# Security risk assessment report

|  |
| --- |
| **Part 1: Select up to three hardening tools and methods to implement** |
| 1. Enforcing strong password policies. 2. Regular firewall maintenance. 3. Implement MFA. |
|

|  |
| --- |
| **Part 2: Explain your recommendations** |
| Strong password policies will secure against brute force attacks. Passwords must be minimum of 12 characters including at least 1 special character, 1 digit and one capital letter.  Firewall configuration must be checked regularly to ensure no suspicious traffic goes in or out of the network. The default setting should deny all access to the network.  MFA prevents brute force attacks and in the event a password is compromised the second factor can ensure account is secure. |