Control assessment

List of assets

Assets managed by the IT Department include:

- On-premises equipment for in-office business needs
- Employee equipment: end-user devices (desktops/laptops, smartphones), Remote workstations, headsets, cables, keyboards, mice, docking stations, Surveillance cameras etc.
- Management of systems, software, and services: accounting, Telecommunication, database, security, ecommerce, and inventory Management
- Internet access
- Internal network
- Vendor access management
- Data center hosting services
- Data retention and storage
- Badge readers
- Legacy system maintenance: end-of-life systems that require human Monitoring

Administrative Control

Control name	**Control type and Explanation**	**Need to be implemented (X)**	**Priority**
Principle of least privilege	Preventive: Giving least possible amount of access to data and other control to employees and customer to complete their business smoothly	X	High
Disaster recovery plan	Corrective: Having proper backup of		

	data to some remote server to avoid hindrance incase data breach occurs	X	High
Password policy	Preventive: Insuring that employees and customer create strong password, have at least 8 words including special characters, to reduce likelihood of account compromise via Brute force or dictionary attack technique	X	High
Access Control policies	Preventive: assigning a suitable person to have administrative control of data and should be responsible to maintain the Confidentiality of data and other assets of company	X	High
Account management policies	Preventive: reducing attack surface area by deactivating accounts of former employees, conducting regular security test to find	X	High

	out vulnerabilities in system, regular monitoring of logs to mitigate potential risks		
Separation of duties	Preventive: proper separation of duties of that none of employee enjoy enough privilege to act as threat actor	X	High

Technical Control			
Control name	**Control type and Explanation**	**Need to be implemented (X)**	**Priority**
Fire wall	Preventive: Have updated firewall to prevent unwanted access to system	X	High
IDS/IPS	Detective: having Intrusion Detection System and Intrusion Prevention System software to detect and prevent suspicious network traffics	X	High
Encryption	Deterrent: convert sensitive information into cipher text to strengthen the confidentiality of data	X	Medium
Password management	Preventive: avoid password fatigue by using password	X	Low

	management software like Nordpass		
Backup	Corrective: Ensure proper backup of data to main continuity of business. Backup data can be stored on cloud platform	X	High
Antivirus Software(AV)	Preventive: install AV software to detect and quarantine possible threats	X	Medium
Manual monitoring, maintenance and intervention	Preventive: regular monitoring of systems to identify out-of-date system to mitigate threat risk and vulnerabilities	X	Low

Physical Control

Control name	**Control type and Explanation**	**Need to be implemented (X)**	**Priority**
Time-controlled safe	Deterrent:reduce attack surface/impact on physical assets	X	Low
Closed circuit television (CCTV)	Deterrent/preventive: To monitor any malicious activity performed by any employee	X	Medium/High
Adequate lighting	Deterrent: To limit Hiding places	X	Low
Locking Cabinet for Network room	Preventive: avoid threat actor to access	X	Low

	to network room		
Biometric Locks	Preventive: Installing Biometric locks in office to have record of who came when	X	Low
Fire detection and prevention	Preventive: installing proper fire detection system and prevention system like sprinklers	X	Low
Locks	Preventive: to store confidential data	X	High