# Security risk assessment report

|  |
| --- |
| **Part 1: Select up to three hardening tools and methods to implement** |
| 1. **Password Policies and Default Password Changes**    * Enforce strong, unique passwords and eliminate the use of default or shared passwords. 2. **Multifactor Authentication (MFA)**    * Require additional verification steps for all administrative and user accounts. 3. **Firewall Maintenance with Port Filtering**    * Implement and regularly update firewall rules to filter incoming and outgoing network traffic, blocking unauthorized access. |
|

|  |
| --- |
| **Part 2: Explain your recommendations** |
| **Password Policies and Default Password Changes** Implementing robust password policies is critical because shared and default passwords create easy entry points for attackers. By enforcing the use of complex, unique passwords and requiring that default credentials be changed immediately, the organization reduces the risk of unauthorized access through brute force or credential stuffing attacks. Regular audits and monitoring ensure that employees adhere to these policies, reducing the vulnerability of compromised credentials.  **Multifactor Authentication (MFA)** MFA adds an extra layer of security by requiring users to provide additional verification (such as a one-time password or biometric confirmation) along with their standard credentials. This measure is highly effective against attacks where passwords may be guessed or shared, as the extra factor is much harder for an attacker to compromise. MFA is generally set up once and maintained, making it a sustainable security improvement for mitigating risks related to unauthorized access.  **Firewall Maintenance with Port Filtering** Given that the current firewall lacks rules to filter traffic, regular firewall maintenance and implementing port filtering are essential. These practices ensure that only authorized traffic passes through, reducing the risk of malicious actors exploiting open or misconfigured ports. Regularly reviewing and updating firewall configurations helps the organization stay ahead of new threats and minimizes the chance of unauthorized network access, thereby preventing potential data breaches.  Together, these measures address the critical vulnerabilities identified and strengthen the overall network security posture, helping to prevent future data breaches and unauthorized access incidents. |