Stakeholder memorandum

TO: IT Manager, Stakeholders
FROM: Rocio Gutierrez
DATE: 05/31/2023
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.

Scope:

- Current user permissions set, implemented controls, procedures and protocols set in the following systems:
    - Accounting
    - End point detection
    - Firewalls
    - 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:

- Adhere to National Institute of Standards and Technology Cybersecurity Framework (NIST CSF)
- Establish a better process for their systems to ensure compliance with GDPR, PCI DSS, SOC1 and SOC2
- Fortify system controls
- Implement the concept of least permissions to user credential management
- Establish policies and procedures, which includes playbooks
- Ensure company is meeting compliance requirements

Critical findings (must be addressed immediately):

- **Policies must be developed and implemented to adhere to PCI DSS and GDPR requirements.**
- **Policies must be developed and implemented to adhere to SOC1 and SOC2 requirements.**
- Least Privilege
- Separation of duties
- Disaster recovery plans
- Password policies
- Access control policies
- Account management policies
- Intrusion Detection System (IDS)
- Encryption (for transactions)
- Backups (in case of breach)
- Password management system
- Antivirus (AV) software
- Manual monitoring, maintenance, and intervention
- Locks
- Fire detection and prevention (fire alarm, sprinkler system, etc.)

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

- Time-controlled safe
- Adequate lighting
- Closed-circuit television (CCTV) surveillance
- Locking cabinets (for network gear)
- Signage indicating alarm service provider

Summary/Recommendations: Botium Toys must develop and implement policies to stay within compliance of GDPR, PCI DSS, SOC1, and SOC2 regulations. It is also important to implement proper access and account management, adding explicit policies for access control, account management, and password management. Encryption will assist with keeping customers' transactions safe. There is a need for more employees within the department to manually monitor our current and future physical systems, in the event these systems fail and need human intervention. Having fire detection and prevention systems keeps our employees and assets safer in the event of a fire. Having both IDS and AV software will prevent and detect technological breaches to lessen risk. Backups will ensure valuable data can be recovered. Relating

to my findings, physical locations should have proper security, but do not have to be implemented immediately as employees will be ensuring the safety of our assets. Adding a time-controlled safe, adequate lighting, etc. will increase our depth of defense, further bolstering our security posture.