Internal Security Audit Report: Botium Toys

# Controls and Compliance Checklist

## Controls Assessment

|  |  |  |
| --- | --- | --- |
| Control | In Place? | Notes |
| Least Privilege | No | Access permissions should be assigned based on job roles. |
| Disaster Recovery Plans | No | Disaster recovery and business continuity planning is needed. |
| Password Policies | No | Existing password policies are outdated and weak. |
| Separation of Duties | No | Critical tasks should be split among multiple users. |
| Firewall | Yes | Configured with security rules to block unwanted traffic. |
| Intrusion Detection System (IDS) | No | IDS should be implemented to monitor for malicious activity. |
| Backups | No | Data backups are currently not in place – high risk. |
| Antivirus Software | Yes | Antivirus is active and monitored by the IT team. |
| Manual Monitoring (Legacy Systems) | No | No regular schedule or clear procedures for legacy systems. |
| Encryption | No | Data encryption is not in place for sensitive information. |
| Password Management System | No | No centralized system for enforcing password policies. |
| Physical Locks | Yes | Locks in place for office, storefront, and warehouse. |
| CCTV Surveillance | Yes | Surveillance systems are functional and up to date. |
| Fire Detection/Prevention | Yes | Fire alarms and prevention systems are operational. |

# Compliance Assessment

## PCI DSS

|  |  |  |
| --- | --- | --- |
| Best Practice | In Place? | Notes |
| Only authorized users have access to credit card info | No | All employees currently have access to sensitive data. |
| Secure storage, processing, and transmission of credit card data | No | Credit card info is locally stored without encryption. |
| Data encryption procedures | No | Encryption is not being used for transaction data. |
| Secure password management policies | No | Policies exist but are weak and not enforced. |

## GDPR

|  |  |  |
| --- | --- | --- |
| Best Practice | In Place? | Notes |
| EU customers' data is secure | Yes | Privacy policies are implemented. |
| Breach notification plan within 72 hours | Yes | Notification plan is in place. |
| Data classification and inventory | No | No formal classification process implemented. |
| Enforced privacy policies and documentation | Yes | Data handling procedures are followed. |

## SOC 1/2

|  |  |  |
| --- | --- | --- |
| Best Practice | In Place? | Notes |
| User access policies | No | Lack of clearly defined user access controls. |
| Sensitive data confidentiality | No | PII/SPII is accessible to all employees. |
| Data integrity ensured | Yes | Integrity controls are present. |
| Authorized data access | No | Data access is overly permissive. |

# Recommendations to IT Manager (Optional)

Botium Toys currently has a high-risk security posture, with a risk score of 8/10. Immediate steps should be taken to:  
- Implement least privilege and separation of duties to limit unnecessary access.  
- Deploy an Intrusion Detection System (IDS) to detect suspicious activities.  
- Encrypt sensitive data, especially credit card information, to meet PCI DSS compliance.  
- Strengthen password policies and introduce a centralized password management system.  
- Initiate regular backups and establish a disaster recovery plan.  
  
These measures will reduce risk, improve compliance, and enhance the overall security posture of the organization.