Controls and compliance checklist for Botium Toys

Controls assessment checklist

Yes	No	Control	*Explanation*
☐	☑	Least Privilege	*Currently, all employees have access to customer's internally stored data including cardholder data and PII/SPII.*
☐	☑	Disaster recovery plans	*No disaster recovery plan or backups of critical data in place.*
☐	☑	Password policies	*Existing policy in place, however does not adhere to minimum password complexity requirements (e.g. at least eight letters, one number, special characters etc)*
☐	☑	Separation of duties	*Currently not implemented.*
☑	☐	Firewall	*The IT department have implemented a firewall that blocks traffic based on an appropriately defined set of security rules.*
☐	☑	Intrusion detection system (IDS)	*The IT department needs an IDS in place to help identify possible intrusions by threat actors.*
☐	☑	Backups	*The IT department needs to*

			have backups of critical data to ensure business continuity in the case of a breach.
☑	☐	Antivirus software	*Antivirus software is installed and monitored regularly by the IT department.*
☐	☑	Manual monitoring, maintenance, and intervention for legacy systems	*Legacy systems are in use. They are monitored and maintained, however there are no regular schedules in place for these tasks and intervention methods are unclear.*
☐	☑	Encryption	*Encryption is not used to provide confidentiality to the storage of customer's credit card information that is accepted, processed, transmitted and stored locally on the company's internal database.*
☐	☑	Password management system	*There is no password management system currently in place; implementing this control would improve IT department/other employee productivity in the case of password issues by reducing the number of password reset/recoveries submitted by employees or vendors.*
☑	☐	Locks (offices, storefront, warehouse)	*The store's physical location, which includes the company's main offices, store front, and warehouse of products, has sufficient locks.*
☑	☐	Closed-circuit television	*CCTV is installed/functioning*

		(CCTV) surveillance	*at the store's physical location.*
☑	☐	Fire detection/prevention (fire alarm, sprinkler system, etc.)	*Botium Toys' physical location has a functioning fire detection and prevention system.*

Compliance checklist

Select "yes" or "no" to answer the question: *Does Botium Toys currently adhere to this compliance best practice?*

Payment Card Industry Data Security Standard (PCI DSS)

Yes	No	Best practice	***Explanation***
☐	☑	Only authorised users have access to customers' credit card information.	*Currently, all employees have access to the company's internal data.*
☐	☑	Credit card information is accepted, processed, transmitted, and stored internally, in a secure environment.	*Credit card information is not encrypted and all employees currently have access to internal data, including customers' credit card information.*
☐	☑	Implement data encryption procedures to better secure credit card transaction touchpoints and data.	*The company does not currently use encryption to better ensure the confidentiality of customers' financial information.*
☐	☑	Adopt secure password management policies.	*Password policies are nominal and no password management system is currently in place.*

General Data Protection Regulation (GDPR)

Yes	No	Best practice	*Explanation*
☐	☑	E.U. customers' data is kept private/secured.	*The company does not currently use encryption to better 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.	*There is a plan to notify E.U. customers within 72 hours of a data breach.*
☐	☑	Ensure data is properly classified and inventoried.	*Current assets have been inventoried/listed, but not classified.*
☑	☐	Enforce privacy policies, procedures, and processes to properly document and maintain data.	*Privacy policies, procedures, and processes have been developed and enforced among IT team members and other employees, as needed.*

<u>System and Organizations Controls (SOC type 1, SOC type 2)</u>

Yes	No	Best practice	*Explanation*
☐	☑	User access policies are established.	*Controls of Least Privilege and separation of duties are not currently in place; all employees have access to internally stored data.*
☐	☑	Sensitive data (PII/SPII) is confidential/private.	*Encryption is not currently used to better ensure the confidentiality of PII/SPII.*
☑	☐	Data integrity ensures the data is consistent, complete, accurate, and has been validated.	*Data integrity is in place.*

☐	☑	Data is available to individuals authorised to access it.	*While data is available to all employees, authorization needs to be limited to only the individuals who need access to it to do their jobs.*

Recommendations:

Multiple controls need to be introduced to increase Botium Toys' security posture:

- *Least privilege*
- *Disaster recovery plans*
- *Password policies*
- *Separation of duties*
- *An IDS/IPS*
- *Backups of critical data*
- *Schedules and intervention plans for the monitoring and management of legacy systems*
- *Encryption for sensitive data stored on local databases*
- *A password management system*

In order to adhere to compliance best practices, Botium Toys must:

- *Ensure least privilege is adopted so only authorised users have access to PII/SPII*
- *Encrypt all locally stored PII/SPII*
- *Enforce strong password policies and ensure a password management system is in place*
- *Classify all company assets*
- *Enforce separation of duties*