**Compliance Controls and Checklist**

*To complete the controls assessment checklist, refer to the information provided in the scope, targets, and risk assessment report. For more details about each control, including the type and purpose, see the control categories document.*

*Then type in the "yes" or "no" column to answer the question: Does Botium Toys currently have this control?*

**Controls Assessment Checklist**

|  |  |
| --- | --- |
| **Answer** | **Control** |
| No | Least Privilege |
| No | Disaster recovery plans |
| No | Password Policies |
| No | Separation of duties |
| Yes | Firewall |
| No | Intrusion Detection System (IDS) |
| No | Backups |
| Yes | Anti-Virus Software |
| No | Manual monitoring, maintenance, and intervention for legacy systems |
| No | Encryption |
| No | Password management system |
| Yes | Locks (offices, storefront, warehouse) |
| Yes | Closed Circuit Television (CCTV) Surveillance |
| Yes | Fire detection/prevention (fire alarm, sprinkler system, etc.) |

*To complete the compliance checklist, refer to the information provided in the scope, goals, and risk assessment report. For more details on each compliance regulation, review the controls, frameworks, and compliance reading.*

*Then, type in the "yes" or "no" column to answer the question: Does Botium Toys currently adhere to this compliance best practice?*

**Compliance checklist**

Payment Card Industry Data Security Standard (PCI DSS)

|  |  |
| --- | --- |
| **Answer** | **Best Practices** |
| No | Only authorized users have access to customers' credit card information |
| No | Credit card information is stored, accepted, processed, and transmitted internally in a secure environment |
| No | Implementing data encryption procedures to better protect touchpoints and credit card transaction data |
| No | Adopting secure password management policies |

General Data Protection Regulation (GDPR)

|  |  |
| --- | --- |
| **Answer** | **Best Practices** |
| Yes | EU customer data is kept private/protected. |
| Yes | There is a plan in place to notify EU customers within 72 hours if their data is compromised/there is a breach. |
| No | Certification that the data is properly classified and inventoried. |
| No | Enforcing privacy policies, procedures, and processes to properly document and maintain data. |

Systems and Organization Controls (SOC Type 1, SOC Type 2)

|  |  |
| --- | --- |
| **Answer** | **Best Practices** |
| No | User access policies are established. |
| No | Sensitive data (PII/SPII) is sensitive/private. |
| Yes | Data integrity ensures that data is consistent, complete, accurate, and validated. |
| No | The data is available to individuals authorized to access it. |

*This section is optional and can be used to provide a summary of recommendations to the IT manager on what compliance controls and/or best practices Botium Toys needs to implement, based on the risk posed if not implemented in a timely manner.*

**Recommendations (optional):**

Botium Toys' customer data is not receiving proper handling and is severely exposed to leaks by internal or external attackers.

Because there are several security breaches, there is no compliance with current laws, and in the imminent case of a leak of data stored by the company, there are multiple negative impacts resulting from these failures:

* damage to the company's reputation and image, as well as loss of trust
* financial impacts due to business continuity disruption, error correction costs, loss of customers
* government-enforced fines and sanctions
* lawsuits filed by customers in the event of PII and SPII data leaks that may lead to identity theft and fraud

Insider Threat Prevention

Adopting the control of least privilege and separation of duties for Botium Toys employees are measures that mitigate possible compromise by internal actions, as they limit data access only to those who really need it.

External Threat Prevention

Despite having a firewall and antivirus software maintained and monitored by the IT department, Botium Toys is exposed to external attackers who have a higher level of knowledge, due to the lack of more defense mechanisms. Recommended measures to address these vulnerabilities are:

* encryption applied to the customers’ stored data and company's industrial secrets data
* implementation of an intrusion detection system (IDS)
* greater rigor in the rules for creating passwords for employees, requiring a minimum of 8 characters, with at least one in upper case, one in lower case, one numeral and one special character, and the adoption of multifactorial validation
* define and apply a fixed schedule for monitoring legacy systems until they are completely replaced, which is highly recommended and should be done as soon as possible
* implementing of a data backup, even if it has defense mechanisms against fire and intrusion, hardware defects are unpredictable and can occur without warning, a backup stored in the cloud, on a reliable server, ensures that data can be recovered, whether by hardware loss, ransomware or any virus that may compromise its availability.