Security risk assessment report

1. **The organization’s employees' share passwords.**
2. **The admin password for the database is set to the default.**
3. **The firewalls do not have rules in place to filter traffic coming in and out of the network.**
4. **Multifactor authentication (MFA) is not used.**

Part 1: Select up to three hardening tools and methods to implement
Three hardening tools that will work best to remedy the lapses in network security are firewall maintenance to begin filtering out the internet traffic which is left unchecked, password policies to ensure admin access can not be trivially gained by simply utilizing the default password, and network access privileges to stop password sharing and the ability for any given employee to access accounts outside their privilege.

Part 2: Explain your recommendations
Firewall maintenance is the first step as the current state of the network would enable any outside attacker to, at the minimum successfully, try any attack, as we are not limiting network access. Password policies are necessary as the admin account being unprotected by a good password would allow any adversary to easily gain the highest level of access enabling any action they could desire. Network access privilege will further make such that any successful attack on one employee account does not compromise the entire network due to password sharing and open privilege.