### Internal Security Audit and Risk Assessment for Botium Toys

#### Scope and Goals of the Audit

\*\*Scope:\*\*

The audit covers the entire security program at Botium Toys, including all assets, internal processes, and procedures related to controls and compliance best practices.

\*\*Goals:\*\*

- Assess existing assets.

- Complete the controls and compliance checklist.

- Determine which controls and compliance best practices need to be implemented to improve Botium Toys' security posture.

#### Current Assets Managed by IT Department

- \*\*On-premises equipment:\*\* Business needs, employee devices (desktops, laptops, smartphones, remote workstations, headsets, cables, keyboards, mice, docking stations, surveillance cameras, etc.).

- \*\*Storefront products:\*\* Available for retail sale on-site and online; stored in the company’s adjoining warehouse.

- \*\*Management systems:\*\* Accounting, telecommunication, database, security, e-commerce, and inventory management.

- \*\*Internet access and internal network.\*\*

- \*\*Data retention and storage.\*\*

- \*\*Legacy system maintenance:\*\* End-of-life systems that require human monitoring.

#### Risk Assessment

\*\*Risk Description:\*\*

Botium Toys currently has inadequate management of assets and lacks proper controls, leading to non-compliance with U.S. and international regulations. The risk score is assessed at 8 out of 10 due to insufficient controls and adherence to compliance best practices.

\*\*Potential Impact:\*\*

- \*\*Medium impact on business continuity:\*\* Due to the IT department's inability to determine which assets are at risk.

- \*\*High risk of regulatory fines:\*\* Due to non-compliance with necessary controls and regulations.

#### Detailed Control and Compliance Checklist

\*\*Controls Checklist:\*\*

| Control | In Place (Yes/No) |

|---------------------------------------------------------|-------------------|

| Least Privilege | No |

| Disaster recovery plans | No |

| Password policies | No |

| Separation of duties | No |

| Firewall | Yes |

| Intrusion detection system (IDS) | No |

| Backups | No |

| Antivirus software | Yes |

| Manual monitoring maintenance and intervention for legacy systems | Yes |

| Encryption | No |

| Password management system | No |

| Locks (offices, storefront, warehouse) | Yes |

| Closed-circuit television (CCTV) surveillance | Yes |

| Fire detection/prevention (fire alarm, sprinkler system, etc.) | Yes |

\*\*Compliance Checklist:\*\*

| Compliance | In Place (Yes/No) |

|---------------------------------------------------------|-------------------|

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

| Only authorized users have access to customers’ credit card information. | No |

| Credit card information is stored, accepted, processed, and transmitted internally in a secure environment. | No |

| Implement data encryption procedures to better secure credit card transaction touchpoints and data. | No |

| Adopt secure password management policies. | No |

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

| E.U. customers’ data is kept private/secured. | No |

| There is a plan in place to notify E.U. customers within 72 hours if their data is compromised/there is a breach. | Yes |

| Ensure data is properly classified and inventoried. | No |

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

| \*\*System and Organizations Controls (SOC type 1 SOC type 2)\*\* | |

| User access policies are established. | No |

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

| Data integrity ensures the data is consistent, complete, accurate, and has been validated. | Yes |

| Data is available to individuals authorized to access it. | Yes |

#### Recommendations

1. \*\*Implement Least Privilege and Separation of Duties:\*\*

- Reduces the risk of unauthorized access and malicious insider threats.

- Improves overall security by limiting access to critical systems and data.

2. \*\*Develop and Update Disaster Recovery Plans:\*\*

- Ensures business continuity in case of an incident.

- Establish regular backups of critical data.

3. \*\*Enforce Stronger Password Policies:\*\*

- Require passwords with at least eight characters, a combination of letters, numbers, and special characters.

- Implement a centralized password management system to enforce policies and reduce password fatigue.

4. \*\*Install Intrusion Detection System (IDS):\*\*

- Detects and responds to potential security breaches.

- Monitors network traffic for suspicious activity.

5. \*\*Encrypt Sensitive Data:\*\*

- Ensure confidentiality of customers' credit card information.

- Comply with PCI DSS and GDPR regulations.

6. \*\*Classify and Inventory Data:\*\*

- Enhance data management and protection.

- Ensure data is properly classified and inventoried.

7. \*\*Continue to Enforce Privacy Policies and Data Integrity Measures:\*\*

- Maintain data security and compliance with regulations.

- Protect sensitive information and ensure data accuracy.

By implementing these recommendations, Botium Toys can significantly improve its security posture, ensure compliance with relevant regulations, and mitigate potential risks and vulnerabilities.