Stakeholder Memorandum

TO: IT Manager, Stakeholders
FROM: Jacob Suveges
DATE: May 18, 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:

- **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**
- **Separation of Duties**
- **Intrusion Detection Systems**
- **Encryption**
- **Backups**
- **Password Management Systems**
- **Antivirus Software**
- **Manual Monitoring, Maintenance, and Intervention**
- **CCTV**
- **Locks**
- **GDPR Compliance**
- **PCI DSS Compliance**
- **SOC 1 and SOC 2 Compliance**

Findings (should be addressed, but no immediate need):
- **Time-Controlled Safe**
- **Adequate Lighting**
- **Locking Cabinets**
- **Alarm Service Provider Signage**
- **Fire Detection and Prevention**

Summary/Recommendations:

The importance of the scope of this audit revolved around compliance with regulations, implemented controls in multiple systems, and current procedures and protocols. These scope assets played very nicely with the significant goals of this audit which were to ensure the meeting of compliance requirements, establish policies

and procedures, as well as to fortify system controls. The reason that the scope was good for the goals at hand was because the audit uncovered an alarming amount of non-compliance and inadequate procedures and protocols. Some of the more critical findings include the implementation of disaster recovery plans, multiple policies relating to user security, and compliance with both national and international compliance standards and regulations. There are also issues that aren't as concerning such as ensuring adequate lighting, cabinets that can lock, and fire detection and prevention. In note there are many things to fix and to implement, however it is of the utmost importance to first make sure the compliances are up to date and completed as those can result in large fines and possible class action lawsuits.