# Security risk assessment report

|  |
| --- |
| **Part 1: Select up to three hardening tools and methods to implement** |
| 1. Multifactor authentication (MFA) 2. Encryption using the latest standards. 3. Password policies |
|

|  |
| --- |
| **Part 2: Explain your recommendations** |
| 1. MFA allows access based on two identifications of the user e.g. say one is a password and the other can be an OTP or fingerprint or face detection etc., which makes it very difficult for anyone to gain unauthorized access. Even if someone was able to find the password, they still might need a fingerprint as a second authentication step to gain access. This Hardening method makes sure to verify the user in two or more ways which reduces the likelihood that a malicious actor can access a network through any attack. 2. Setting rules to allow and block unwanted network traffic through firewall configuration can prevent the company assets from being harmed by any external unauthorized access. 3. Password policies are more of an administrative control wherein the user or employees of the company must follow certain conditions to set up the password. Conditions like passwords should be 8 characters long, passwords should have at least one capital letter, passwords should be alphanumeric, passwords to be changed after every 3 months, passwords should not be repeated, etc. Such rules prevent the use of default passwords and have strong passwords to prevent brute-force attacks. |