**Memorandum on Key findings of the security Audit**

To: All Stakeholders

From: Oku Ediomo Samuel [Cybersecurity Analyst]

Date: 10th February 2024.

Re: Summary of the key Findings from the Recent Security

Audit.

Dear Stakeholders,

I am writing to brief on the significant findings from our recent comprehensive security audit conducted at BOTIUM TOYS. The audit was extensive, covering various aspect of the company’s security infrastructure, policies, and practices. Below is a summary of the findings.

System Vulnerabilities: The audit Identify several critical vulnerabilities in our software system, particularly in areas related to data encryption and user authentication. Immediate attention and remediation are advised

Compliance Issues: we have areas of non compliance and industry standards and regulations specifically concerning data protection (GDPR) and customer privacy.

Physical Security Lapses: There are notable weaknesses in our physical security measures at several facilities , including inadequate surveillance and access control systems.

Employee Training Deficiencies: The audit highlighted a lack of regular security training and awareness program for employees, leading to potential risks in handling sensitive information and recognizing phishing attacks.

Incident Respond Plan: Our current incident respond pan is outdated and does not align with best practices, potentially hindering our ability to effectively respond to and recover from security incidents.

Vendor Risks: Several third party vendors do not meet our security standards, posing a risk to our data security and supply chain integrity.

Positive Highlights: The audit also recognized areas of strength, including robust network security measures and effective use of encryption in certain applications.

Next Steps:

Immediate Action: Address critical vulnerabilities in our system and update our incident respond plan.

Compliance Alignment: Work towards full compliance with relevant regulations by Q3 2024.

Employee Training: Implement regular security training for all employees.

Physical Security Enhancement: Upgrade physical security measures at key facilities.

Vendor Management: Review and reinforce vendor security requirements.

We will convene a meeting to discuss these findings in details and formulate a comprehensive action plan. Your insight and involvement in the process are invaluable as we work to strengthen our security posture and protect our company’s assets and reputation.

Thank you for your attention to this critical matter.

Sincerely,

Oku Ediomo Samuel

Cybersecurity Analyst

07032630259