# Controls and compliance checklist

**Controls assessment checklist**

|  |  |  |
| --- | --- | --- |
| **Yes** | **No** | **Control** |
|  | ✔ | Least Privilege |
|  | ✔ | Disaster recovery plans |
|  | ✔ | Password policies |
|  | ✔ | Separation of duties |
| ✔ |  | Firewall |
|  | ✔ | Intrusion detection system (IDS) |
|  | ✔ | Backups |
| ✔ |  | Antivirus software |
|  | ✔ | Manual monitoring, maintenance, and intervention for legacy systems |
|  | ✔ | Encryption |
|  | ✔ | Password management system |
| ✔ |  | Locks (offices, storefront, warehouse) |
| ✔ |  | Closed-circuit television (CCTV) surveillance |
| ✔ |  | Fire detection/prevention (fire alarm, sprinkler system, etc.) |

**Compliance checklist**

Payment Card Industry Data Security Standard (PCI DSS)

|  |  |  |
| --- | --- | --- |
| **Yes** | **No** | **Best practice** |
|  | ✔ | Only authorized users have access to customers’ credit card information. |
|  | ✔ | Credit card information is stored, accepted, processed, and transmitted internally, in a secure environment. |
|  | ✔ | Implement data encryption procedures to better secure credit card transaction touchpoints and data. |
|  | ✔ | Adopt secure password management policies. |

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** |
|  | ✔ | User access policies are established. |
|  | ✔ | Sensitive data (PII/SPII) is confidential/private. |
| ✔ |  | Data integrity ensures the data is consistent, complete, accurate, and has been validated. |
|  | ✔ | 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 regarding which controls and/or compliance best practices Botium Toys needs to implement, based on the risk posed if not implemented in a timely manner.

**Recommendations:**

**1. Controls Implementation Recommendations**

* **Least Privilege**: Implement the principle of least privilege across all systems and applications to ensure users have only the minimum access necessary to perform their duties. This reduces the risk of unauthorized access or accidental misuse.
* **Backups**: Ensure regular and secure backups of critical data are performed and tested for reliability. This will mitigate risks associated with data loss due to system failures, cyberattacks, or disasters.
* **Encryption**: Strengthen encryption practices for data at rest and in transit, particularly for sensitive information such as customer data and payment details. This will protect against data breaches and unauthorized access.
* **Intrusion Detection System (IDS)**: Regularly update and monitor the IDS to detect and respond to potential threats in real-time. This will help identify and mitigate security incidents before they escalate.
* **Manual Monitoring for Legacy Systems**: Develop a plan to phase out legacy systems or implement automated monitoring tools to reduce the risk of human error and improve efficiency.

**2. Compliance Recommendations**

* **Payment Card Industry Data Security Standard (PCI DSS)**:
  + Ensure that only authorized personnel have access to customers’ credit card information. Regularly review and update access controls.
  + Conduct periodic audits to verify that credit card data is stored, processed, and transmitted securely.
  + Enhance encryption protocols for all credit card transaction touchpoints to meet PCI DSS requirements.
* **General Data Protection Regulation (GDPR)**:
  + Develop and maintain a comprehensive data classification and inventory system to ensure E.U. customers' data is properly managed and secured.
  + Regularly test the breach notification plan to ensure compliance with the 72-hour notification requirement in the event of a data breach.
  + Review and update privacy policies and procedures to ensure they align with GDPR requirements and are consistently enforced.
* **System and Organizations Controls (SOC Type 1, SOC Type 2)**:
  + Establish and enforce user access policies to ensure sensitive data (PII/SPII) remains confidential and private.
  + Implement data validation processes to ensure data integrity, consistency, and accuracy.
  + Regularly review access controls to ensure data is available only to authorized individuals.

**3. General Recommendations**

* **Risk Assessment Updates**: Conduct regular risk assessments to identify new threats and vulnerabilities, and update controls and compliance practices accordingly.
* **Employee Training**: Provide ongoing security awareness training to employees to ensure they understand and adhere to security policies and procedures.
* **Third-Party Vendor Management**: Ensure that third-party vendors comply with Botium Toys' security and compliance standards, particularly those handling sensitive data.
* **Incident Response Plan**: Develop and test an incident response plan to ensure the organization is prepared to respond effectively to security incidents or breaches.