# Checklist and Security Audit: Botium Toys

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

**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.) |

*Does Botium Toys currently adhere to this compliance best practice?*

**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:**

There are so many ways that Botium Toys can improve their security posture and move into compliance with important regulations like the PCI DSS, GDPR, and SOC Controls, as well as taking concrete steps to bring themselves up to industry standards. Luckily many items can be controlled from services that the IT team already has access to, so let’s get started!

First, The IT team needs to implement the principle of least privilege. An intern who needs a login to work on social media and marketing doesn’t need access to the entirety of the organization’s file system! The IT department can use the basic functionalities built into their (most likely) windows Operating systems to make sure that users are assigned access to files based on their need-to-know basis (Separation of duties). Getting an idea of what items need to be kept private then keeping them private will bolster their adherence with the GDPR, and the PCI DSS.  
  
Next, the company needs to implement a new password policy that is in keeping with modern password best practices. Having employees run their passwords through Bitwarden and other password checking tools will help give them an adequate idea of what their work passwords should look like.

Then, the company should start using the integrated Encryption systems on their server and PC deployments for various systems. Bitlocker is commonly used by windows and can provide amazing levels of security at VERY low expense!! This would really help the organization improve their standing with the PCI DSS.

Finally, it is important for IT to establish a monthly check in on legacy systems and continue to evaluate the security and reliability of antiquated systems.

All of these low-to-no-cost solutions will put Botium in compliance with almost all relevant regulations!

It is important that the team at Botium contract a security professional to help develop a data recovery plan, or turn the task over to IT. What will happen if the core infrastructure burns down? How will you respond if data is leaked? Speaking with a professional and building out a robust plan can really help you feel prepared when the worst happens! Many consultant groups can even drill your IT team on how to respond!

We here at Last Minute Cybersecurity will go on to recommend some other things that can further improve Botium’s security posture.  
  
1. Offsite Backups: In case of a fire in the Botium main storage area, having secure cloud data backups can help a business like Botium get back on its feet even after its local infrastructure is destroyed. Keeping you in contact with the customers and vendors that make up your consumer base!

2. Implementing a suite of SIEM tools, these are suites of tools that allow you to monitor and manage network traffic, file access, and many other activities of security interest of concern. I can hear you reaching for your pocketbooks to hide your credit cards! Wait! There are established open-source solutions for SIEM, so if Botium has IT staff that are ready to make the jump into being a Cybersecurity Analyst, they may be able to configure an open-source tool like GrayDog! You could purchase subscriptions to cloud based platforms like Sumo Logic that may have better support and ease of deployability, or true tested enterprise solutions like IBM Q-Radar which will have a heftier price tag, but there will be robust support in helping you establish the system and train your IT department on how to handle it!

Botium is a wonderful company, whose toys have brought joy to their customers all over! Remaining out of compliance just isn’t an answer, because a worried mind can struggle so much to produce anything joyful. Find peace in cybersecurity and protect this business you’ve worked so hard to establish. YOU GOT THIS!