# Botium Controls and compliance checklist

**Controls assessment checklist**

|  |  |  |  |
| --- | --- | --- | --- |
| **Yes** | | **No** | **Control** |
|  | |  | Least Privilege |
|  | |  | Disaster recovery plans |
|  | |  | Password policies |
|  | |  | Separation of duties |
|  | |  | Firewall |
|  | |  | Intrusion detection system (IDS) |
|  | |  | Backups |
|  | |  | Antivirus software |
|  |  | | Manual monitoring, maintenance, and intervention for legacy systems |
|  | |  | Encryption |
|  | |  | Password management system |
|  | |  | Locks (offices, storefront, warehouse) |
|  | |  | Closed-circuit television (CCTV) surveillance |
|  | |  | Fire detection/prevention (fire alarm, sprinkler system, etc.) |

**Compliance checklist**

Payment Card Industry Data Security Standard (PCI DSS)

|  |  |  |
| --- | --- | --- |
| **Yes** | **No** | **Best practice** |
|  |  | Only authorized users have access to customers’ credit card information. |
|  |  | Credit card information is stored, accepted, processed, and transmitted internally, in a secure environment. |
|  |  | Implement data encryption procedures to better secure credit card transaction touchpoints and data. |
|  |  | Adopt secure password management policies. |

Botium Toys does not currently follow PCI DSS being the international standard for storing accepting and processing credit card information in a secure environment as they are not only a physical store but also an ecommerce store that handles payments as part of its daily organization’s operations.

General Data Protection Regulation (GDPR)

|  |  |  |
| --- | --- | --- |
| **Yes** | **No** | **Best practice** |
|  |  | E.U. customers’ data is kept private/secured. |
|  |  | There is a plan in place to notify E.U. customers within 72 hours if their data is compromised/there is a breach. |
|  |  | Ensure data is properly classified and inventoried. |
|  |  | Enforce privacy policies, procedures, and processes to properly document and maintain data. |

Botium Toy’s operations do not fall within the GDPR data regulations and may cause customer data and information to be compromised and this may result in fines and penalties in the case that Botium Toys expands and begins operations in the EU

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

|  |  |  |
| --- | --- | --- |
| **Yes** | **No** | **Best practice** |
|  |  | User access policies are established. |
|  |  | Sensitive data (PII/SPII) is confidential/private. |
|  |  | Data integrity ensures the data is consistent, complete, accurate, and has been validated. |
|  |  | Data is available to individuals authorized to access it. |

Although Botium toys have preserved its data integrity, it lacks established user access policies. This poses a risk to sensitive data being compromised in the event of a malicious actor within the company staff, given that all employees currently have access to internally stored data, rather than only the individuals that should have access to it.

Recommendations

Based on the identified risks and vulnerabilities from Botium toys some of the recommendations may be implemented to improve security controls and compliance practices

User Access controls

* Implementation of role-based access control systems to restrict the access to sensitive data. Only authorized personnel should have access to cardholder data and customer PII/SPII
* Adoption of principles of least privilege and separations of duties to limit access to data based on the job roles and responsibilities

Data encryption

* Implement robust encryption mechanisms to safeguard customer credit card information from point-to-point transactions.

Intrusion detection and prevention

* Install and regularly update an intrusion detection system IDS to monitor and detect unauthorized access or malicious activities.

Disaster recovery and data backup

* Develop and regularly test disaster recovery plans to ensure business continuity in the event of data loss or security beach.
* Implement regular data backup procedures

By implementing these recommendations Botium Toys can significantly reduce the risk associated with data breaches, non-compliance and unauthorized access, thereby enhancing overall security and safeguarding sensitive information.