**Security Assessment Report**

**Security Shortcomings:**

The following security shortcomings are considered major vulnerabilities to the organization's security posture and must be addressed immediately.

* The organization’s employee’s share passwords
* The admin password to the database is set to default
* The firewalls do not have rules in place to filter incoming and outgoing traffic
* Multifactor authentication is not enforced

**Security Recommendations:**

* Stricter password policies should be implemented
  + Employees should not have equal access to all systems. Employee access should be limited to only the systems necessary to fulfill their roles within the organization and each employee should have a unique username/password to access the systems.
  + The admin password should not be the default password of the database server. This makes it highly susceptible to brute force attacks. All passwords should meet modern standards by including a range of letters, lettercasings, numbers and special characters.
* Firewall rules should be updated to better monitor incoming and outgoing traffic
  + The firewall rules should implement port filtering rules to limit the types of incoming and outgoing traffic to the network and limit unwanted communications.
* Network segmentation
  + Touched on briefly in the password policy recommendation but employee access to systems on the network should be limited to only the systems necessary to fulfill their respective roles. This limits the attack surface available to malicious actors and prevents the entire network from becoming corrupted in the case of a system becoming corrupted.

**Security Justifications:**

All recommendations provided in this report are intended to reduce the organization’s attack surface area and improve their security posture. As their security currently stands the organization is susceptible to a host of attacks including DoS attacks, IP spoofing and brute force attacks. The loss of sensitive data can be mitigated and the assurance of business continuity could be raised significantly by implementing the recommended security improvements.