# Security risk assessment report

| **Part 1: Select up to three hardening tools and methods to implement** | |
| --- | --- |
| 1. Password Policies 2. Multifactor Authentication (MFA) 3. Firewall maintenance / port filtering | |
|

| **Part 2: Explain your recommendations** |
| --- |
| Our first recommendation is incorporating and enforcing strong password policies. As noted, organization’s employees are currently sharing passwords, which is a practice extremely susceptible to a brute force attack. The current state of password management makes it very easy for a threat actor, which can include a previous or disgruntled employee, to access customers' personal information. Password policies recommended include having strong password rules such as including a capital letter, numbers, symbols, mandating passwords be changed every few months, and using a password manager so that simple, sharable passwords are not possible. Particularly for the admin password, this should be revised immediately to prevent a possible attack.  The 2nd recommendation is to use multifactor authentication. Since employees and admins have access to PII, it is crucial to create layers of defense (defense in depth). By using multifactor authentication such as 2FA or otherwise verifying the employee’s identity, we can be sure the person accessing the information is not for outside of the organization.  The 3rd recommendation is firewall maintenance and port filtering. As the current firewall does not currently filter traffic coming in and out, we recommend placing firewall rules against unknown websites going both in and out. We can also create rules so that any unused ports are blocked off. By creating these firewall rules, we are able to narrow down exactly which websites and ports are used by the organization to complete the work and not be even more susceptible to potential attacks from unknown websites. The firewall should then be maintained to allow or block off any exceptions or changes. |