Functional Requirements:

1. Access Control and User Management or Security

* Implement RBAC or Role Based Access Control. This will assign specific roles in the company like HR, accounting, IT, Management and more to specific restrictions and permissions based on their roles and no more. Also IT will have privileged access control to where they can control things like an admin account.
* Implementing Domain Accounts. This is to basically create more security by creating company specific email accounts for all employees.

1. Building Security/Physical Security

* Transition to traditional badge systems. We will assign access badges to employees, with an image of their face and their role in the company as well as enabling tracking and logging of physical access. We will configure the system so that it records entry and exit times and it restricts access based on role in the company.

1. Data Storage

* We will digitize all physical files and create or develop a structured digital storage system. We will create a company file database with file management security protocols that will be accessible by specific roles. We will create and include backup systems to ensure that there is data recovery and integrity.

1. On/Off Boarding Procedures

* Establish a good and secure onboarding process. In this process when we on board an employee we will assign roles and access permissions based on their new role and nothing more, we will also have training for security awareness. For the off boarding process it will be very strict where we will revoke all of their access and recover any and all company issued items like devices and badges before they fully leave.
* Implementing an ISO. The ISO will be used so that when we are onboarding new employees there will be an image that appears on their computer that contains things like our company’s operating system, software, security policies, configurations and more. This will allow for better consistency, cohesion and security. Also we can separate what image is shown to different new employees based on their role in the company, furthering security. Different roles would see in the image different applications needed for their role, like for example new IT personnel would see an admin tool application in the image compared to someone in finance who would see an accounting application. This makes the on boarding process much more secure and easier.

Non Functional Requirements:

1. IT Infrastructure and Team Improvement

* Expand the IT team. We will hire more IT Members with a lot of experience so that we can increase the number of technically skilled members. This will enhance our ability to cover system maintenance, monitoring, and incident response capabilities. This will also give us the chance to update and secure all systems to maintain the best performance and have high availability.

1. Network and Website Security

* For Website Security we can replace the existing website with a new secure custom built website that uses SSL encryption and a lot of industry standard security practices and policies for websites.
* For Network Security, it would be best to improve and create more Firewall policies that are more strict as well as add an IPS as well as an IDS to our Network Security. We can have firewall policies for network segmentation and with IPS and IDS enabled we can detect and prevent malicious software from entering our network. For IDS we can have an anomaly based IDS that detects unusual behavior within our network. For IPS we can have a signature based detection that uses a database of previously prevented threats to detect new network attacks.

1. Security Standards and Policies

* Implementing a Strong Password Policy and MFA. All logins require 2FA and the password policy is complex. All passwords require eight or more characters, one number, one letter, one capital letter, one symbol, and the password can not include your first or last name. Also the password resets after every quarter. This password policy enforces great security and good practice to prevent against brute force attacks and more.
* Include a very regular security audit. In this audit IT members will check and update security policies/procedures, permissions, network security, website security, physical security, technical security, and administrative security. This check will also update firewall, IPS, and IDS settings so that they defend against current day threats.

1. Disaster Recovery

* Develop a Disaster Recovery Plan. In this plan we should schedule a very regular backup for our most important data and configurations. Also we need to ensure we have redundancy for servers and key network components so that we can minimize downtime in case something happens. Another thing that is safe to have is an off site data backup storage in case of natural disasters in our area.