

# Security risk assessment report

## Part 1: Select up to three hardening tools and methods to implement

We recommend the following security measures:

1. Creation of a strong password policy specifically disallowing password sharing, requiring password changes every 6 months and MFA to be set-up; 2
2. Implementation of port-filtering and regular firewall maintenance;
3. And conducting regular security audits that include penetration tests.

## Part 2: Explain your recommendations

1. An adequate password policy helps mitigate the risk of system admins passwords getting compromised, and thus increases the overall security of the assets and reliability of the IT team when responding to incidents.
2. Port filtering and regular firewall maintenance helps mitigate the risk of threat actors connecting to the network and sending malicious traffic, thus mitigating the risk of further data-breaches.
3. Regular security audits that include pen tests is of utmost importance to avoid making similar mistakes of missing common and industry-standard security controls and measures to mitigate the risk of attacks, both similar to this specific one and of other types.