# Security risk assessment report

| **Part 1: Select up to three hardening tools and methods to implement** | |
| --- | --- |
| 1. Setting up a high level password complexity policy 2. Use of Multi factor Authentication- password, fingerprints, authenticator apps 3. Encryption and Network Firewall rules | |
|

| **Part 2: Explain your recommendations** |
| --- |
| 1. Setting up a high level password complexity policy. This is recommended because employees share passwords and the admin password of the database is set to default. Threat actors have access to documentations and application updates as they are released by the vendors or OEM and it is also easy for them to bruteforce the shared password which is easy for them to guess. Thus implementing password policy by setting up complexities such as a certain length of characters must be used in the password, including: uppercase, lowercase and numbers and ensuring the employees modify the password periodically. Secondly, using MFA adds another layer of hardening to the security of the systems and applications. Lastly, encryption will ensure that while the threat actor is able to guess the shared password it wont be able to modify the data thus preserving the integrity of the data. The network firewall rules must be configured to allow needed ports and block unneeded ports and also ensure. The combination of all the three hardening techniques conforms with the principle of defense in depth which states that having several layers of security or hardening makes security more effective for the social media company. |