Controls assessment

To review control categories, types, and the purposes of each, read the [control categories](https://docs.google.com/document/d/1Ut_H5A9FHwuQEy6_qG6Lfy3zwF6GSJnj3DZTMaNRWEE/template/preview?usp=sharing&resourcekey=0-i4dR5qZFqQyfzr8uk3OOmA) 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, e-commerce, 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 ensuring vendors and non-authorized staff only have access to the assets/data needed to do their jobs. | **X** | High |
| Disaster recovery plans | Corrective: business continuity to ensure systems can 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 | X | High |
| Password policies | Preventative: establish password strength rules to improve security/reduce the 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 the attack surface and limit the overall impact from disgruntled/former employees | X | Medium |
| Separation of duties | Preventative: ensure no one has so much access that they can abuse the system for personal gain | X | 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 the internal network. | X | High |
| Intrusion Detection System (IDS) | Detective: allows the IT team to identify possible intrusions (e.g., abnormal traffic) quickly. | X | Medium |
| Encryption | Deterrent; makes confidential information/data more secure (e.g., website payment transactions) | X | Medium |
| 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, lockout notifications | X | Medium |
| Antivirus (AV) software | Corrective: detect and quarantine known threats | X | High |
| 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 | X | low |
| Adequate lighting | Deterrent: limit “hiding” places to deter threats | X | medium |
| Closed-circuit television (CCTV) surveillance | Preventative/detective; can reduce risk of certain events; can be used after the event for investigation | X | medium |
| Locking cabinets (for network gear) | Preventative: increase integrity by preventing unauthorized personnel/individuals from physically accessing/modifying network infrastructure gear | X | medium |
| Signage indicating alarm service provider | Deterrent: makes the likelihood of a successful attack seem low | X | medium |
| Locks | Preventative: physical and digital assets are more secure | X | low |
| 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 |