Current Assets

The assets managed by the IT Department include:

- On-site equipment for office operations
- Employee devices: end-user equipment like desktops, laptops, smartphones, remote workstations, headsets, cables, keyboards, mice, docking stations, surveillance cameras, etc.
- Management of systems, software, and services: covering areas like accounting, telecommunications, databases, security, e-commerce, and inventory management
- Internet connectivity
- Internal network infrastructure
- Vendor access management
- Data center hosting services
- Data retention and storage solutions
- Badge readers
- Maintenance of legacy systems: systems that are outdated and require manual oversight

Administrative Controls

Control Name	**Control Type and Explanation**	**Needs to be Implemented (X)**	**Priority**
Least Privilege	Preventative; limits access to necessary assets/data for vendors and unauthorized personnel	X	High
Disaster Recovery Plans	Corrective; ensures business continuity by maintaining systems operation during incidents, minimizing downtime and impact, including aspects like computer room environment, hardware, connectivity, applications, and data restoration	X	High
Password Policies	Preventative; enforces strong password criteria to enhance security and prevent account breaches from brute force or dictionary attacks	X	High
Access Control Policies	Preventative; enhances data confidentiality and integrity	X	High
Account Management Policies	Preventative; reduces risks from disgruntled or former employees	X	High/Medium

Separation of Duties	Preventative; prevents individuals from having excessive access that could be exploited for personal gain	X	High

Technical Controls

Control Name	Control Type and Explanation	Needs to be Implemented (X)	Priority
Firewall	Preventative; existing firewalls filter unwanted or malicious traffic from the internal network	NA	NA
Intrusion Detection System (IDS)	Detective; helps the IT team quickly identify potential intrusions like unusual traffic	X	High
Encryption	Deterrent; secures sensitive information and data (e.g., website payment transactions)	X	Medium
Backups	Corrective; ensures continuous productivity during incidents, aligned with the disaster recovery plan	X	High
Password Management System	Corrective; facilitates password recovery, resets, and lockout notifications	X	Medium
Antivirus (AV) Software	Corrective; detects and quarantines known threats	X	High
Manual Monitoring, Maintenance, and Intervention	Preventative/Corrective; necessary for legacy systems to detect and address potential threats, risks, and vulnerabilities	X	High

Physical Controls

Control Name	Control Type and Explanation	Needs to be Implemented (X)	Priority
Time-Controlled Safe	Deterrent; reduces exposure to physical threats	X	Low
Adequate Lighting	Deterrent; limits areas where threats can hide	X	Low
Closed-Circuit Television (CCTV) Surveillance	Preventative/Detective; helps reduce certain risks and aids post-event investigations	X	Medium
Locking Cabinets (for Network Gear)	Preventative; enhances integrity by preventing unauthorized physical access or modifications to network equipment	X	Medium

Signage Indicating Alarm Service Provider	Deterrent; discourages potential attacks by indicating a lower chance of success	X	Low
Locks	Preventative; secures physical and digital assets	X	High
Fire Detection and Prevention (fire alarm, sprinkler system, etc.)	Detective/Preventative; detects fires in the physical store location to prevent damage to inventory, servers, etc.	X	Low