Controls and compliance checklist exemplar

*Does Botium Toys currently have this control in place?*

**Controls assessment checklist**

|  |  |  |  |
| --- | --- | --- | --- |
| **Yes** | **No** | **Control** | ***Explanation*** |
|  | X | Least Privilege | *All employees currently have unrestricted access to customer data. Access rights should be minimized to only what is necessary for each role to reduce the risk of data breaches.* |
|  | X | Disaster recovery plans | *No formal disaster recovery strategy exists. A documented plan is essential to ensure operations can resume quickly after an unexpected event.* |
|  | X | Password policies | *Existing password requirements are weak, increasing the likelihood of unauthorized access through compromised employee accounts. Stronger password rules are needed.* |
|  | X | Separation of duties | *Critical tasks are not divided among different individuals. For example, the CEO manages daily operations and payroll, which increases the risk of fraud. Segregating duties is necessary for internal control.* |
| X |  | Firewall | *The current firewall is active and effectively filters network traffic based on well-defined security rules.* |
|  |  |  |  |
|  | X | Intrusion detection system (IDS) | *There is no IDS in place to detect malicious activity on the network. Implementing one would help monitor and alert for potential intrusions.* |
|  | X | Backups | *Regular data backups are not in place. Implementing this control is crucial for recovering important information in case of a cyberattack or data loss.* |
| X |  | Antivirus software | *Antivirus tools are installed and actively monitored by the IT team, providing a basic layer of protection against malware.* |
|  | X | Manual monitoring, maintenance, and intervention for legacy systems | *Although legacy systems are listed as assets, there's no consistent schedule or defined procedures for maintaining them. This increases their vulnerability to threats.* |
|  | X | Encryption | *Sensitive data is not currently encrypted. Adding encryption would enhance the confidentiality and security of customer and business information.* |
|  | X | Password management system | *There is no centralized system to manage passwords. Adopting one would simplify secure password handling and reduce related IT support issues.* |
| X |  | Locks (offices, storefront, warehouse) | |  | | --- | |  |  |  | | --- | | *The office, storefront, and warehouse are properly secured with locks, providing adequate physical access control.* | |
| X |  | Closed-circuit television (CCTV) surveillance | *CCTV systems are in place and operational, ensuring surveillance of the company's physical premises.* |
| X |  | Fire detection/prevention (fire alarm, sprinkler system, etc.) | *The facility is equipped with fire alarms and sprinkler systems, ensuring basic fire safety compliance.* |

**Compliance checklist**

Type an X in the “yes” or “no” column to answer the question: *Does Botium Toys currently adhere to this compliance best practice?*

Payment Card Industry Data Security Standard (PCI DSS)

|  |  |  |  |
| --- | --- | --- | --- |
| **Yes** | **No** | **Best practice** | ***Explanation*** |
|  | X | Only authorized users have access to customers’ credit card information. | *All staff currently have access to internal data, including credit card information. This violates the principle of restricting access to authorized personnel only.* |
|  | X | Credit card information is accepted, processed, transmitted, and stored internally, in a secure environment. | *Cardholder data is not encrypted and is accessible to all employees. A secure environment for processing and storing this information is necessary.* |
|  | X | Implement data encryption procedures to better secure credit card transaction touchpoints and data. | *No encryption is applied to transaction data. This leaves credit card information vulnerable to interception and misuse.* |
|  | X | Adopt secure password management policies. | *Passwords are not governed by a strict policy, and no management tool exists. A secure password framework is essential for protecting customer data.* |

General Data Protection Regulation (GDPR)

|  |  |  |  |
| --- | --- | --- | --- |
| **Yes** | **No** | **Best practice** | ***Explanation*** |
|  | X | E.U. customers’ data is kept private/secured. | *Customer data, especially from the E.U., is not encrypted, compromising its confidentiality.* |
| 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 procedure in place to inform affected E.U. customers within 72 hours in the event of a data breach.* |
|  | X | Ensure data is properly classified and inventoried. | |  |  | | --- | --- | |  | | |  |  |  | | --- | | *Assets have been inventoried, but data has not been categorized according to sensitivity or function. Classification is necessary for proper data handling.* | |
| X |  | Enforce privacy policies, procedures, and processes to properly document and maintain data. | *Policies related to data protection are in place and followed by both IT and relevant staff.* |

System and Organizations Controls (SOC type 1, SOC type 2)

|  |  |  |  |
| --- | --- | --- | --- |
| **Yes** | **No** | **Best practice** | ***Explanation*** |
|  | X | User access policies are established. | *Access controls are not implemented — all employees can view sensitive company data. This conflicts with least privilege and duty separation principles.* |
|  | 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. | *Controls exist to ensure that business data is complete, consistent, and accurate.* |
|  | X | Data is available to individuals authorized to access it. | *While data is accessible, it is not restricted to only authorized personnel. This overexposure increases the risk of data leaks or unauthorized actions.* |

**Security Audit Recommendations for Botium Toys**

**1. Access Control**

* Implement Least Privilege: Restrict access to customer and internal data based on role requirements to minimize data exposure.
* Establish User Access Policies: Define and enforce access permissions for systems, applications, and databases.
* Introduce Role-Based Access Control (RBAC): Ensure only authorized personnel can access sensitive resources.

**2. Network & System Security**

* Deploy an Intrusion Detection System (IDS): Monitor network traffic to detect suspicious activities in real time.
* Regularly Update Antivirus Software: Keep antivirus definitions up to date and run periodic scans.
* Enhance Firewall Rules: Review and update firewall configurations to align with current threat landscapes.
* Implement Encryption: Use encryption for sensitive data at rest and in transit to protect confidentiality and integrity.

**3.** Data Protection & Compliance

* Encrypt Customer & Financial Data: Especially credit card info, to meet PCI DSS requirements.
* Implement a Password Management System: Provide secure, centralized credential storage and enable strong password policies.
* Comply with GDPR:
  + Classify and inventory customer data.
  + Ensure privacy policies are enforced across departments.
  + Maintain breach notification plans and test them regularly.

**4. Operational Security**

* Establish a Disaster Recovery Plan: Define procedures for data recovery and business continuity in case of system failures or breaches.
* Enforce Separation of Duties: Assign financial and operational responsibilities to different staff members to reduce fraud risk.
* Document IT Policies & Procedures: Maintain clear SOPs for data handling, backups, system maintenance, and incident response.

**5. Physical Security**

* Maintain Physical Security Controls: Ensure locks, CCTV, and fire detection systems are functional and routinely checked.
* Restrict Physical Access: Limit access to server rooms and sensitive physical records to authorized personnel only.

**6. System Maintenance**

* Schedule Regular Maintenance for Legacy Systems: Create and follow a maintenance calendar and define clear intervention protocols.
* Back Up Data Regularly: Automate backups and store them off-site or in the cloud to prevent data loss.

**Optional (but Valuable):**

* Conduct Regular Security Awareness Training: Educate employees on phishing, social engineering, and secure behavior.
* Run Annual Penetration Testing: Identify vulnerabilities in network infrastructure before attackers do.