Security Audit Findings

TO: IT Manager, Stakeholders
FROM: Danielle Johnson
DATE: July 6, 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 audit Assessed the following

- **User permissions for accounting, end point detection, firewalls, intrusion detection system, security information, and event management (SIEM) tool.**
- **Implemented controls for accounting, end point detection, firewalls, intrusion detection system, security information, and event management (SIEM) tool.**
- **Procedures and protocols for accounting, end point detection, firewalls, intrusion detection system, security information, and event management (SIEM) tool.**
- **Ensure items listed above align with compliance requirements • Ensure all technology is accounted for.**

Goals:

- **Adhere to NIST CSF.**
- **Establish better processes to ensure compliance.**
- **Fortify system controls.**
- **Implement Least Privilege for user credential management.**
- **Establish procedures and policies to include in the playbooks.**
- **Ensure compliance requirements are met.**

Critical findings (must be addressed immediately):

- Controls that need to be implemented immediately to meet the audit goals are :
    - Least Privilege

    - Disaster Recovery Plans
    - Password Polices
    - Access Control Polices
    - Account Management Polices
    - Separation of Duties
    - Intrusion Detection System
    - Encryption
    - Backups
    - Password Management System
    - Manual Monitoring, Maintenance, and Intervention for Legacy Systems
    - Locks
    - Fire Detection and prevention

- Policies need to be developed to meet compliance requirements around PCI DSS and GDPR
- In order to ensure data safety, policies should be developed to align with SOC Type1 and Type 2 guidance.

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

- Time- Controlled Safe
- Adequate Lighting
- Closed Circuit Television Surveillance (CCTV)
- Locking Cabinets
- Signs indicating the alarm service provider

Summary/Recommendations:

In order to follow the Payment Card Industry Data Security Standard, companies must ensure that all data containing credit card information is stored, accepted, processed and transmitted in a secure environment. All Critical Findings assist in compliance with PCI DSS. The General Data Protection Regulation protects all European Union citizens' data and their right to privacy. It states that after a breach, the citizen must be informed within 72 hours of the incident. Intrusion Detection System and the SIEM toll will assist with knowing if there is a breach. System and Organizations Controls (SOC type 1 and SOC type 2) focuses on access policies to cover confidentiality, privacy, integrity, availability, security, and general data safety. Failure to control in this area opens more risk for fraud. Least Privilege, Strong Password Policies, Access Control Policies, Account Management Polices, and Separation of duties will all help follow the

guidelines for SOC type 1 and type 2. Additionally, there were findings that should be addressed but aren't needed immediately. Data backups will help in the event of an event and should be in the disaster recovery plan. Adequate Lighting and Closed-Circuit Television Surveillance will not only help keep your employees safe but will also act as deterrents to a physical breach.