# Security risk assessment report

| **Part 1: Select up to three hardening tools and methods to implement** | |
| --- | --- |
| **Firewall Maintenance**   * **Why**: The organization lacks firewall rules, exposing it to unfiltered traffic that could lead to data breaches or malware infections. * **How**: Implement and regularly update firewall rules to control inbound and outbound traffic. Ensure only authorized services and ports are accessible.   **Password Policies**   * **Why**: Employees are sharing passwords and default credentials are being used. Weak password hygiene greatly increases the risk of credential-based attacks. * **How**: Follow the **NIST (National Institute of Standards and Technology)** guidelines to:   + Require long and complex passwords (minimum 8–12 characters, with upper/lowercase letters, numbers, symbols)   + Prevent reuse of previous passwords   + Set password expiration intervals   + Enforce account lockouts after multiple failed attempts   + Avoid shared passwords entirely   **Multi Factor Authentication (MFA)**   * **Why**: MFA adds a second layer of defense even if passwords are compromised or shared. The current absence of MFA makes accounts easy targets. * **How**: Implement MFA for all users, especially for administrative and sensitive systems, using authenticator apps or biometric options when possible. | |
|

| **Part 2: Explain your recommendations** |
| --- |
| **Recommendation 1: Implement and Maintain Firewall Rules** **Explanation:** Firewalls serve as the first line of defense by controlling traffic entering and exiting the network. Without defined rules, unauthorized or malicious traffic can flow freely, increasing the risk of breaches. By configuring firewall rules to allow only necessary services and blocking everything else, the organization can significantly reduce its attack surface.   * **Effectiveness:** Prevents unauthorized access, malware communication, and external exploitation by filtering traffic based on IP address, port, and protocol. * **Implementation Frequency:** Firewall rules should be reviewed and updated at least monthly, or immediately after any major network or application change. Continuous monitoring should be enabled to detect and respond to anomalies in real time.   **Recommendation 2: Enforce Strong Password Policies**  **Explanation:** Implementing strong password policies is critical to addressing the issue of employees sharing passwords and using default credentials. A well-designed policy ensures passwords are difficult to guess, not reused, and changed regularly. It also helps prevent unauthorized access due to weak or exposed credentials. By adhering to standards such as those set by NIST, the organization strengthens its access controls and reduces the risk of brute force and credential stuffing attacks.   * **Effectiveness**: Prevents unauthorized access and credential misuse. * **Implementation Frequency**: Passwords should be reviewed and changed every 60–90 days. Policy audits should occur at least quarterly.   **Recommendation 3: Implement Multi Factor Authentication (MFA)**  **Explanation:** MFA provides a critical second layer of security. Even if an attacker obtains a valid password, they would still need the second authentication factor (e.g., a code from an authenticator app or biometric confirmation). This makes unauthorized access significantly more difficult and helps safeguard sensitive systems, especially administrative accounts.   * **Effectiveness**: Highly effective against phishing, credential theft, and account takeover. * **Implementation Frequency**: MFA should be enforced continuously and reviewed during regular security audits (e.g., quarterly or bi-annually) to ensure compliance and effectiveness. |