# Controls and compliance checklist

Type an X in the “yes” or “no” column to answer the question: *Does Botium Toys currently have this control in place?*

**Controls assessment checklist**

|  |  |  |  |
| --- | --- | --- | --- |
| **Yes** | **No** | **Control** | ***Explanation*** |
|  | X | Least Privilege | |  | | --- | | *Everyone sees data need restrict access.* |  |  | | --- | |  | |
|  | X | Disaster recovery plans | |  | | --- | | *No plans, we need to add recovery steps.* |  |  | | --- | |  | |
|  | X | Password policies | |  | | --- | | *Weak passwords, enforce need stronger ones.* |  |  | | --- | |  | |
|  | X | Separation of duties | |  | | --- | | *CEO does everything, need to split roles.* |  |  | | --- | |  | |
| X |  | Firewall | *blocks traffic* |
|  |  |  |  |
|  | X | Intrusion detection system (IDS) | |  | | --- | | *No IDS, need to install one.* |  |  | | --- | |  | |
|  | X | Backups | |  | | --- | | *Need backups* |  |  | | --- | |  | |
| X |  | Antivirus software | |  | | --- | | *Installed and regularly monitored.* |  |  | | --- | |  | |
|  | X | Manual monitoring, maintenance, and intervention for legacy systems | |  | | --- | | *Unscheduled checks, unclear policies.* |  |  | | --- | |  | |
|  | X | Encryption | |  | | --- | | *No encryption; must add it.* |  |  | | --- | |  | |
|  | X | Password management system | |  | | --- | | *None yet have to implement one .* |  |  | | --- | |  | |
| X |  | Locks (offices, storefront, warehouse) | *The office is secured with locks* |
| X |  | Closed-circuit television (CCTV) surveillance | *All the cameras work.* |
| X |  | Fire detection/prevention (fire alarm, sprinkler system, etc.) | *Fire system works.* |

**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 employees access data freely.* |  |  | | --- | |  | |
|  | X | Credit card information is accepted, processed, transmitted, and stored internally, in a secure environment. | |  | | --- | | *No encryption all the data is open to all.* |  |  | | --- | |  | |
|  | X | Implement data encryption procedures to better secure credit card transaction touchpoints and data. | *No encryption needs to be added.* |
|  | X | Adopt secure password management policies. | *Weak passowords and bad management.* |

General Data Protection Regulation (GDPR)

|  |  |  |  |
| --- | --- | --- | --- |
| **Yes** | **No** | **Best practice** | ***Explanation*** |
|  | X | E.U. customers’ data is kept private/secured. | *No encryption nothing is private* |
| X |  | There is a plan in place to notify E.U. customers within 72 hours if their data is compromised/there is a breach. | *No plan to notify within 72 hrs.* |
|  | X | Ensure data is properly classified and inventoried. | *Listed but not classified.* |
| X |  | Enforce privacy policies, procedures, and processes to properly document and maintain data. | *Have privacy policies and follow it* |

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

|  |  |  |  |
| --- | --- | --- | --- |
| **Yes** | **No** | **Best practice** | ***Explanation*** |
|  | X | User access policies are established. | *Everyone has access* |
|  | X | Sensitive data (PII/SPII) is confidential/private. | *Plans exist for quick notice* |
| X |  | Data integrity ensures the data is consistent, complete, accurate, and has been validated. | *Data integrity is in place.* |
|  | X | Data is available to individuals authorized to access it. | *Accessible to all, needs more restriction.* |

**Recommendations:** Toys needs to add encryption to protect sensitive data. Stronger passwords should be required for all employees. An intrusion detection system should be installed for better monitoring. Access should be limited to only those who need it. Backup and recovery plans must be created soon. These steps will improve security and compliance overall.