# Security risk assessment report

|  |
| --- |
| **Part 1: Select up to three hardening tools and methods to implement** |
| 1. Implementing stronger password policies. 2. Implementing two-factor authentication (2FA). 3. Performing firewall maintenance regularly   A stronger password policy could include having a minimum length restriction, and a requirement that all passwords include numbers or special characters. Additionally, an encouragement to users not to share passwords for safety would be necessary as well.  A simple 2FA could be implemented where users have to enter a one-time code sent to their email or phone before they log in to their device/network.  Firewall rules should be set and updated regularly in accordance with security events. This is to ensure that only the needed and accepted traffic is being accepted into the network, reducing the attack surface of the network and maintaining a good security posture. |
|

|  |
| --- |
| **Part 2: Explain your recommendations** |
| All of the listed hardening tools are in response to the organizations high likelyhood of brute force attacks as an attack vector. This is due to their easy to guess, and non-unique default passwords – and due to a lack of property security controls to regulate the flow of access. By enforcing better password policies, it makes the organization less prone to brute-force password guessing attacks. By also enforcing 2FA, the organization would be adding another layer of security towards authentication of a user – which is great for minimizing the possibility of a brute-force attack. Additionally, a regular firewall maintenance is necessary because it is responsible for protecting the network against unrelated and malicious traffic. Regular updates to the firewall rules to only allow intended traffic and match up with constantly changing security policies is important to ensure a good security posture and protection of the internal network. |