**Botium Toys Audit Report**

**Summary**

To perform a cybersecurity audit for Botium Toys which need to be align with current business practices with industry standards. The goal of this audit is to provide mitigation recommendations for vulnerabilities which is classified as “high risk” and recommend an overall strategy for improving the security posture of the organization. Hence, the audit team needs to document their findings, provide solutions plans and efforts also communicate with stakeholders on improving the security posture.

**Scope**

The scope of the audit includes assessment on the list physical and digital assets to ensure Botium Toys’ Information Technology (IT) practices are meeting industry and organizational standards specifically Payment Card Industry Data Security Standard (PCI DSS), General Data Protection Regulation (GDPR) and System and Organizations Controls (SOC type 1, SOC type 2).

Internal Audit areas of focus include:

* On-premises equipment
* End-user devices
* Storefront products
* Management of systems, applications and software’s
* Internet access
* Internal Network
* Data retention and storage
* Legacy system maintenance

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.
* The implemented controls set in the following systems: accounting, end point detection, firewalls, intrusion detection system, security information and event management (SIEM) tool.
* The current procedures and protocol set in the following systems: accounting, end point detection, firewalls, intrusion detection system, security information and event management (SIEM) tool.
* To improve plans on disaster recovery plans and implement back-ups for critical data.
* The current privacy policies, procedures and processes improve, and set comply with Payment Card Industry Data Security Standard (PCI DSS) and General Data Protection Regulation (GDPR)
* Ensure current user permissions, controls, procedures, and protocols are in place align with respective compliance requirements.
* Ensure current technology is accounted for both hardware and software system access.
* To recommend Botium Toys’ to have manual monitoring, maintenance, and intervention practices for technical and operational controls.

**Goals**

The goal of the audit is to assess existing assets and complete the controls and compliance checklist to determine which controls and compliance best practices need to be implemented to improve Botium Toys’ security posture. This also helps to identify weakness or vulnerabilities within Botium Toys’ and understand the failures in processes and procedures and correct them with NIST CSF Framework.

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