Controls and compliance checklist

Does Botium Toys currently have this control in place?

Controls assessment checklist

Yes	No	Control	Explanation
☐	☑	Least Privilege	Currently, all employees have access to all type of data including PII and SPII
☐	☑	Disaster recovery plans	There are no disaster recovery plans currently in place. This needs to be implemented for business continuity
☐	☑	Password policies	A password policy exists but they are nominal and not in line with the current minimum password complexity requirements and hence need to be implemented
☐	☑	Separation of duties	The separation of duties have not been implemented. And there is a high risk of fraud.
☑	☐	Firewall	Already implemented
☐	☑	Intrusion detection system (IDS)	This needs to be implemented for continue monitoring for potential threats or risk of unauthorised access.
☐	☑	Backups	The company does

			not have backups of critical data. And if a breach may occur, it can impact business continuity.
☑	☐	Antivirus software	Already implemented
☐	☑	Manual monitoring, maintenance, and intervention for legacy systems	The legacy systems are monitored and maintained, there is no regular schedule in place for these tasks and intervention methods are unclear.
☐	☑	Encryption	Customers' card and other information need to be encrypted to provide greater confidentiality of sensitive information.
☐	☑	Password management system	There is no centralized password management system that enforces the password policy's minimum requirements. Which may affect productivity.
☑	☐	Locks (offices, storefront, warehouse)	Already implemented
☑	☐	Closed-circuit television (CCTV) surveillance	Already implemented
☑	☐	Fire detection/prevention (fire alarm, sprinkler system, etc.)	Already implemented

---

Does Botium Toys currently adhere to this compliance best practice?

Compliance checklist

Payment Card Industry Data Security Standard (PCI DSS)

Yes	No	Best practice	Explanation
☐	☑	Only authorized users have access to customers' credit card information.	All Botium Toys employees have access to internally stored data and may be able to access cardholder data and customers' PII/SPII. Which puts the confidentiality at risk.
☐	☑	Credit card information is stored, accepted, processed, and transmitted internally, in a secure environment.	Credit card information is not Encrypted. It is handled locally in the company's internal database.
☐	☑	Implement data encryption procedures to better secure credit card transaction touchpoints and data.	The company does not currently use encryption.
☐	☑	Adopt secure password management policies.	Password policies are nominal, and there is no password management system.

General Data Protection Regulation (GDPR)

Yes	No	Best practice	Explanation
☐	☑	E.U. customers' data is kept private/secure.	The company does not currently use encryption to ensure the confidentiality of customers' Financial information.
☑	☐	There is a plan in place to notify E.U. customers within 72 hours if their data is compromised/there is a breach.	Already implemented
☐	☑	Ensure data is properly classified and inventoried.	
☑	☐	Enforce privacy policies, procedures, and processes to properly document and maintain data.	Already implemented

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

Yes	No	Best practice	Explanation
☐	☑	User access policies are established.	Access controls and separation of duties have not been implemented.
☐	☑	Sensitive data (PII/SPII) is confidential/private.	Does not currently use encryption to ensure confidentiality.
☑	☐	Data integrity ensures the data is consistent, complete, accurate, and has been validated.	The IT department has ensured availability and integrated controls to ensure data integrity.

☐	☑ Data is available to individuals authorized to access it.	Data is available for all employees of the company, and hence puts it at a higher risk of breach.

Recommendations:

- Give employees access only to the systems and data they need for their specific job roles to reduce the risk of unauthorized access.
- Develop a disaster recovery plan to ensure systems and data can be quickly restored in case of emergencies.
- Enforce strong password policies, including regular updates and complexity requirements, to improve account security.
- Assign different roles and responsibilities to separate individuals to reduce the risk of fraud or accidental errors.
- Install an intrusion detection system to monitor network activity and quickly identify suspicious behavior.
- Regularly update and maintain older systems to close security gaps and prevent vulnerabilities.
- Use encryption to protect sensitive information during storage and transmission.
- Introduce a password management system to help employees create and store strong, unique passwords.
- Classify assets based on sensitivity to identify where stronger controls are needed.
- Focus on applying key controls such as least privilege, separation of duties, and encryption to meet compliance requirements and protect data.