Controls and compliance checklist

Does Botium Toys currently have this control in place?

Controls assessment checklist

Yes	**No**	**Control**
□	☑	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 (fire alarm, sprinkler system, etc.)

Compliance checklist

Payment Card Industry Data Security Standard (PCI DSS)

Yes	No	Best practice
☐	☑	Only authorized users have access to customers’ credit card information.
☐	☑	Credit card information is stored, accepted, processed, and transmitted internally, in a secure environment.
☐	☑	Implement data encryption procedures to better secure credit card transaction touchpoints and data.
☐	☑	Adopt secure password management policies.

General Data Protection Regulation (GDPR)

Yes	No	Best practice
☐	☑	E.U. customers’ data is kept private/secured.
☑	☐	There is a plan in place to notify E.U. customers within 72 hours if their data is compromised/there is a breach.
☐	☑	Ensure data is properly classified and inventoried.
☑	☐	Enforce privacy policies, procedures, and processes to properly document and maintain data.

System and Organizations Controls (SOC type 1, SOC type 2)

Yes	No	Best practice
☐	☑	User access policies are established.
☐	☑	Sensitive data (PII/SPII) is confidential/private.

☑	☐	Data integrity ensures the data is consistent, complete, accurate, and has been validated.
☑	☐	Data is available to individuals authorized to access it. Note: Authorization should only be limited to those who need it to do their jobs, technically all employees currently have access, therefore are (incorrectly) “authorized” to access it, therefore this is yes

Recommendations:

- Urgent: things to do immediately to prevent further damage
    - Establish and enforce access control policies
        - Least privilege: only allow those who are authorized to view certain data, employees should only have the bare minimum permissions to complete their tasks
    - Encrypt user data to ensure confidentiality
    - Incorporate an intrusion detection system (IDS) into their infrastructure
    - Create a recovery plan and run backups of critical data before they are affected
    - Reset employee passwords and enforce stricter password policies
- Important
    - Implement account management policies; have a centralized password management system
    - Have routine audits of legacy systems following existing frameworks