Controls and compliance checklist

Checklist based on [scope, goals, and risk assessment report](https://docs.google.com/document/d/1s2u_RuhRAI40JSh-eZHvaFsV1ZMxcNSWXifHDTOsgFc/template/preview#heading=h.evidx83t54sc) from the *Botium Toys: Scope, goals, and risk assessment report.*

**Controls assessment checklist**

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

**Compliance checklist**

Payment Card Industry Data Security Standard (PCI DSS)

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

General Data Protection Regulation (GDPR)

|  |  |  |
| --- | --- | --- |
| **Yes** | **No** | **Best practice** |
|  | X | E.U. customers’ data is kept private/secured. |
| X |  | There is a plan in place to notify E.U. customers within 72 hours if their data is compromised/there is a breach. |
|  | X | Ensure data is properly classified and inventoried. |
| X |  | 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** |
|  | X | User access policies are established. |
|  | X | Sensitive data (PII/SPII) is confidential/private. |
| X |  | Data integrity ensures the data is consistent, complete, accurate, and has been validated. |
| X |  | Data is available to individuals authorized to access it. |

**Recommendations :**

* To adress some security issues in Botium Toys Security posture, we recomend the following:  
   Implement User access policies and controls for Acess Management: Role Based Acess Management, Mandatory Acess Management or Discritory Acess Management. to ensure the only people authorize can acess sensitive data.  
  Encryption of Dana in all states: At rest, in Use or in Motion.
* Aplying Separation of duties and least privilage principals.
* Estableshy Bussiness Countinuity Plan(BCP) and Disastrer recovery plan(DRP).with backups as part of DRP.
* Reinforce Password polices with more complex requiriments And implement a centralized Password Management system to help productivity when employees/vendors submit a ticket to the IT department to recover or reset a password.
* Implement Next Genaration Firewall with have IDS built-in.  
  Use one secure envirioment to ensure credit card information is store, accepted, processed, and transmitted internally on a secure way.
* Make periodically Assets Invetory as well categorize and labeling assets in the process.