Botium Toys: Scope, Goals, and Risk Assessment Report

Best Practice	In Place?	In Place? (n)	Explanation
User access policies are established		X	Controls of Least Privilege and separation of duties are not currently in place
Sensitive data (PII/SPII) is confidential/private		X	PII/SPII and other sensitive data is confidental and private
Data integrity is ensured (complete, accurate, validated)	X		Data Integrity is validated.
Data availability for authorized users	X		Authorized for all users.

Botium Toys: Scope, Goals, and Risk Assessment Report

Best Practice	In Place? (y)	In Place? (n)	Explanation
E.U. customer data is kept private and secure		X	the company doesn't utilize any strong encryption
There's a plan to notify E.U. customers within 72 hours of a breach	X		There's plans to notify customers in case of breach within 72hours
Data is properly classified and inventoried		X	They're inventoried but not classified
Privacy policies and procedures are enforced and documented	X		Both privacy policies and procedures are enforced and documented within this company

Botium Toys: Scope, Goals, and Risk Assessment Report

Yes	No	Best Practice	Explanation
	X	Only authorized users have access to customers' credit card information	No, because all employees have acess to company's data
	X	Credit card info is stored/processed/transmitted in a secure environment	No, credit card info isn't encrypted
	X	Data encryption used at all credit card data touchpoints	Company does not use data encryption at all credit card data touchpoints.
	X	Secure password management policies are adopted	No password policies adopted.

Botium Toys: Scope, Goals, and Risk Assessment Report

Yes	No	Control	Explanation /Recomendation
	X	Least Privelegdge	All employees currently have access to customer data; implement role-based access to limit breaches.
	X	Disaster Recovery Plans	No recovery plans exist; develop and test a disaster recovery strategy to ensure business continuity.
X		Password Policies	Current password requirements are weak; strengthen policies to meet modern security standards.
	X	Separation of Duties	Critical tasks are not divided; establish separation of duties to reduce fraud and insider threats.
X		Firewall	A firewall is in place and effectively filtering malicious traffic.
	X	Intrusion Detection System (IDS)	No IDS implemented; deploy IDS to monitor and detect suspicious network activity.
	X	Backups	No data backups exist; create regular automated backups to prevent data loss.
X		Antivirus Software	Antivirus is active and regularly monitored to protect against malware threats.
X		Manual Monitoring, Maintenance, and Intervention (Legacy Systems)	Legacy systems are monitored but lack a formal schedule; implement regular, documented maintenance.
	X	Encryption	Customer data is unencrypted; introduce encryption for data in transit and at rest.
	X	Password Management System	No centralized management exists; implement a password management system to enforce security policies.
X		Locks (Offices, Storefront, Warehouse)	Physical locks are in place and effectively securing facilities.
X		Closed-Circuit Television (CCTV) Surveillance	CCTV is operational and helps deter and monitor unauthorized physical access.
X		Detection/Prevention (Fire alarm, sprinkler system, etc.)	Fire protection systems are installed and functional to safeguard physical assets.