Control Name	Control Type
Least Privilege	Preventative
Disaster recovery plans	Corrective
Password policies	Preventative
Access control policies	Preventative
Account management policies	Preventative
Separation of duties	Preventative

Control Name	Control Type
Firewall	Preventative
IDS/IPS	Detective
Encryption	Deterrent
Backups	Corrective
Password management	Preventative
Antivirus (AV) software	Preventative
Manual monitoring, maintenance, and intervention	Preventative

Control Name	Control Type
Time-controlled safe	Deterrent
Adequate lighting	Deterrent
Closed-circuit television (CCTV)	Preventative/Detective
Locking cabinets (for network gear)	Preventative
Signage indicating alarm service provider	Deterrent
Locks	Deterrent/Preventative
Fire detection and prevention (fire alarm, sprinkler system, etc.)	Detective/Preventative

Administrative/Managerial Controls

Control Purpose	Required?
Reduce risk and overall impact of malicious insider or compromised accounts	☑
Provide business continuity	☑
Reduce likelihood of account compromise through brute force or dictionary attack techniques	☑
Bolster confidentiality and integrity by defining which groups can access ormodify data	☑
Managing account lifecycle, reducing attack surface, and limiting overall impact from disgruntled former employees and default account usage	☐
Reduce risk and overall impact of malicious insider or compromised accounts	☑

Technical Controls

Control Purpose	Required?
To filter unwanted or malicious traffic from entering the network	☐
To detect and prevent anomalous traffic that matches a signature or rule	☑
Provide confidentiality to sensitive information	☑
Restore/recover from an event	☑
Reduce password fatigue	☑
Scans to detect and quarantine known threats	☐
Necessary to identify and manage threats, risks, or vulnerabilities to out-of-date systems	☑

Physical/Operational Controls

Control Purpose	Required?
Reduce attack surface and overall impact from physical threats	☐
Deter threats by limiting “hiding” places	☑
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	☐
Bolster integrity by preventing unauthorized personnel and other individuals from physically accessing or modifying network infrastructure gear	☑
Deter certain types of threats by making the likelihood of a successful attack seem low	☐
Bolster integrity by deterring and preventing unauthorized personnel, individuals from physically accessing assets	☑
Detect fire in physical location and prevent damage to physical assets such as inventory, servers, etc.	☑

Existing control practices
All employees have access to sensitive customer data. This needs to be changed with proper access management in place.
There are no disaster recovery plans currently in place, and the company does not have backups of critical data.
Password policy is in place. Need to inforce strict guidelines and follow protocols.
No access policies implemented.
not applicable
Not implemented.

Existing control practices
Currently in place. Blocks traffic based on an appropriately defined set of security rules.
Not installed
Currently not used.
No recovery plans and no backup for critical data.
no centralized password management
Installed and monitored regularly.
Legacy systems are monitored but not regular. Needs automation and proper scheduling.

Existing control practice s
Required but not applicable in this assessment
Installed and functioning
No physical security measures that prevents unauthorized access such as badges.
Required but not applicable in this assessment
No physical security measures that prevents unauthorized access such as badges.
Installed and functioning