# Botium Toys Control assessment

To review control categories, types and the purpose of each including but not limited to   
  
Control categories

* Administrative/ managerial control
* Technical controls
* Physical/operational controls

## Control types

* Preventative
* Corrective
* Detective
* Deterrent

## 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.

* Storefront products available for retail sale on site and online; stored in the company’s adjoining warehouse
* Management of systems, software, and services: accounting, telecommunication, database, security, ecommerce, and inventory management
* Internet access
* Internal network
* Data retention and storage
* Legacy system maintenance: end-of-life systems that require human
* Monitoring

## Administrative controls

|  |  |  |  |
| --- | --- | --- | --- |
| Administrative controls | | | |
| Control name | Control type | Explanation | Priority |
| Least Privilege | Preventative | Reduces risk of malicious insiders of compromised accounts by ensuring that staff only has access to assets they need to do their job | High |
| Disaster recovery plan | Corrective | Provides business continuity to ensure systems keep running in the event of an incident | High |
| Password policies | Preventative | Establishment of password strength rules to improve security and reduces the likeliness of compromised accounts via brute force or dictionary attacks | High |
| Access control policies | Preventative | Bolster confidentiality and integrity by defining which groups can access and modify data | High |
| Account management policies | Preventative | Managing account lifecycle, reducing attack surface and limiting overall impact from disgruntled former employees and default account usage | Medium |
| Separation of duties | Preventative | Reduces risk and overall impact of malicious inside or compromised account | High |

|  |  |  |  |
| --- | --- | --- | --- |
| Technical controls | | | |
| Control name | Control type | Explanation | Priority |
| Firewall | Preventative | To filter unwanted or malicious traffic from entering the network | High |
| Intrusion detection system (IDS) | Detective | To detect intrusions and prevent anomalous traffic that matches a signature or rule | High |
| Encryption | Deterrent | Provides confidentiality to sensitive information | Medium |
| Backups | Corrective | Restores/recover from an event. Aligns with disaster recovery plans | High |
| Password management system | Preventative | Reduces password fatigue and provides password recovery, reset, lockout notifications | Medium |
| Antivirus software | Preventative | Scans to detects and quarantine known threats | High |
| Manual monitoring, maintenance and intervention | Preventative | Required to identify and mange threats and risks or vulnerabilities to out of date systems | High |

|  |  |  |  |
| --- | --- | --- | --- |
| Physical controls | | | |
| Control name | Control type | Explanation | Priority |
| Time controlled safe | Deterrent | Reduce attack surface and overall impact from physical threats | Low |
| Adequate lighting | Deterrent | Deters threats by limiting hiding spaces | Low |
| Closed circuit tv  CCTV | Preventative /detective | The presence of CCTV can reduce the risk of events occurring and also be used after an event for investigation | Medium |
| Locking cabinets for network gear | Preventative | Increase integrity by preventing unauthorized access from physically accessing or modifying network infrastructure | High |
| Signage indicating alarm service provider | Deterrent | Deters certain types of threats by making the likelihood of a successful attack seem low | Low |
| Locks | Deterrent/ preventative | Bolsters integrity by preventing unauthorized personnel from accessing assets | High |
| Fire detective and prevention | Detective/ preventative | Detects fires in physical locations and prevents damage to physical assets such as inventory, servers etc | High |