

Controls assessment

To review control categories, types, and the purposes of each, read the [control categories](#) document.

Current 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 Controls			
Control Name	Control type and explanation	Needs to be implemented (X)	Priority
Least Privilege	Preventative; reduces risk by making sure vendors and non-authorized staff only have access to the assets/data they need to do their jobs	X	High
Disaster recovery	Corrective; business continuity	X	High

Administrative Controls			
plans	to ensure systems are able to run in the event of an incident/there is limited to no loss of productivity downtime/impact to system components, including: computer room environment (air conditioning, power supply, etc.); hardware (servers, employee equipment); connectivity (internal network, wireless); applications (email, electronic data); data and restoration		
Password policies	Preventative; establish password strength rules to improve security/reduce likelihood of account compromise through brute force or dictionary attack techniques	X	Medium
Access control policies	Preventative; increase confidentiality and integrity of data	X	High
Account management policies	Preventative; reduce attack surface and limit overall impact from disgruntled/former employees		Medium
Separation of duties	Preventative; ensure no one has so much access that they can abuse the system for personal gain		Medium

Technical Controls			
Control Name	Control type and explanation	Needs to be implemented (X)	Priority
Firewall	Preventative; firewalls are already in place to filter unwanted/malicious traffic from entering internal network		N/A
Intrusion Detection System (IDS)	Detective; allows IT team to identify possible intrusions (e.g., anomalous traffic) quickly	X	Medium
Encryption	Deterrent; makes confidential information/data more secure (e.g., website payment transactions)	X	High
Backups	Corrective; supports ongoing productivity in the case of an event; aligns to the disaster recovery plan	X	High
Password management system	Corrective; password recovery, reset, lock out notifications	X	Medium
Antivirus (AV) software	Corrective; detect and quarantine known threats	X	Medium
Manual monitoring, maintenance, and intervention	Preventative/corrective; required for legacy systems to identify and mitigate potential threats, risks, and vulnerabilities	X	Medium

Physical Controls			
Control Name	Control type and explanation	Needs to be implemented (X)	Priority
Time-controlled safe	Deterrent; reduce attack surface/impact of physical threats		Medium
Adequate lighting	Deterrent; limit “hiding” places to deter threats		Medium
Closed-circuit television (CCTV) surveillance	Preventative/detective; can reduce risk of certain events; can be used after event for investigation		Low
Locking cabinets (for network gear)	Preventative; increase integrity by preventing unauthorized personnel/individuals from physically accessing/modifying network infrastructure gear	X	High
Signage indicating alarm service provider	Deterrent; makes the likelihood of a successful attack seem low		Medium
Locks	Preventative; physical and digital assets are more secure		High
Fire detection and prevention (fire alarm, sprinkler system, etc.)	Detective/Preventative; detect fire in the toy store’s physical location to prevent damage to inventory, servers, etc.	X	High