# Security risk assessment report

| **Part 1: Select up to three hardening tools and methods to implement** | |
| --- | --- |
| Based off of the current state of network security within the organization, I would recommend the following hardening tools/methods   1. Password Policies 2. Port Filtering 3. Multifactor Authentication | |
|

| **Part 2: Explain your recommendations** |
| --- |
| 1. Password Policies are the first thing recommended for the company, due to the potential for data leaks as the passwords currently stand. By using the default password for the admin database, as well as sharing passwords among employees, the company is much more likely to be subject to a brute force attack. As is, if an attacker was to correctly determine one employees password, they would have access to every employees data as well. By adjusting these and adhering to password guidelines in place, It would significantly decrease not only the scope of an attack, but also the likelihood of one as well. 2. As the firewall is currently set up, there is no filter to the traffic coming in and out of the network. This leaves an extreme amount of vulnerability within the system from attackers outside of the private network of the company. By reducing the number of ports in use as well as blocking ports that are not in use by the company, there is a significantly lower risk to unauthorized traffic entering the network and potentially leaking patrons data. 3. By enabling and enforcing Multifactor Authentication for employees, it lowers the risk of leaking sensitive data into the wrong hands. Multifactor Authentication for logins require multiple forms of verification in order to access the network, which would make it much more difficult for attackers to access and leak sensitive information. Biometric authentication would leave the least room for breaches. |