TO: IT Manager, Stakeholders
FROM: (Your Name)
DATE: (Today's Date)
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:

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.
- 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:

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

Critical findings (must be addressed immediately):

- ❖ **Administrative Controls**
- Least Privilege
- Password policies

- Access control policies
- Separation of duties

❖ **Technical Controls**
- Encryption
- Password management system
- Antivirus (AV) software

❖ **Physical Controls**
- Closed-circuit television (CCTV) surveillance
- Locking cabinets (for network gear)

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

❖ **Administrative Controls**
- Disaster recovery plans

❖ **Technical Controls**
- Manual monitoring, maintenance, and intervention
- Firewall

❖ **Physical Controls**
- Fire detection and prevention (fire alarm, sprinkler system, etc.)

Summary/Recommendations:

Immediate attention should be given to address the critical findings identified during the internal IT audit at Botium Toys. The following actions are recommended:

Enhance administrative controls:

- Implement the concept of least privilege by granting users the minimum necessary permissions required to perform their duties effectively.

- Strengthen password policies by enforcing complexity requirements, regular password changes, and secure storage of passwords.

- Define and enforce access control policies to ensure that access to sensitive systems and data is granted based on appropriate authorization levels.

- Ensure proper separation of duties to prevent conflicts of interest and reduce the risk of unauthorized activities.

Improve technical controls:

- Implement encryption measures to protect sensitive data in transit and at rest, ensuring its confidentiality and integrity.

- Adopt a robust password management system to enforce strong password practices, facilitate secure storage of passwords, and enable centralized management.

- Keep antivirus software up to date across all systems to detect and mitigate potential threats, safeguarding against malware and other malicious activities.

Strengthen physical controls:

- Enhance CCTV surveillance to monitor and record physical access to critical areas, ensuring a higher level of security and facilitating incident investigation if necessary.

- Secure network gear in locked cabinets to restrict unauthorized physical access, reducing the risk of tampering or theft.

Additionally, it is recommended to address the non-critical findings in a timely manner:

- Develop comprehensive disaster recovery plans that outline clear procedures and actions to be taken in the event of emergencies, ensuring business continuity and minimizing downtime.

- Implement automated monitoring and maintenance systems to reduce manual interventions, enhance efficiency, and promptly identify and address any system irregularities or vulnerabilities.

- Enhance the existing firewall to reinforce network security, preventing unauthorized access and protecting against potential threats.

- Furthermore, it is essential to regularly review and update all policies, procedures, and playbooks to align with current best practices and compliance requirements.

- By promptly addressing both the critical and non-critical findings, Botium Toys can establish a more secure and compliant IT infrastructure, safeguard sensitive data, and effectively mitigate potential risks. It is strongly advised to allocate the necessary resources and assign responsible individuals to ensure the successful implementation of the above recommendations.