# Security risk assessment report

|  |
| --- |
| **Part 1: Select up to three hardening tools and methods to implement** |
| * **Multi-Factor Authentication (MFA)**: Implement MFA for all administrative and user accounts to prevent unauthorized access. * **Firewall Maintenance and Port Filtering**: Set up regular firewall maintenance and configure port filtering to limit inbound and outbound traffic, allowing only necessary communication. * **Password Policies**: Enforce strong password policies, including the use of password hashing and salting techniques to prevent brute force and password guessing attacks. |
|

|  |
| --- |
| **Part 2: Explain your recommendations** |
| **Multi-Factor Authentication (MFA):**   * Why it’s effective: MFA requires multiple forms of authentication (such as a password and a one-time code) to verify user identity. This drastically reduces the risk of unauthorized access, even if a password is compromised. By implementing MFA, the organization ensures that login attempts from malicious actors are blocked, protecting critical systems. * Frequency of implementation: MFA is set up once for all accounts but should be reviewed and maintained regularly to ensure security settings remain effective and that users are adhering to the policy.   **Firewall Maintenance and Port Filtering:**   * Why it’s effective: Firewalls control incoming and outgoing network traffic based on predetermined security rules. Port filtering restricts unnecessary traffic and helps prevent unauthorized access to the network by blocking malicious traffic. With regular firewall maintenance, the organization can keep up with potential new threats and ensure that abnormal traffic is stopped before causing damage. * Frequency of implementation: Firewall rules should be reviewed monthly or in response to incidents, and port filtering should be updated as needed based on changing security needs.   **Password Policies:**   * Why it’s effective: Strong password policies that enforce password complexity, hashing, and salting make it harder for attackers to guess or brute-force passwords. Additionally, password policies ensure that employees do not use shared or default passwords, reducing the risk of credential-based attacks. * Frequency of implementation: Password policies should be implemented immediately and enforced continuously. Password audits should be performed regularly to ensure compliance. |