# Security risk assessment report

|  |
| --- |
| **Part 1: Select up to three hardening tools and methods to implement** |
| 1. Multifactor authentication (MFA) 2. Firewall maintenance 3. Password policies |
|

|  |
| --- |
| **Part 2: Explain your recommendations** |
| 1. Multifactor authentication (MFA) (MFA prevent unauthorized access into staff accounts event if their passwords remain compromised. This typically is a one-off task, but it could be required to be updated as industry trends dictates). 2. Firewall maintenance (this enables firewalls to be frequently equipped to detect and stop malicious traffic in & out of the Network. As sec analysts become aware of more malicious traffics, they update their IP and port restriction lists). 3. Password policies (every account must strictly follow password standards that are hard to guess, not shared or repeated nor default. Ensure a strict password compliance would prevent cases of one-point compromise of the whole network). |