# Security risk assessment report

|  |
| --- |
| **Part 1: Select up to three hardening tools and methods to implement** |
| 1. Enforce strong password policy (mix of upper and lowercase letters, numbers, special characters and minimum 8-12 characters long). 2. Implement multi factor authentication (MFA) for all users and admin accounts. 3. Configure and update firewall to filter and monitor traffic. 4. Train employees to not share their personal password with anyone |
|

|  |
| --- |
| **Part 2: Explain your recommendations** |
| * **Strong passwords**: Complex passwords make it harder for attackers to guess or crack credentials through brute force or dictionary attacks. * **Multi-factor authentication (MFA)**: Even if a password is compromised, MFA ensures an attacker cannot log in without an additional verification factor. * **Firewall updates**: Properly configured firewalls block malicious traffic and prevent unauthorized access to the internal network. * **Employee training**: Educating employees helps prevent risky behaviors such as password sharing, reducing insider threats and human error. |