Internal Security Audit Report — Botium Toys

Scope and Goals
Scope: The audit covers the entire security program at Botium Toys, including assets, network, and systems.
Goals: Assess existing assets, controls, and compliance practices to determine which best practices need to be implemented to improve security posture.

Controls Assessment Checklist

Control	Implemented
Least Privilege	No
Disaster Recovery Plans	No
Password Policies	Yes
Separation of Duties	No
Firewall	Yes
Intrusion Detection System (IDS)	No
Backups	No
Antivirus Software	Yes
Manual Monitoring (Legacy Systems)	Yes
Encryption	No
Password Management System	No
Locks (Offices, Storefront, Warehouse)	Yes
CCTV Surveillance	Yes
Fire Detection/Prevention	Yes

Compliance Checklist

PCI DSS
Best Practice	Implemented
Only authorized users have access to credit card info	No
Credit card info is securely stored and transmitted	No
Data encryption for credit card transactions	No
Secure password management policies	No

GDPR
Best Practice	Implemented
EU customers’ data kept private/secure	Yes
72-hour breach notification plan	Yes
Data classification and inventory	No
Enforce privacy policies and processes	Yes

SOC 1 & 2
Best Practice	Implemented
User access policies established	No
Sensitive data remains confidential/private	No
Data integrity ensured	Yes
Data available to authorized users	Yes

Recommendations
1. Implement **least privilege** and **separation of duties** to reduce insider threat risk.
2. Deploy an **IDS** and implement **regular backups** for business continuity.

3. Introduce **encryption** for customer and payment data.
4. Establish a **centralized password management system** aligned with modern standards.
5. Develop **disaster recovery plans** and formal **legacy system maintenance schedules**.
6. Strengthen **PCI DSS compliance** to avoid regulatory fines.