Subject: Security Recommendations for Botium Toys Stakeholders

Dear Botium Toys Stakeholders,

I am writing to share the results of the recent security audit conducted by the IT department at Botium Toys. The audit evaluated various security controls and compliance measures within your organization. While there are areas where you have made commendable progress, there are also important aspects that require immediate attention and improvement.

**Controls Assessment Checklist:**

**Availability Controls:**

1. Least Privilege: You currently do not have a least privilege policy in place. It is recommended to implement this policy to restrict user access to only the necessary resources and functionalities required for their roles.

2. Disaster Recovery Plans: Unfortunately, you do not have comprehensive disaster recovery plans in place. It is crucial to develop and implement these plans to ensure business continuity in the event of unforeseen disruptions.

3. Separation of Duties: The organization lacks a separation of duties policy. You should establish clear roles and responsibilities to prevent conflicts of interest and enhance security.

4. Intrusion Detection System (IDS): Currently, you do not have an IDS in place. Implementing an IDS will help in identifying and responding to potential security threats in real-time.

5. Backups: You do not have a backup strategy defined. Regular backups are essential to protect data integrity and ensure recoverability in case of data loss.

6. Encryption: Encryption measures are currently not employed. Encryption should be implemented to safeguard sensitive data during transmission and storage.

7. Password Management System: A password management system is not in use. Adopting such a system will improve password security and management.

**Compliance Checklist:**

**Payment Card Industry Data Security Standard (PCI DSS):**

1. Only authorized users have access to customers’ credit card information: Currently, this control is not in place. You need to ensure that only authorized personnel can access credit card information.

2. Credit card information is stored, accepted, processed, and transmitted internally, in a secure environment: This control is not met. You must establish secure environments for handling credit card data.

3. Implement data encryption procedures to better secure credit card transaction touchpoints and data: Encryption procedures are not implemented. Encryption should be employed to protect sensitive cardholder data.

4. Adopt secure password management policies: Unfortunately, you do not have secure password management policies. You should implement strong password policies to enhance security.

**General Data Protection Regulation (GDPR):**

1. E.U. customers’ data is kept private/secured: This control is met. You are currently ensuring the privacy and security of E.U. customers' data.

2. There is a plan in place to notify E.U. customers within 72 hours if their data is compromised/there is a breach: You have a plan in place for timely notification, meeting this requirement.

3. Ensure data is properly classified and inventoried: This control is met, as data classification and inventory practices are in place.

4. Enforce privacy policies, procedures, and processes to properly document and maintain data: Privacy policies, procedures, and processes are enforced, ensuring proper data documentation and maintenance.

**System and Organizations Controls (SOC Type 1, SOC Type 2):**

1. User access policies are established: Currently, you do not have user access policies. It is recommended to establish clear access control policies.

2. Sensitive data (PII/SPII) is confidential/private: This control is not in place. You should implement measures to safeguard sensitive data.

3. Data integrity ensures the data is consistent, complete, accurate, and has been validated: You currently meet this requirement, ensuring data integrity.

4. Data is available to individuals authorized to access it: Data availability to authorized individuals is ensured.

In light of these audit findings, I recommend that Botium Toys takes immediate action to address the identified gaps in our security controls and compliance measures. Implementing these recommendations will enhance our organization's overall security posture and ensure that we meet industry standards and regulations.

If you have any questions or would like to discuss these recommendations further, please do not hesitate to reach out to me or the IT department. Your cooperation and support in strengthening our security measures are greatly appreciated.

Sincerely,

WAREEZ BUSARI

SECURITY AUDITOR

Botium Toys