TO: IT Manager, Stakeholders
FROM: Christopher Hatcher
DATE: 05/16/2023
SUBJECT: Internal IT Audit Findings and Recommendations

Dear Colleagues,

Please review the following information regarding the Botium Toys internal audit scope, goals, critical findings, summary and recommendations.

Scope: Entire Security Program at Botium Toys

Goals: Improve Security Posture & Adhere to Compliance Regulations

Critical findings : I found the security posture of our company to be inadequate to manage all the company assets under our care. We have a lack of effective controls concerning the PII and SPII of our customers, and the handling of information of our international customers. We do not have the managerial controls implaced to assign responsibilities for certain equipment and the custodianship of its keeping. We need to immediately implement safeguards of our data with back-up storages, and physical controls to protect those assets digitally and physically. While also implementing technical controls to protect our network from outside attacks. The most pressing issue is administrative controls that need to be implemented immediately to protect the security of our customers.

Findings : We do not have the controls necessary to be in compliance with regulatory laws.

Summary/Recommendations:

It is strongly advised to promptly address any significant issues related to complying with the Payment Card Industry Data Security Standard (PCI DSS) and the General Data Protection Regulation (GDPR) for Botium Toys, as the company accepts online payments from customers worldwide, including those in the European Union. Furthermore, as part of the audit process, it is crucial to align with the principle of least permissions and incorporate guidelines from SOC1 and SOC2 to establish appropriate user access policies and ensure overall data safety. Developing comprehensive policies and procedures for disaster recovery and maintaining regular backups is of utmost importance as they contribute to business continuity in the event of an incident. By integrating Intrusion Detection Systems (IDS) and Anti-Virus (AV) software into the existing systems, Botium Toys can enhance its ability to identify and mitigate potential risks, particularly for intrusion detection, as the current legacy systems necessitate manual monitoring and intervention. To further enhance the security of assets housed at Botium Toys' physical location, implementing measures such as locks, closed-circuit television (CCTV) surveillance, and diligent monitoring to investigate potential threats is essential. While not immediately urgent, employing encryption techniques, installing time-controlled safes, ensuring adequate lighting, utilizing locking cabinets, implementing fire detection and prevention systems, and displaying signage indicating the presence of an alarm service provider will further augment the overall security posture of Botium Toys.