Botium Toys - Security Audit Report

This report summarizes the findings of an internal IT security audit conducted for Botium Toys. The audit follows the NIST Cybersecurity Framework and evaluates controls against compliance requirements including PCI DSS and GDPR.

Control Category	Implemented?	Evidence or Notes	Compliant?
Access Control	No	Admin accounts not protected by MFA; no...	No
Data Security	No	Customer PII is stored without encrypt...	No
Patch Management	Partial	Workstations have outdated software; pa...	No
Incident Response Plan	No	No formal policy exists; team reacts a...	No
Backup & Recovery	Yes	Regular backups are taken and tested mo...	Yes
Network Security	Yes	Firewalls and antivirus are in place; ...	Yes
GDPR Compliance	No	No record of processing activities; no...	No
PCI DSS Compliance	Partial	Cardholder data is transmitted securel...	Partial
Training & Awareness	Partial	Basic training provided, no phishing s...	Partial
Vendor Management	No	No review of third-party services for ...	No

Summary & Recommendations

1. Implement encryption for stored customer data.
2. Enforce MFA and apply role-based access controls.
3. Create a formal incident response plan.
4. Appoint a Data Protection Officer (DPO) and complete GDPR documentation.
5. Fully comply with PCI DSS including securing data storage.
6. Initiate a vendor risk management program.
7. Improve training with phishing simulations and refreshers.