**CONTROL AND COMPLIANCE CHECK LIST FOR BOTIUM TOYS**

The letter X indicates “yes” or “no” column to answer the question: *If Botium Toys currently adhere to this compliance best practice?*

**CONTROLS ASSESSMENT CHECKLIST**

|  |  |  |  |
| --- | --- | --- | --- |
| **Yes** | **No** | **Control** | ***Explanation*** |
|  | X | Least Privilege | *Currently, all employees have access to customer data; privileges need to be limited to reduce the risk of a breach.* |
|  | X | Disaster recovery plans | *There are no disaster recovery plans in place. These need to be implemented to ensure business continuity.* |
|  | X | Password policies | *Employee password requirements are minimal, which could allow a threat actor to more easily access secure data/other assets via employee work equipment/the internal network.* |
|  | X | 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.* |
| X |  | Firewall | *The existing firewall blocks traffic based on an appropriately defined set of security rules.* |
|  |  |  |  |
|  | X | Intrusion detection system (IDS) | *The IT department needs an IDS in place to help identify possible intrusions by threat actors.* |
|  | X | Backups | *The IT department needs to have backups of critical data, in the case of a breach, to ensure business continuity.* |
| X |  | Antivirus software | *Antivirus software is installed and monitored regularly by the IT department.* |
|  | X | Manual monitoring, maintenance, and intervention for legacy systems | *The list of assets notes the use of legacy systems. The risk assessment indicates that these systems are monitored and maintained, but 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.* |
|  | X | Encryption | *Encryption is not currently used; implementing it would provide greater confidentiality of sensitive information.* |
|  | X | 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.* |

|  |  |  |  |
| --- | --- | --- | --- |
| X |  | 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.* |
| X |  | Closed-circuit television (CCTV) surveillance | *CCTV is installed/functioning at the store’s physical location.* |
| X |  | Fire detection/prevention (fire alarm, sprinkler system, etc.) | *Botium Toys’ physical location has a functioning fire detection and prevention system.* |

**COMPLIANCE CHECKLIST**

**PAYMENT CARD INDUSTRY DATA SECURITY STANDARD**

|  |  |  |  |
| --- | --- | --- | --- |
| **Yes** | **No** | **Best practice** | ***Explanation*** |
|  | X | Only authorized users have access to customers’ credit card information. | *Currently, all employees have access to the company’s internal data.* |
|  | X | 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.* |
|  | X | 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.* |
|  | X | Adopt secure password management policies. | *Password policies are nominal and no password management system is currently in place.* |

**GENERAL DATA PROTECTION REGULATION**

|  |  |  |  |
| --- | --- | --- | --- |
| **Yes** | **No** | **Best practice** | ***Explanation*** |
|  | X | E.U. customers’ data is kept private/secured. | *The company does not currently use encryption to better ensure the confidentiality of customers’ financial information.* |
| X |  | 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.* |
|  | X | Ensure data is properly classified and inventoried. | *Current assets have been inventoried/listed, but not classified.* |
| X |  | 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.* |

**SYSTEM AND ORGANIZATIONS CONTROLS**

|  |  |  |  |
| --- | --- | --- | --- |
| **Yes** | **No** | **Best practice** | ***Explanation*** |
|  | X | 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.* |
|  | X | Sensitive data (PII/SPII) is confidential/private. | *Encryption is not currently used to better ensure the confidentiality of PII/SPII.* |
| X |  | Data integrity ensures the data is consistent, complete, accurate, and has been validated. | *Data integrity is in place.* |
|  | X | Data is available to individuals authorized 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.* |

**CONCLUSION AND RECOMMENDATIONS**

From the audit done, Botium Toys need to put some compliance and implement some security measures to improve its security and ensure confidentiality.