Stakeholder memorandum

TO: IT Manager, Stakeholders
FROM: Lucas Ferreira
DATE: May 30
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 following systems are in scope: accounting, end point detection, firewalls, intrusion detection system, SIEM tool. The systems will be evaluated for:

- Current user permissions
    - Current implemented controls
    - Current 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:
The goals for this audit are to adhere to the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF), establish more efficient processes, and fortify system controls.

Critical findings (must be addressed immediately):

- Compliance with the General Data Protection Regulations (GDPR) and the Payment Card Industry Data Security Standards (PCI DSS).
- SOC1 and SOC2 policies must be implemented to improve overall data safety
- Least privilege
- Disaster recovery plan
- Passwords policies and password management systems
- Access control policies

- Account management policies
- Separation of duties
- IDS
- Encryption
- Backups
- Antivirus software
- Locks
- Fire detection and prevention
- Manual monitoring, maintenance and intervention for legacy systems
- CCTV

Findings (should be addressed, but no immediate need):
The following should be implemented when possible:

- Signage indicating alarm service provider
- Adequate lighting
- Time-controlled safe

Summary/Recommendations:
Compliance to the GDPR and the PCI DSS must be adhered to as soon as possible in order to accept card payments worldwide. Additionally, SOC1 and SOC2 must be implemented to assure data safety. CCTV must be used to monitor and secure physical locations.
While some of these findings don't need immediate action they must be addressed eventually.