**Cybersecurity Measures at Botium Toys presented at the stakeholders' memorandum**

Botium Toys is an international organization that trades toys with expansion. Botium migrated to virtual sales in 2023, where they have recently made the most sales, as reflected in the result of the 2023 yearly audit. As we look to partner with stakeholders, I present to you the cybersecurity measures implemented at Botium Toys to ensure the security and confidentiality of our sensitive information, as well as to protect the integrity of our systems and the data of our customers and partners.

We recognize the importance of maintaining a good security posture and complying with cybersecurity practices in today's world. Our commitment to safeguarding information spans across all areas of our operations, including data storage, customer interactions, and supply chain management.

Our organization comprises over 500 staff, physically and virtually, with a customer base exceeding 1 million people. What makes this organization out is our quality.

We take a look and popular security controls and how much they are being implemented here. We would also list the frameworks we implement here:

**Firewalls** – Currently, we have found the stateful firewall really helpful. This would help filter traffic according to the recommendations fit for a particular time. Stateful firewalls have worked well for us in recent years to mitigate attack traffic.

**Access Controls** – To help limit access to authorized persons, we utilize multifactor authentication featuring what the customer knows and what they have. We also implement the principle of least privilege, meaning users have the lowest permission possible to carry out a task. We regularly ensure passwords are changed, and unused accounts nullified

**Intrusion Detection System** – The host-based IDS is used to ensure that each host system has added protection for malicious traffic that evades the firewall; the IDS detects and alerts the security team, enabling them to make their decision on whether to allow it or terminate it. Very critical assets make use of the Intrusion Prevention System, meaning that malicious traffic is terminated on discovery.

**Patching** – We regularly ensure that our software and applications are up to date. We look out for novel ideas and monitor zero attacks ensuring that the application is robust enough to prevent attacks.

**Business Continuity Plans** – We have developed a comprehensive plan for Business Continuity Plans that would ensure that business is not out-phased during a disaster.

We also have frameworks we implement, such as:

1. Payment Card Industry Data Security Standard (PCI DSS)
2. General Data Protection Regulation

Botium Toys is committed to continuous improvement in the field of cybersecurity. We stay abreast of emerging threats and technologies, regularly updating our security protocols to adapt to the evolving cybersecurity landscape

We understand the trust you place in us, and we take our responsibility to protect your information seriously. If you have any questions or concerns regarding our cybersecurity measures, please do not hesitate to reach out.