Administrative/Managerial Controls				
Control Name	**Control Type**	**Control Purpose**	**Required?**	**Existing control practices**
Least Privilege	Preventative	Reduce risk and overall impact of malicious insider or compromised accounts	☑	All employees have access to sensitive customer data. This needs to be changed with proper access management in place.
Disaster recovery plans	Corrective	Provide business continuity	☑	There are no disaster recovery plans currently in place, and the company does not have backups of critical data.
Password policies	Preventative	Reduce likelihood of account compromise through brute force or dictionary attack techniques	☑	Password policy is in place. Need to inforce strict guidelines and follow protocols.
Access control policies	Preventative	Bolster confidentiality and integrity by defining which groups can access ormodify data	☑	No access policies implemented.
Account management policies	Preventative	Managing account lifecycle, reducing attack surface, and limiting overall impact from disgruntled former employees and default account usage	☐	not applicable
Separation of duties	Preventative	Reduce risk and overall impact of malicious insider or compromised accounts	☑	Not implemented.

Technical Controls				
Control Name	**Control Type**	**Control Purpose**	**Required?**	**Existing control practices**
Firewall	Preventative	To filter unwanted or malicious traffic from entering the network	☐	Currently in place. Blocks traffic based on an appropriately defined set of security rules.
IDS/IPS	Detective	To detect and prevent anomalous traffic that matches a signature or rule	☑	Not installed
Encryption	Deterrent	Provide confidentiality to sensitive information	☑	Currently not used.
Backups	Corrective	Restore/recover from an event	☑	No recovery plans and no backup for critical data.
Password management	Preventative	Reduce password fatigue	☑	no centralized password management
Antivirus (AV) software	Preventative	Scans to detect and quarantine known threats	☐	Installed and monitored regularly.

Manual monitoring, maintenance, and intervention	Preventative	Necessary to identify and manage threats, risks, or vulnerabilities to out-of-date systems	☑	Legacy systems are monitored but not regular. Needs automation and proper scheduling.

Physical/Operational Controls				
Control Name	**Control Type**	**Control Purpose**	**Required?**	**Existing control practice s**
Time-controlled safe	Deterrent	Reduce attack surface and overall impact from physical threats	☐	Required but not applicable in this assessment
Adequate lighting	Deterrent	Deter threats by limiting “hiding” places	☑	
Closed-circuit television (CCTV)	Preventative/ Detective	Closed circuit television is both a preventative and detective control because it’s presence can reduce risk of certain types of events from occurring, and can be used after an event to inform on event conditions	☐	Installed and functioning
Locking cabinets (for network gear)	Preventative	Bolster integrity by preventing unauthorized personnel and other individuals from physically accessing or modifying network infrastructure gear	☑	No physical security measures that prevents unauthorized access such as badges.
Signage indicating alarm service provider	Deterrent	Deter certain types of threats by making the likelihood of a successful attack seem low	☐	Required but not applicable in this assessment
Locks	Deterrent/Preventative	Bolster integrity by deterring and preventing unauthorized personnel, individuals from physically accessing assets	☑	No physical security measures that prevents unauthorized access such as badges.
Fire detection and prevention (fire alarm,	Detective/Preventative	Detect fire in physical location and prevent damage to physical assets such as inventory, servers, etc.	☑	Installed and functioning