## Internal IT Security Audit Report

**Prepared for**: Botium Toys

**Prepared by**: Rikita Bhattarai

**Audit Date**: March 22, 2025

### Executive Summary

This Internal IT Security Audit was conducted to assess Botium Toys' cybersecurity practices, controls, and regulatory compliance. The review focused on the company's assets managed by the IT department, identifying key risks and gaps against the NIST Cybersecurity Framework, PCI DSS, and GDPR requirements. Significant vulnerabilities were found in data access controls, encryption, disaster recovery planning, and password policies. Immediate action is recommended to reduce the risk of data breaches, regulatory fines, and reputational damage.

### Audit Scope and Goals

Scope:

- On-premises devices and equipment
- Storefront and warehouse assets
- Data retention and storage
- Internal network
- Legacy System Maintenance

Goals:

- Adhere to the NIST Cybersecurity Framework
- Establish policies and procedures to ensure compliance with regulations

Assets managed by the IT Department

- On-premises business equipment
- Employee devices: End-user devices (desktops/laptops, smartphones), remote workstations, headsets, cables, keyboards, surveillance cameras, etc.
- Storefront products (online and physical)
- Software and services (database, e-commerce, etc.)
- Internal network along with internet access
- Data retention and storage

- Legacy System Maintenance

**Risk Assessment and Summary**

Risk Description:

- Inadequate asset management
- Missing critical controls
- Non-compliance with U.S. and international regulations (including the E.U.)

Key Risks Identified:

- Unrestricted employee access to sensitive data (PII/SPII)
- Lack of data encryption
- Absence of access controls (less privilege; separation of duties)
- No backup plans
- Weak password policies and no centralized password management
- No intrusion detection system (IDS)

Risk Score: 8/10 (High)

Additional Comments

The likelihood of potential fines, data breaches, and non-compliance issues is high because the company lacks controls and adherence to necessary compliance regulations and standards.

**Controls Assessment**

| Control Item | Yes/No | Comments |
|---|---|---|
| Least Privilege | No | Not implemented, all employees have access to all data |
| Disaster recovery plans | No | No disaster recovery plans |
| Password policies | No | Not in compliance with the current minimum password complexity requirements |
| Separation of duties | No | Not implemented, all employees must be assigned with their set of duties |

| | | |
|---|---|---|
| Firewall | Yes | Installed and configured aligning with security rules |
| Intrusion detection system (IDS) | No | Needs to be installed |
| Backups | No | Needs to have data backups in case of a breach |
| Antivirus software | Yes | Well-installed and monitored |
| Manual monitoring, maintenance, and intervention for legacy systems | No | Monitored but needs to have a proper scheduled time |
| Encryption | No | Not implemented; highly recommended for increased confidentiality |
| Password management system | No | Not implemented, crucial in case of password issues |
| Locks (offices, storefront, warehouse) | Yes | In place |
| Closed-circuit television (CCTV) surveillance | Yes | All areas covered and up to date |
| Fire Detection/Prevention (Alarms, Sprinklers) | Yes | Fully functional |

**Compliance Checklist**

Payment Card Industry Data Security Standard (PCI DSS)

| Best Practice | Yes/No | Explanation |
|---|---|---|
| Only authorized users have access to a customer's credit card information. | No | All the employees have access to the company data. |
| Credit card information is stored, accepted, processed, and transmitted internally, in a secure environment. | No | Credit card information is not encrypted, and all the employees have access to customer credit card information. |
| Implement data encryption procedures to better secure credit card transaction touchpoints and data. | No | No data encryption is used for confidentiality purposes. |
| Adopt secure password management policies. | No | Password is used but does not follow complexity requirements. |

General Data Protection Regulation (GDPR)

| Best Practice | Yes/No | Explanation |
|---|---|---|
| E.U. customers' data is kept private/secured. | No | The company does not use data encryption to ensure costumer's confidentiality. |
| There is a plan in place to notify E.U. customers within 72 hours if their data is compromised/there is a breach. | Yes | The company plans to notify E.U. customers within 72 hours in case of a data breach. |
| Ensure data is properly classified and inventoried. | No | Current assets only have been listed and not classified. |
| Enforce privacy policies, procedures, and processes to properly document and maintain data. | Yes | Necessary privacy policies and procedures have been enforced among the team members. |

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

| Best Practice | Yes/No | Explanation |
|---|---|---|
| User access policies are established. | No | The principle of Least Privilege and Separation of duties are not enforced. |
| Sensitive data (PII/SPII) is confidential/private. | No | Data is not encrypted. |
| Data integrity ensures the data is consistent, complete, accurate, and has been validated. | Yes | Data integrity is followed. |
| Data is available to individuals authorized to access it. | No | Data is available to all employees; lacks authorization. |

**Recommendations for Improvement**

Several security controls need to be implemented to improve Botium Toys' security posture and better ensure the confidentiality of sensitive information. This includes enforcing Least Privilege and Separation of Duties, developing backup plans, enforcing strong password policies with complexity requirements and regular updates, implementing a centralized password management system, and deploying an Intrusion Detection System (IDS). Additionally, the company must encrypt sensitive data such as PCI-DSS and PII/SPII. Strengthening physical security through periodic audits, classifying assets, and training staff on compliance obligations is also necessary to maintain GDPR and U.S. data protection standards.