# Security risk assessment report

| **Part 1: Select up to three hardening tools and methods to implement** | |
| --- | --- |
| The network security team recommends the following three network hardening policies as initial steps:   1. National Institute of Standards and Technology (NIST) password policies. 2. Two-factor/multi-factor authentication (2FA/MFA). 3. Firewall Maintenance | |
|

| **Part 2: Explain your recommendations** |
| --- |
| 1. Employees are currently sharing accounts and passwords. This creates an unacceptable risk of compromise and violates best practices. 2. Users should have individual accounts and passwords. In addition to passwords that meet NIST password policies, users will be required to have a second (or more) method of authenticating their identity. This will mitigate the risk of a compromised password. 3. Firewalls currently do not have rules to filter inbound and outbound traffic. Rules that limit traffic only to business needs will reduce the attack surface of the organization. |