TO: IT Manager, Stakeholders
FROM: Aya KHEDDA
DATE: July 13, 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:

- The systems in scope are: accounting, end point detection, firewalls, intrusion detection system, security information and event management (SIEM) tool. The systems will be assessed for:
    - User permissions
    - Implemented controls
    - Procedures and protocols
- Ensure current user permissions, controls, procedures, and protocols in place align with PCI, DSS and GDPR 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):

- Critical controls need to be put in place including:
    - Least Privilege
    - Disaster recovery plans
    - Password policies
    - Access control policies

    - Account management policies
    - Separation of duties
    - Intrusion Detection System
    - Encryption
    - Backups
    - Password management system
    - Antivirus software
    - Manual monitoring, maintenance, and intervention
    - CCTV
    - Locks
    - Fire detection and prevention
- Policies need to be developed and implemented to meet the PCI, DSS and GDPR compliance requirements.
- Policies need to be developed and implemented to align with SOC1 and SOC2 to ensure data safety

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

- Other controls need to be implemented as well when possible, including:
    - Adequate lighting
    - Time-controlled safe
    - Locking cabinets (for network gear)
    - Signage indicating alarm service provider

Summary/Recommendations:

It is recommended that critical findings regarding compliance with PCI, DSS and GDPR need to be addressed immediately since Botium Toys accepts payments from customers worldwide. In addition, SOC1 and SOC2 guidance related to user access policies should be used to develop policies and procedures to ensure overall data safety. Disaster recovery plans and backups are mandatory in order to preserve business continuity in case of an incident. Moreover, an IDS and AV need to be integrated into the system to support our ability to detect and mitigate potential risks.

Furthermore, to protect the physical assets at Botium Toy's location, fire detection and prevention, locks and CCTV should be used. Although not required right away, having adequate lighting, a time-controlled safe, signage indicating alarm service provider and locking cabinets will improve Botium Toy's security posture.