# Security risk assessment report

|  |
| --- |
| **Part 1: Select up to three hardening tools and methods to implement** |
| After a review and fully considering what recently happened in this organization to protect and prevent the safety of our customers some protective actions need to be taken. Since the organization has been compromised and based on the evaluation we must implement more layers of security for the security of organization, employees and customers.  The password policies should be implemented to prevent attackers from easily guessing user credentials. This method will help and follow the latest recommendation of the NIST standards. This will enforce to frequently change password for everyone within the organization and clients as well.  Alongside password policies, an essential extra layer of security that should be implemented is Multi Factor authenticator that was not used. This will require a user to verify their identity in two or more ways to access the system or network. This can help to protect or prevent against a brute force attack.  Firewalls should have specific rules for filtering traffic based on configurations to stay ahead of potential threats. This method can be used to block or allow network traffic into the network. |

|  |
| --- |
| **Part 2: Explain your recommendations** |
| To improve security, these actions should be taken immediately. Following password policies will help the organization ensure that everyone follows a standard of rules for password policies for creating and managing passwords. These policies will make sure that passwords expire regularly and that new ones are required. Helping to the brute force attacks. By implementing these policies, the organization will follow the best practices for passwords policies. Another important step to take action that is adding an extra layer of security with MFA. This will require an extra prove of identity of who they are or they have. This will ensure security for both customers and the organization by making it harder for attackers to gain access.  Firewalls maintenance is essential in a network. Setting up of specific set of rules will help the organization to stay ahead in case of threats such as men in the middle attack. This technique allows or block network traffic based on security rules, helping to control what enters and exits the network. Following this recommendation will help to prevent future threats or attacks. It is very important to stay up to date with the latest standards and practices. |