Stakeholder Memorandum for Botium Company

TO: IT Manager, Stakeholders
FROM: Matthew Ruiz Diaz
DATE: September 12th, 2023
SUBJECT: Internal IT Audit Findings and Recommendations

Dear Colleagues,

Please review the following information regarding the Botium Company internal audit scope, goals, critical findings, summary and recommendations.

Scope:

- Hardware and access systems are all within the scope and accounted for.
- Make sure user permissions, controls, procedures, and protocols in current use are complying with necessary regulations such as PCI DSS, GDPR, SOC type 1, SOC type 2.
- All Botium systems such as: accounting, end point detection, firewalls, intrusion detection (IDS), and system event information (SIEM) tools will be rated on these aspects:
    - User permissions
    - Controls
    - Procedures and protocols

Goals:

- Adhere to NIST CSF
- Establish a better process for Botium systems to ensure compliance
- Strengthen system controls
- Implement the practice of least permissions (better manage user credentials)
- Establish Botium policies and procedures by updating playbooks
- Ensure Botium is in compliance with all necessary regulation requirements

Critical findings (must be addressed immediately, or high priority findings):

- Updating company policy playbooks to adhere to GDPR, PCI DSS, and SOC regulations
- Implementing the following controls:

    - Principle of least privilege
    - Disaster recovery plans
    - Password policies
    - Access control policies
    - Separation of duties
    - Intrusion detection system (IDS)
    - Backups
    - Antivirus software
    - Manual monitoring of legacy systems
    - CCTV surveillance
    - Locking network technology in cabinets
    - Locks

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

- Implementing the following controls:
    - Account management policies
    - Encryption
    - Password management system
    - Fire detection and prevention

Summary/Recommendations:

The recommended steps from this audit are to immediately train Botium employees on new policies regarding password and account management, as well as assign an IT team to integrate and manage IDS, SIEM, Antivirus, and CCTV tools. The IT department must also assign staff to monitor the legacy systems still being used. Taking these steps will eliminate the majority of high risk vulnerabilities within the organization. Concurrently, the IT department must update its policy playbooks to adhere to current GDPR, PCI DSS, and SOC regulations and ensure that all high priority controls are in compliance due to the company actively performing credit card transactions internationally. The steps listed above are the most important to take, but there are other tasks once these are completed. Establishing proper physical controls at Botium's one physical location is important, which means fire detection and prevention should be installed, as well as locks for every company asset, especially network technology. Creating a disaster recovery plan is highly important as well and should be done in a timely manner to ensure business continuity. Once these tasks are completed, the IT department should address all medium and low priority issues in a

sequential way to ensure the audit was successful. At the end of this process Botium's security posture should be the industry standard posture.