|  |  |  |  |
| --- | --- | --- | --- |
| Yes  **Botium Toys Internal Audit-Controls and Compliance Checklist**  **Controls Assessment Checklist:** | No | Control | Explanation |
|  | X | Least Privilege | All employees have access to customer data. Access must be limited to reduce breach risks. |
|  | X | Disaster Recovery Plans | No recovery plans exist. Needed to ensure business continuity during incidents. |
|  | X | Password Policies | Current password requirements are weak, making systems vulnerable to brute force attacks. |
|  | X | Separation of Duties | The CEO manages both operations and payroll—segregation needed to reduce fraud risk. |
| X |  | Firewall | A firewall is in place and configured with security rules. |
|  | X | Intrusion Detection System (IDS) | No IDS is implemented. Necessary to detect potential intrusions. |
|  | X | Backups | No mention of regular data backups. Needed to recover from breaches or hardware failure. |
| X |  | Antivirus Software | Antivirus software is installed and monitored. |
|  | X | Manual Monitoring for Legacy Systems | Legacy systems are monitored manually but not on a defined schedule, which increases risk. |
|  |  |  | No encryption is used. Implementing it will improve data confidentiality. |
|  | X | Encryption |  |
|  |  | Password Management System | Not in place. Would help employees and IT with secure password practices. |
| X |  | Locks (Physical Security) | Offices, storefront, and warehouse are physically secure with locks. |
| X |  | CCTV Surveillance | CCTV is installed and operational. |
| X |  | Fire Detection/Prevention | Systems like alarms and sprinklers are in place and working. |

**Compliance Checklist:  
PCI DSS:**

|  |  |  |  |
| --- | --- | --- | --- |
| Yes | No | Best Practice | Explanation |
|  | X | Only authorized users have access to credit card info | Currently, all employees can access sensitive data. |
|  | X | Credit card info is securely stored | Data isn’t encrypted and is accessible by all employees. |
|  | X | Data encryption is implemented | Encryption is not currently used to protect credit card data. |
|  | X | Password management policies exist | Weak passwords and no management system increase risk. |

**GDPR:**

|  |  |  |  |
| --- | --- | --- | --- |
| Yes | No | Best Practice | Explanation |
|  | X | E.U. customer data is secured | No encryption for EU data; confidentiality is not guaranteed. |
| X |  | Breach notification plan in place | There is a plan to notify EU customers within 72 hours. |
|  | X | Data is classified and inventoried | Assets are inventoried but not formally classified. |
| X |  | Privacy policies are enforced | IT staff follow enforced privacy policies. |

**SOC 1 & 2:**

|  |  |  |  |
| --- | --- | --- | --- |
| Yes | No | Best Practice | Explanation |
|  | X | User access policies are enforced | No Least Privilege or separation of duties exist. |
|  | X | PII/SPII is protected | No encryption is used to protect sensitive personal information. |
| X |  | Data integrity is maintained | Data is consistent and validated. |
|  | X | Data is only available to authorized users | All employees currently have access. This needs to be restricted. |

**Recommendations:**

To improve Botium Toys’ security posture and compliance:

* Implement access controls (Least Privilege, Separation of Duties).
* Encrypt sensitive data, especially customer and payment information.
* Create a Disaster Recovery Plan and schedule regular backups.
* Set up an IDS to detect suspicious activities.
* Establish and enforce strong password policies and implement a password management system.
* Classify assets for better visibility and prioritization of security measures.
* Continue enforcing physical security measures like CCTV and fire systems.