CONTROLS ASSESSMENT CHECKLIST  
────────────────────────────────────────────────────────

Instructions: For each control, select “Yes” if it is in place or “No” if it is not in place at Botium Toys, based on the scenario.

[ ] Yes [X] No Least Privilege  
→ Not implemented; employees can access all data (including cardholder data).

[ ] Yes [X] No Disaster Recovery Plans  
→ None exist; no backups or documented DR procedures.

[X] Yes [ ] No Password Policies  
→ A nominal policy exists, though it does not meet modern complexity requirements.

[ ] Yes [X] No Separation of Duties  
→ Not implemented; also cited in the scenario as absent.

[X] Yes [ ] No Firewall  
→ Confirmed. The IT department has a firewall blocking unwanted traffic.

[ ] Yes [X] No Intrusion Detection System (IDS)  
→ Not installed.

[ ] Yes [X] No Backups  
→ None in place. No mention of backup routines for critical data.

[X] Yes [ ] No Antivirus Software  
→ Installed and monitored regularly by the IT department.

[X] Yes [ ] No Manual Monitoring, Maintenance, and Intervention for Legacy Systems  
→ Legacy systems are monitored, though the schedule and methodology are unclear.

[ ] Yes [X] No Encryption  
→ Not used to secure cardholder data.

[ ] Yes [X] No Password Management System  
→ No centralized password management solution; resets processed manually by IT.

[X] Yes [ ] No Locks (offices, storefront, warehouse)  
→ Physical facility has sufficient locks.

[X] Yes [ ] No Closed-Circuit Television (CCTV) Surveillance  
→ Up-to-date CCTV is present on the premises.

[X] Yes [ ] No Fire Detection/Prevention (Fire Alarm, Sprinkler System, etc.)  
→ Fire detection and prevention systems are functioning.

────────────────────────────────────────────────────────  
COMPLIANCE CHECKLIST  
────────────────────────────────────────────────────────

PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI DSS)

[ ] Yes [X] No Only authorized users have access to customers’ credit card information.  
→ All employees can currently see credit card data; not restricted by role or privilege.

[ ] Yes [X] No Credit card information is stored, accepted, processed, and transmitted internally, in a secure environment.  
→ No encryption or least privilege; environment is not considered “secure” per PCI standards.

[ ] Yes [X] No Implement data encryption procedures to better secure credit card transaction touchpoints and data.  
→ The company does not use encryption for card data.

[ ] Yes [X] No Adopt secure password management policies.  
→ Current password policy is minimal and no centralized password management exists.

GENERAL DATA PROTECTION REGULATION (GDPR)

[ ] Yes [X] No E.U. customers’ data is kept private/secured.  
→ All employees have access (+ no encryption), so not sufficiently secured.

[X] Yes [ ] No There is a plan in place to notify E.U. customers within 72 hours if their data is compromised.  
→ The IT department has such a plan.

[ ] Yes [X] No Ensure data is properly classified and inventoried.  
→ Assets are not formally classified; employees can freely access data.

[X] Yes [ ] No Enforce privacy policies and procedures to properly document and maintain data.  
→ Privacy policies/procedures exist and are enforced for IT staff (though improvements may be needed).

SYSTEM AND ORGANIZATIONS CONTROLS (SOC 1, SOC 2)

[ ] Yes [X] No User access policies are established.  
→ No robust access controls (least privilege, separation of duties) are in place.

[ ] Yes [X] No Sensitive data (PII/SPII) is confidential/private.  
→ Currently not restricted; effectively viewable by all employees.

[X] Yes [ ] No Data integrity ensures the data is complete, accurate, and validated.  
→ The IT department has integrated controls to ensure data integrity and availability.

[X] Yes [ ] No Data is available to individuals authorized to access it.  
→ Data availability is in place, though “authorized” is loosely defined since nearly all employees have access.

────────────────────────────────────────────────────────  
OPTIONAL: RECOMMENDATIONS  
────────────────────────────────────────────────────────

1. Implement Access Controls and Least Privilege  
   • Restrict who can view or modify credit card and personal data.  
   • Segment duties to improve accountability and reduce the insider threat risk.
2. Deploy Encryption for Sensitive Data  
   • Encrypt credit card data at rest and in transit to meet PCI DSS requirements.  
   • Evaluate full-disk encryption for end-user devices that handle sensitive information.
3. Establish Disaster Recovery (DR) and Backup Procedures  
   • Create and test a robust DR plan to address data loss or corruption scenarios.  
   • Schedule frequent data backups, store them securely (offsite or in the cloud), and test restores.
4. Improve Password Policy and Management  
   • Enforce minimum length, complexity, and rotation requirements aligned to modern standards.  
   • Consider adopting a centralized password management solution to reduce manual reset tickets.
5. Adopt an Intrusion Detection/Prevention System (IDS/IPS)  
   • Enhance network visibility and threat detection for real-time monitoring.  
   • Correlate logs and alerts for faster incident response.
6. Formalize Asset Classification and Inventory  
   • Develop an asset-management plan that identifies and categorizes assets by criticality.  
   • Limit access to the most sensitive data to only those roles that truly require it.