# Security risk assessment report

|  |
| --- |
| **Part 1: Select up to three hardening tools and methods to implement** |
| 1. Implement strong password policies.    1. Use encryption protocols.    2. Require at least one character, one number and at least 8 length.    3. Enforce requirement for passwords to be unique.    4. Add a rule that passwords have to be changed every 3 months.    5. Add a disclaimer to discourage password sharing (i.e., require password to be unique.    6. Limit unsuccessful attempts to 3. 2. Implement multi-factor authentication (MFA). This requires users to use more than one way to verify their credentials before accessing an application. Examples of MFA methods include ID cards, pin numbers, and fingerprint scans. 3. Performing firewall maintenance regularly. |
|

|  |
| --- |
| **Part 2: Explain your recommendations** |
| 1. Enforcing strong password policies discourages brute force attacks and makes the passwords harder to guess. This only needs to be applied once as a security measure. 2. Requiring users to verify their identity via MFA adds another layer of security and also makes password sharing less useful. This only needs to be applied once as a security measure. 3. Firewall maintenance and updating firewall configuration will allow users to triage traffic coming into the network. This way abnormal network activity can be identified and prevented—this measure also helps to protect against DoS and DDoS attacks. This needs to be implemented regularly. |