# Security risk assessment report

| **Part 1: Select up to three hardening tools and methods to implement** | |
| --- | --- |
| To protect the organization’s network and prevent future data breaches, I recommend implementing the following three network hardening tools and methods:   1. Implement Multifactor Authentication (MFA)   MFA requires users to provide two or more verification factors to gain access to resources. This ensures that even if a password is compromised, unauthorized access is still prevented.   1. Configure Strong Firewall Rules   Firewalls should be configured with rules to filter both inbound and outbound traffic. This limits exposure to malicious traffic and restricts unnecessary external communication   1. Enforce Secure Password Policies and Password Management Tools   Password sharing and default passwords expose critical vulnerabilities. Implementing strong password policies (e.g, complexity, expiration, uniqueness) and using tools like password managers will reduce this risk. | |
|

| **Part 2: Explain your recommendations** |
| --- |
| 1. Multi Factor Authentication(MFA)   MFA is effective because it adds an additional layer of security beyond passwords. It can be implemented using an app (like Google Authenticator), SMS verification, or biometric verification. MFA should be enforced for all user logins, especially administrators and sensitive data systems. THis method should be implemented permanently with periodic reviews for compliance.   1. Firewall Rules Configuration   Proper firewall configuration is critical for defending against unauthorized access and data exfiltration. Defining inbound/outbound rules ensures only necessary traffic is allowed. Rules should be reviewed and updated weekly or monthly based on security logs and access patterns.   1. Secure Password Policies and Tools   By disabling default passwords and enforcing strong password requirements, organizations significantly reduce the risk of brute -force and credential -stuffing attacks. Passwords should be updated regularly (eg, every 90 days) and password management tools should be deployed to encourage unique, complex and non-reused passwords across accounts. |