**TO: IT Manages & Stakeholders**

**FROM: Oduntan Toluwani**

**DATE: 14-08-2023**

**SUBJECT:** Internal IT audit findings and recommendations

Dear Colleagues,

Kindly review the findings and information about Botium Toys scope, goals ,critical findings and reccommendations

**Scope:** The scope is defined as the entire security program at Botium Toys. This means all assets need to be assessed alongside internal processes and procedures.

Botium Toys internal IT audit will 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.

**The goals for Botium Toys’ internal IT audit are:**

* 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

Critiical Findings (Must be addressed immediately)

Various controls must be implemented to meet the audit goals:

* Principle of less privilege
* Disaster recovery plans
* Password policies
* Access control policies
* Account management policies
* Seperation of duties
* Intrusion detection system
* Encryption
* Backups
* Antivirus
* Manual monitoring and intervention
* Locks

Findings(Can be addressed later)

* Password management systems
* Adequate lightening
* Alarm service provider

Summary/Reccommendation

It is important that Botium toys follow the appropriate regulation and guidelines. They must comply to GDPR, PCI DSS and NIST cyber security frameworks so as to secure the company’s infrastructure and help identify and mitigate the potential risks threats or vulnerabilities to critical assets. Data recovery plans are very important as well and they should be put in place for business continuity. To further inporove the security of the physical location, Locks and CCTV should be in place. Fire detection systems should be available throughout the premises in the case of any fire hazaRd.