## Goals:

| Target Assessments | Systems |
| --- | --- |
| | Current user permissions | | --- | | Current implemented controls | | Current procedures & protocols | | Current compliance Requirements are met | | Current hardware and systems access are accounted for. | | | Accounting | | --- | | End Point Detection | | Firewalls | | Intrusion Detection System (IDS) | | Security Information & Event Management (SIEM) tool | |

## 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

## Controls Assessment

| **Administrative Controls** | | | |
| --- | --- | --- | --- |
| **Control Name** | **Control type and explanation** | **Needs to be implemented**  **(X)** | **Priority**  **(X)** |
| 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 plans | Corrective; business continuity 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 | X | High |
| Password policies | Preventative; establish password strength rules to improve security/reduce likelihood of account compromise through brute force or dictionary attack techniques | X | High |
| 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 | X | High |
| Separation of duties | Preventative; ensure no one has so much access that they can abuse the system for personal gain | X | High |

| **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 | NA | NA |
| Intrusion Detection System (IDS) | Detective; allows IT team to identify possible intrusions (e.g., anomalous traffic) quickly | X | High |
| 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, lock out 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 | High |

| **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 | Low |
| Closed-circuit television (CCTV) surveillance | Preventative/detective; can reduce risk of certain events; can be used after 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 | High |
| Signage indicating alarm service provider | Deterrent; makes the likelihood of a successful attack seem low | X | Low |
| Locks | Preventative; physical and digital assets are more secure | X | 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 | Medium |

## 

## Compliance Checklist

* **General Data Protection Regulation (GDPR)**

GDPR is a European Union (E.U.) general data regulation that protects the processing of E.U. citizens’ data and their right to privacy in and out of E.U. territory. Additionally, if a breach occurs and a E.U. citizen’s data is compromised, they must be informed within 72 hours of the incident.

**Explanation:** Due to the increasing online presence and international sales, Botium Toys needs to be compliant with the E.U. GDPR to protect their European customers.

* **Payment Card Industry Data Security Standard (PCI DSS)**

PCI DSS is an international security standard meant to ensure that organizations storing, accepting, processing, and transmitting credit card information do so in a secure environment.

**Explanation:** Due to the increasing online presence, Botium Toys needs to be PCI DSS compliant to ensure all payments are conducted in a secure manner and customer data is protected.

* **System and Organizations Controls (SOC type 1, SOC type 2)**

The SOC1 and SOC2 are a series of reports that focus on an organization’s user access policies at different organizational levels. They are used to assess an organization’s financial compliance and levels of risk. They also cover confidentiality, privacy, integrity, availability, security, and overall data safety. Control failures in these areas can lead to fraud.

**Explanation:** It is advisable that Botium toys obtain a SOC report to ensure best practices are followed with regard to user access for external & internal personnel and mitigating risks to data security.