# Botium Toys - Controls and Compliance Audit Report

## Controls Assessment Checklist

**Least Privilege - No**

Currently, all employees have access to customer data; privileges need to be limited to reduce the risk of a breach.

**Disaster Recovery Plans - No**

There are no disaster recovery plans in place. These need to be implemented to ensure business continuity.

**Password Policies - No**

Employee password requirements are minimal, which could allow a threat actor to more easily access secure data.

**Separation of Duties - No**

Needs to be implemented to reduce the possibility of fraud since the CEO manages day-to-day operations and payroll.

**Firewall - Yes**

The existing firewall blocks traffic based on an appropriately defined set of security rules.

**Intrusion Detection System (IDS) - No**

The IT department needs an IDS to identify possible intrusions by threat actors.

**Backups - No**

The IT department needs to have backups of critical data to ensure business continuity in case of a breach.

**Antivirus Software - Yes**

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

**Legacy System Monitoring - No**

Systems are monitored and maintained but lack a regular schedule and clear intervention procedures.

**Encryption - No**

Encryption is not currently used; implementing it would provide greater confidentiality of sensitive information.

**Password Management System - No**

There is no password management system in place; implementing one would improve productivity.

**Locks (offices, storefront, warehouse) - Yes**

The store's physical location has sufficient locks.

**CCTV Surveillance - Yes**

CCTV is installed and functioning at the store's physical location.

**Fire Detection/Prevention - Yes**

Botium Toys' physical location has a functioning fire detection and prevention system.

## Compliance Checklist - PCI DSS

**Only authorized users have access to customers' credit card information. - No**

All employees have access to internal data.

**Credit card information is accepted, processed, transmitted, and stored securely. - No**

Credit card information is not encrypted, and all employees have access.

**Implement data encryption procedures. - No**

Encryption is not used to ensure confidentiality of financial information.

**Adopt secure password management policies. - No**

Password policies are nominal and no password management system is in place.

## Compliance Checklist - GDPR

**E.U. customers' data is kept private/secured. - No**

Encryption is not used to ensure confidentiality of customer information.

**Plan to notify E.U. customers within 72 hours if their data is compromised. - Yes**

There is a plan to notify customers within 72 hours.

**Ensure data is properly classified and inventoried. - No**

Assets are listed but not classified.

**Enforce privacy policies and procedures. - Yes**

Policies have been developed and enforced among IT and other employees.

## Compliance Checklist - SOC (Type 1 & 2)

**User access policies are established. - No**

Least Privilege and separation of duties are not in place; all employees have data access.

**Sensitive data (PII/SPII) is confidential/private. - No**

Encryption is not used to protect sensitive data.

**Data integrity ensures consistency and accuracy. - Yes**

Data integrity is maintained.

**Data is available to authorized individuals. - No**

Data is available to all employees; access needs to be restricted.

## Recommendations

Multiple controls need to be implemented to improve Botium Toys' security posture and ensure the confidentiality of sensitive information, including: Least Privilege, disaster recovery plans, password policies, separation of duties, an IDS, encryption, and a password management system. Additionally, classify all assets and enforce regular monitoring of legacy systems. These improvements will help address compliance gaps and better protect sensitive data.