# Controls and compliance checklist

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

**Controls assessment checklist**

| Yes | No | Control | Explanation |
|---|---|---|---|
| ☐ | ☑ | Least Privilege | All the employees have access to every data no matter the level of secure data. |
| ☐ | ☑ | Disaster recovery plans | There are no recovery plans or backups in case of disaster. |
| ☐ | ☑ | Password policies | Password policy is not in line with minimum password complexity. |
| ☐ | ☑ | Separation of duties | Needs to be implemented to reduce the possibility of fraud/access to critical data, since the company CEO currently runs day-to-day operations and manages the payroll. |
| ☑ | ☐ | Firewall | The existing firewall blocks traffic based on an appropriately defined set of security rules. |
| ☐ | ☑ | Intrusion detection system (IDS) | There needs to be IDS installed in order to regularly monitor and identify potential intrusions. |
| ☐ | ☑ | Backups | The IT department needs to have backups of critical data, in the case of a breach, to ensure business continuity. |

| | | | |
|---|---|---|---|
| ☑ | ☐ | Antivirus software | The IT department has antivirus installed. |
| ☑ | ☐ | Manual monitoring, maintenance, and intervention for legacy systems | There is not a regular schedule in place for this task and procedures/ policies related to intervention are unclear, which could place these systems at risk of a breach. |
| ☐ | ☑ | Encryption | Encryption is not currently used. |
| ☐ | ☑ | Password management system | There is no password management system currently in place. |
| ☑ | ☐ | 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) surveillance | CCTV is installed/functioning at the store's physical location. |
| ☑ | ☐ | Fire detection/prevention (fire alarm, sprinkler system, etc.) | The company has a working fire detection and prevention system. |

---

**Compliance checklist**

*Type an X in the "yes' ' or "no' ' column to answer the question: Does Botium Toys currently adhere to this compliance best practices?*

Payment Card Industry Data Security Standard (PCI DSS)

| Yes | No | Best practice | Explanation |
|---|---|---|---|
| ☐ | ☑ | Only authorized users have access to customers' credit card information. | Currently, all employees have access to the company's internal data. |
| ☐ | ☑ | Credit card information is stored, accepted, processed, and transmitted 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 |
|---|---|---|
| ☐ | ☑ | E.U. customers' data is kept private/secured. |
| ☑ | ☐ | 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. |
| ☐ | ☑ | 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 |
|---|---|---|

- [ ] [x] User access policies are established.
- [ ] [x] Sensitive data (PII/SPII) is confidential/private.
- [ ] [x] Data integrity ensures the data is consistent, complete, accurate, and has been validated.
- [x] [ ] Data is available to individuals authorized to access it.

---