# Security risk assessment report

| **Part 1: Select up to three hardening tools and methods to implement** | |
| --- | --- |
| **Implement strong password policies and enforce unique passwords for all users.**  **Change all default administrator credentials immediately and regularly audit credentials.**  **Enable and enforce multi-factor authentication (MFA) for all users, especially administrators.** | |
|

| **Part 2: Explain your recommendations** |
| --- |
| **Strong password policies and unique passwords:**  Shared passwords pose a high risk, as they eliminate accountability and increase the chances of unauthorized access. By enforcing strong, unique passwords that meet complexity requirements, the organization reduces the effectiveness of brute force and credential stuffing attacks. This policy should be enforced with regular password expiration intervals (e.g., every 90 days) and disallow reuse of previous passwords.  **Remove default admin credentials and audit passwords:**  Default credentials are widely known and often targeted by automated scanning tools used in cyberattacks. Changing them closes this easy entry point. Admin accounts should also be periodically audited to ensure credentials are secure, rotated, and not stored in plain text.  **Enable Multi-Factor Authentication (MFA):**  MFA adds a critical second layer of defense beyond just the username and password. Even if credentials are compromised, the attacker would still need access to the second factor (e.g., a one-time code, device confirmation, or biometric). This significantly reduces the chance of unauthorized access to sensitive data. MFA should be implemented on all systems that handle sensitive information or administrative access. |