# Security risk assessment report

| **Part 1: Select up to three hardening tools and methods to implement** | |
| --- | --- |
| 1. Set up stronger organizational password policies. Deny use of default passwords. 2. Set up firewall rules 3. Enable MFA | |
|

| **Part 2: Explain your recommendations** |
| --- |
| The social media organisation lacks stricter password policies to restrict password sharing and boost account security. Additionally, updating the password policies will restrict the admin account from using a default password which is likely to be a subject of brute force attacks. Setting up firewall rules will provide added protection to the security zones in the organisation by filtering traffic ingress and egress traffic. It also provides port filtering functions which will allow specific port numbers while blocking the rest.  By using MultiFactorAuthentication, malicious actors are more likely to be kept out of the company network as users have to authenticate twice using a username and password as well as a one-time token. MFA also may reduce the likelihood of password sharing because individuals would still need to possess an additional authentication device. |