# Security risk assessment report

| **Part 1: Select up to three hardening tools and methods to implement** | |
| --- | --- |
| 1. Password policies must be implemented according to the NIST’s proposed standards and password sharing should be discouraged. 2. Regular firewall maintenance should be done in order to stay ahead and avoid potential threats. 3. Multifactor authentication (MFA) | |
|

| **Part 2: Explain your recommendations** |
| --- |
| 1. A. Password policies are used to prevent attackers from easily guessing user passwords, either manually or by using a script to attempt thousands of stolen passwords (commonly called a brute force attack).   B. Implemented according to the changing standards.   1. A. Firewall maintenance entails checking and updating security configurations regularly to stay ahead of potential threats.   B. Happens regularly.   1. A. Reduces the risk of unauthorized users and outside traffic from accessing the internal network. This can be implemented once, or revisited depending on the likelihood of social engineering or brute force attacks. |