TO: IT Manager, Stakeholders
FROM: Michael McCauley
DATE: 7/31/2023
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.

This internal audit assessed the current user permissions, implemented controls, and procedures and protocols set for all company security systems. Special attention was paid to the accounting system, network infrastructure, and the security tools already in place. Additionally we assessed these current user permissions, implemented controls, and procedures and protocols for compliance with relevant requirements per local, state, national and international law. Finally, we accounted for all physical hardware assets as well as access to said assets by personnel and vendors.

Through this audit we sought to adhere to the NIST CSF framework in our approach (Identify, Protect, Detect, Respond, and Recover) to systematically review our infrastructure. We also endeavored to improve our compliance-ensurance process (and ensure compliance generally), strengthen our toolkit of system controls, and rework our credential management controls so that users have the least required access for their role. Finally, we aimed to fully establish basic policies and procedures, including security playbooks for specific types of incidents.

Critically, Botium Toys must institute several basic policies immediately. To be compliant with the GDPR as well as the PCI DSS (requirements for doing overseas business), we must implement encryption systems across all customer personal and financial information, as well as on all transactions involving said information. Along with encryption, comprehensive password and access controls must be maintained across all systems. We have no policies in place to manage business operations in the event of a serious data breach or other threat and we are not maintaining backups for our data in these events. We are not currently making use of critical tools such as anti-malware software and tools to detect intrusions and unauthorized access. Less immediately, there is a lack of physical security features.

We recommend a comprehensive security system to maximize postural effectiveness, involving best-practice password and management practices, limiting employee and vendor access to internal systems based on what is required for their role, preventing unauthorized access to and potential disclosure of sensitive customer personal and financial data per compliance regulations. We also need to maintain regular backups (onsite and offsite) of company data and develop playbooks to deal with common security threats and maintain normal business operations as much as possible in the face of such threats and associated data breaches. As part of developing and deploying these playbooks we will need to make use of basic security tools such as intrusion detection and event management applications, as well as anti-malware tools and the improvement of our existing firewall. Physical security hardening measures we can take include CCTV surveillance and physical lockdown of assets (time-controlled safe and locking cabinets), locks, and–critically–fire protection, essential to protect sales merchandise as well as IT assets.