# Security risk assessment report

| **Part 1: Select up to three hardening tools and methods to implement** | |
| --- | --- |
| **Part 1: Select up to three hardening tools and methods to implement**  1. **Implement Password Management Policies and Education** 2. **Enforce Multi-Factor Authentication (MFA)** 3. **Configure Firewall Rules and Update Default Credentials** | |
|

| **Part 2: Explain your recommendations** |
| --- |
| **1. Implement Password Management Policies and Education** **Why it's effective:** The practice of employees sharing passwords and using default admin credentials poses a significant security risk. Implementing strict password policies—such as requiring complex, unique passwords and regular password changes—can mitigate this vulnerability. Additionally, educating employees on the dangers of password sharing and the importance of cybersecurity hygiene will foster a culture of security awareness.  **Implementation frequency:**   * Password policies should be enforced continuously. * Employee training sessions should be conducted quarterly to reinforce best practices and address emerging threats.  **2. Enforce Multi-Factor Authentication (MFA)** **Why it's effective:** MFA adds an extra layer of security beyond just passwords, requiring users to verify their identity through a second factor (e.g., a mobile app or SMS code). This significantly reduces the risk of unauthorized access, even if passwords are compromised.  **Implementation frequency:**   * MFA should be enabled immediately and enforced for all users without exception. * Regular audits should be performed to ensure MFA remains active and is not bypassed.  **3. Configure Firewall Rules and Update Default Credentials** **Why it's effective:** Firewalls act as the first line of defense against unauthorized network traffic. Configuring strict inbound and outbound rules will prevent malicious traffic from entering or leaving the network. Additionally, changing default admin passwords for databases and other critical systems eliminates a common attack vector exploited by hackers.  **Implementation frequency:**   * Firewall rules should be reviewed and updated monthly to adapt to new threats. * Default credentials should be changed immediately upon system setup and reviewed periodically (e.g., every 6 months). |