**CONTROL AND COMPLIANCE CHECKLIST FOR BOTIUM TOYS INTERNAL SECURITY AUDIT**

**Prepared by Adeleke Odunayo Joseph**

Select **yes** or **no** to answer the question: Does Botium Toys currently have this control in place?

**Controls assessment checklist**

**Yes** **No**  **Control Assessment**

Botium Toys employees have access to internally stored data and may be able to access

cardholder data and customers’ PII/SPII

Encryption is used to ensure confidentiality of customers’ credit

card information that is accepted, processed, transmitted, and stored locally in

the company’s internal database.

Least privilege and Separation of duties

The IT department ensured availability and integrated controls to ensure

data integrity.

The IT department has a firewall that blocks traffic based on an appropriately

defined set of security rules.

Antivirus software is installed and monitored regularly by the IT department.

An intrusion detection system (IDS) installation?

Disaster recovery plans and Backup in place?

Password policies

Password management system

Systems are monitored and maintained?

Offices, storefront, warehouse has sufficient locks?

Up-to-date closed-circuit television (CCTV) surveillance?

Fire detection and prevention systems?

**Compliance checklist**

Select **yes** or **no** to answer the question: Does Botium Toys currently adhere to this

compliance best practice?

Payment Card Industry Data Security Standard (PCI DSS)

**Yes** **No Best practice**

Only authorized users have access to customers’ credit card information.

Data encryption procedures implementation, to better secure credit card

Transaction touchpoints and data.

Credit card information is accepted, processed, transmitted, and stored

internally, in a secure environment.

General Data Protection Regulation (GDPR)

**Yes No Best Practice**

There is a plan in place to notify E.U. customers within 72 hours if their data is

compromised/there is a breach.

E.U. customers’ data is kept private/secured.

Enforce privacy policies, procedures, and processes to properly document and maintain data.

No access to sensitive data and like customer PII, SPII is granted to all employees.

Data is available to individuals authorized to access it.