Security risk assessment report

Part 1: Select up to three hardening tools and methods to implement
Since concern 1 and 2 both share the same vulnerability, Password policies must be implemented, concern 3 must filter unnecessary ports of the network to prevent any potential attacks, concern 4 must set MFA, such that it's nearly impossible to brute force an account.

Part 2: Explain your recommendations
1. Implementing Strong password policies as in case 1. Employees share the same password. This will make it easier for an attacker to compromise an employee's account if one account has been breached. Case 2 is using a default password. This can be vulnerable to brute force attack such as dictionary attack so to prevent attackers gaining an admin account, implementing a strong password policy is a must 2. Not filtering traffic incoming and outgoing from and to the network is dangerous, this could open a lot of attack surface for malicious actors. 3. MFA helps account harder to bruteforce so setting MFA is a standard practice for an organization.