Botium Toys - Controls and Compliance Checklist (Editable Version)

This is an editable version of the controls and compliance checklist developed for the internal audit simulation of Botium Toys.  
Use this template to mark whether each control or best practice is currently in place.

# Controls Assessment Checklist

|  |  |  |
| --- | --- | --- |
| Control | Yes | No |
| 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 (alarm, sprinklers, etc.) | ☐ | ☐ |

## PCI DSS (Payment Card Industry Data Security Standard)

|  |  |  |
| --- | --- | --- |
| Best Practice | Yes | No |
| Only authorized users have access to customers’ credit card information. | ☐ | ☐ |
| Credit card info is stored, accepted, processed, and transmitted securely. | ☐ | ☐ |
| Encryption is used for card data and transactions. | ☐ | ☐ |
| Secure password management policies are adopted. | ☐ | ☐ |

## GDPR (General Data Protection Regulation)

|  |  |  |
| --- | --- | --- |
| Best Practice | Yes | No |
| EU customers’ data is kept private/secured. | ☐ | ☐ |
| Notification plan in place for breaches within 72 hours. | ☐ | ☐ |
| Data is properly classified and inventoried. | ☐ | ☐ |
| Privacy policies and procedures are enforced. | ☐ | ☐ |

## SOC Type 1 / Type 2 (System and Organization Controls)

|  |  |  |
| --- | --- | --- |
| Best Practice | Yes | No |
| User access policies are established. | ☐ | ☐ |
| Sensitive data (PII/SPII) is confidential/private. | ☐ | ☐ |
| Data integrity is ensured (consistent, complete, validated). | ☐ | ☐ |
| Data is accessible to authorized individuals only. | ☐ | ☐ |

# Recommendations (Optional)

Use this section to summarize recommendations for controls and compliance best practices to be implemented based on risks identified.