Controls and Compliance Checklist Report - Botium Toys

Controls Assessment Checklist
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: No
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 - 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

Compliance Checklist - GDPR
E.U. customers' data is kept private/secured: Yes
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

Compliance Checklist - 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 Access Controls: Introduce RBAC, least privilege, and separation of duties.
2. Deploy Encryption: Encrypt sensitive customer data at rest and in transit.
3. Establish a Disaster Recovery Plan: Ensure regular data backups are taken and tested.
4. Improve Password Security: Enforce strong password policies with a management system.
5. Install IDS: Improve detection and response capabilities.
6. Monitor Legacy Systems: Set schedules and procedures for system upkeep.
7. Formalize User Access Policies: Align with SOC and GDPR best practices.