authentication (MFA)

Part 2: Explain your recommendations
1. Password Policies The issue of employees sharing passwords and the admin password being set to default exposes the network to brute force and unauthorized access attacks. Implementing strong password policies based on NIST's recommendations ensures that all passwords are salted, hashed, and stored securely. It also encourages using longer, more memorable passphrases instead of enforcing complex characters that users tend to forget and thus share or write down. **Implementation Frequency:** This should be enforced organization wide and reviewed quarterly. Employees should be required to follow best practices, and password storage mechanisms should be monitored for compliance. **2. Firewall Maintenance** The absence of inbound and outbound firewall rules creates an open gateway for malicious traffic. By configuring and maintaining firewall rules, the organization can control network traffic more effectively and block unauthorized access attempts. Firewall logs should also be monitored to detect abnormal behavior. **Implementation Frequency:** Firewall configurations should be reviewed at least monthly and updated after any major changes or incidents. Regular audits can help detect outdated or misconfigured rules.

3. Multifactor Authentication (MFA)
MFA is a critical line of defense when login credentials are compromised, as it requires an additional layer of verification beyond just a password. Implementing MFA, especially for admin level access and sensitive internal systems can protect against credential stuffing, phishing, and brute force attacks.
Implementation Frequency: MFA should be set up as a one-time configuration for all users, then enforced and monitored continually.

Summary

By enforcing password policies, maintaining strict firewall configurations, and enabling MFA, the organization can significantly reduce its attack surface. These hardening practices directly address the current vulnerabilities and provide a solid foundation for ongoing network security management. Routine enforcement and monitoring of these methods will ensure that the network remains secure and resilient to evolving threats.