# Security risk assessment report

|  |
| --- |
| **Part 1: Select up to three hardening tools and methods to implement** |
| Based on the recent security breaches discovered the following security practicies is strongly recommended:  1. Implement a multi factor authentication  2. Enforce a password policy so that complexity is adopted i.e. mixture of special characters and character length recommended minimum of 12 characters. Furthermore enforce password history so that previous passwords are not repeated. I would recommended a password change every 30 days.  3. Implement firewall rules to block traffic coming from certain ports. |
|

|  |
| --- |
| **Part 2: Explain your recommendations** |
| Here are the main justifications as to why these recommended hardening practices should be implemented:  use of multi factor authentication would resolve the issue with internal password sharing, even if the user attempts to logon with username and password belonging to the account owner they have to validate their identity using MFA which changes every 60 seconds. For MFA its rcommendd to us OTP (one time password) application authenticator from google or microsoft using SMS or email is not recommended as this allows a hacker to eavesdrop using Smishing or phishing attempts to access the passcode. Implementing of this security practice would be a one time operation.  A bad practice was detected where the default admin password remains unchanged which is open to potential threats by imposing a password enforcement policy would prevent internal or external risks where someone could gain access to the system causing harm such as running malicious code or tampering / gaining access to unauthorized data. This security practice would require the operation of ocassional password change once per month.  Disabling ports that are not used by the organisation reduces the attack surface within the network. Thsi reduces the availability and probability of bad actors succeeding in gaining access to the network causing malicious intent. This operation would require frequent reviws depending on possible applications and systems requiring access to aditional ports. |