**25 May 2023**

**TO: IT MANAGER & STAKEHOLDERS**

**SUBJECT:** Internal Audit Findings & Recommendations

Colleagues,

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

#### Scope

This audit was conducted to assess the following:

* Current user permissions set in the following systems: accounting, end point detection, firewalls, intrusion detection system, security information and event management (SIEM) tool.
* Current implemented controls in the following systems: accounting, end point detection, firewalls, intrusion detection system, Security Information and Event Management (SIEM) tool.
* Current procedures and protocols set for the following systems: accounting, end point detection, firewall, intrusion detection system, Security Information and Event Management (SIEM) tool.
* Ensure current user permissions, controls, procedures, and protocols in place align with necessary compliance requirements.
* Ensure current technology is accounted for. Both hardware and system access.

#### Goals

* To adhere to the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF)
* Establish a better process for their systems to ensure they are compliant
* Fortify system controls
* Implement the concept of least permissions when it comes to user credential management
* Establish their policies and procedures, which includes their playbooks
* Ensure they are meeting compliance requirements

#### Critical findings (must be addressed immediately):

* Least Privilege
* Disaster recovery plans
* Password policies
* Access control policies
* Account management policies
* Intrusion Detection System
* Antivirus Software
* Manual monitoring maintenance, and intervention
* Backups
* Encryption
* Closed-circuit television surveillance
* Lock
* Password management system

#### Findings (should be addressed, but no immediate need):

* Fire detection & prevention
* Time-controlled safe
* Adequate lighting
* Signage indicating alarm service provider

#### Summary/Recommendations:

There are a number of issues that require immediate attention to ensure compliance with the NIST CSF. Immediate recommendations are to address critical findings as these pose the most risk to exposing PII and SPII. As Botium is expanding online sales, it is imperative that we are compliant with the EU GDPR to continue business there and PCI DSS to ensure payments are conducted in a secure manner. Other findings that need to be addressed but are not critical are listed and can be fixed with leniency lent to time.

Respectfully,

John Laffey

Cybersecurity Analyst