Botium Toys:

Controls and Compliance Checklist

Select “yes” or “no” to answer the question: *Does Botium Toys currently have this control in place?*

Controls assessment checklist

Yes	No	Control	*Explanation*
☐	☑	Least Privilege	*All employees are able to access customer data.*
☐	☑	Disaster recovery plans	*There are no disaster recovery plans in place.*
☐	☑	Password policies	*Password policy is not in line with current minimum password complexity requirements.*
☐	☑	Separation of duties	*Separation of duties not implemented.*
☑	☐	Firewall	
☐	☑	Intrusion detection system (IDS)	*IDS not installed.*
☐	☑	Backups	*No backups of critical data.*
☑	☐	Antivirus software	
☐	☑	Manual monitoring, maintenance, and intervention for legacy systems	No regular schedule in place for *monitoring and maintaining legacy systems.*
☐	☑	Encryption	*Encryption is not currently used.*

☐	☑	Password management system	*No centralized password management system.*
☑	☐	Locks (offices, storefront, warehouse)	
☑	☐	Closed-circuit television (CCTV) surveillance	
☑	☐	Fire detection/prevention (fire alarm, sprinkler system, etc.)	

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 authorized users have access to customers’ credit card information.	*All employees are able to access customer data.*
☐	☑	Credit card information is accepted, processed, transmitted, and stored internally, in a secure environment.	*Credit card information is not encrypted and all employees are able access to customers’ credit card information.*
☐	☑	Implement data encryption procedures to better secure credit card transaction touchpoints and data.	*Encryption is not currently used.*
☐	☑	Adopt secure password management policies.	*Password policy is not in line with current minimum password complexity requirements and*

			there is no centralized password management system.

General Data Protection Regulation (GDPR)

Yes	No	Best practice	***Explanation***
☐	☑	E.U. customers' data is kept private/secured.	*Encryption is not currently used.*
☑	☐	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.	*Data is not classified.*
☑	☐	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	***Explanation***
☐	☑	User access policies are established.	*All employees are able to access customer data.*
☐	☑	Sensitive data (PII/SPII) is confidential/private.	*Encryption is not currently used.*
☑	☐	Data integrity ensures the data is consistent, complete, accurate, and has been validated.	
☐	☑	Data is available to individuals	*All employees are able to*

authorized to access it. *access customer data.*

Recommendations:

This is a list of controls that Botium Toys can implement in order to improve its security posture:

- Principle of Least Privilege
- Disaster recovery plans
- Password policies
- Separation of duties
- IDS
- Scheduled legacy system monitoring and maintenance
- Data encryption
- Password management system

In addition to implementing the controls mentioned above, the company should start accurately classifying its assets. This will enable Botium Toys to identify additional controls required to improve its security posture and safeguard classified assets much more effectively.