Security Audit for Botium Toys

# Step 1: Review Current Assets and Risks

Assets: On-premises equipment, employee devices, storefront products, internet access, internal network, data storage, and legacy systems.  
  
Key Risks:  
- Inadequate asset management.  
- No use of encryption for credit card data.  
- Lack of least privilege and separation of duties.  
- No disaster recovery plans or backups.  
- Outdated password policies with no centralized password management system.  
- Absence of intrusion detection systems (IDS).  
- Legacy systems are not properly scheduled for monitoring.  
- Compliance issues, especially with U.S. and international regulations (PCI DSS, GDPR, SOC).

# Step 2: Perform the Controls Assessment

|  |  |  |
| --- | --- | --- |
| Control | Yes | No |
| Least Privilege |  | No |
| Disaster recovery plans |  | No |
| Password policies | Yes (but outdated) |  |
| Separation of duties |  | No |
| Firewall | Yes |  |
| Intrusion detection system (IDS) |  | No |
| Backups |  | No |
| Antivirus software | Yes |  |
| Manual monitoring of legacy systems | Yes (but not scheduled) |  |
| Encryption |  | No |
| Password management system |  | No |
| Locks (offices, storefront, warehouse) | Yes |  |
| CCTV surveillance | Yes |  |
| Fire detection/prevention systems | Yes |  |

# Step 3: Perform the Compliance Assessment

|  |  |  |
| --- | --- | --- |
| Compliance Standard | Yes | No |
| PCI DSS: Only authorized users access cardholder data |  | No |
| PCI DSS: Credit card info is stored securely |  | No |
| PCI DSS: Data encryption in place |  | No |
| GDPR: E.U. customers’ data is secured | Yes |  |
| GDPR: Plan to notify within 72 hours of breach | Yes |  |
| SOC: User access policies are established |  | No |
| SOC: Sensitive data confidentiality |  | No |

# Step 4: Provide Recommendations

1. Implement Encryption: Encrypt all credit card data and sensitive PII to comply with PCI DSS and improve confidentiality.  
2. Upgrade Password Policies: Enforce stronger password complexity and introduce a centralized password management system to enhance security and compliance.  
3. Establish Disaster Recovery Plans and Backups: Implement disaster recovery strategies and regular data backups to ensure business continuity.  
4. Install an Intrusion Detection System (IDS): This will help detect any unauthorized access or anomalous network activity.  
5. Enforce Least Privilege and Separation of Duties: Restrict user access to sensitive information, reducing insider threats and improving compliance with SOC standards.  
6. Schedule Regular Monitoring for Legacy Systems: Set up a consistent monitoring and maintenance schedule for end-of-life systems to reduce vulnerabilities.  
7. Enhance Compliance with PCI DSS: Ensure that only authorized personnel have access to cardholder data and that secure storage and encryption measures are in place.