# Security risk assessment report

|  |
| --- |
| **Part 1: Select up to three hardening tools and methods to implement** |
| Three hardening tools and methods that the company needs to implement to ensure the safety of its data and assets area:   * Multifactor authentication (MFA) * Password policies * Firewall maintenance |
|

|  |
| --- |
| **Part 2: Explain your recommendations** |
| Multifactor authentication (MFA): A security measure which requires a user to verify their identity in two or more ways to access a system or network. MFA options include a password, pin number, badge, one-time password (OTP) sent to a cell phone, fingerprint, and more. Can help protect against brute force attacks and similar security events. MFA can be implemented at any time and is mostly a technique that is set up once then maintained.  Password Policies: The National Institute of Standards and Technology's (NIST) latest recommendations for password policies focuses on using methods to salt and hash passwords, rather than requiring overly complex passwords or enforcing frequent changes to passwords. 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).  Firewall maintenance: Firewall maintenance entails checking and updating security configurations regularly to stay ahead of potential threats. This can happen regularly. Firewall rules can be updated in response to an event that allows abnormal network traffic into the network. This measure can be used to protect against various DDoS attacks. |