Botium Toys Security Audit & Compliance Report

Controls & Compliance Checklist (My Answers)

Administrative & Technical Controls

Control	My Answer
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 of Legacy Systems	Yes
Encryption	No
Password Management System	No
Physical Locks	Yes
CCTV Surveillance	Yes
Fire Detection/Prevention	Yes

PCI DSS Checklist

PCI DSS Best Practice	My Answer
Authorized access only	No
Credit card data stored/processed securely	Yes
Encryption on transaction touchpoints	No
Secure password management policies	No

GDPR Checklist

GDPR Requirement	My Answer

Customer data kept private/secure	No
72-hour breach notification	Yes
Proper data classification	No
Privacy policies enforced	Yes

SOC 1 / SOC 2 Checklist

SOC 1 / SOC 2 Requirement	My Answer
User access policies established	No
Sensitive data confidential/private	No
Data integrity controls	Yes
Authorized access only	No