**Gharny’s Botium toy Stakeholder Memoradum**

The purpose of this security audit is to inform you about the current state of Botium toys company cyber security and outline the actions required to enhance the overall security posture.

The audit revealed several areas of concern that require immediate attention. Firstly, our network infrastructure was found to have vulnerabilities that could potentially be exploited by malicious actors. Additionally, our employee training and awareness programmes need improvement to ensure that everyone understands their role in maintaining a secure environment.

Furthermore, the audit identified weakness in our access control mechanism, highlighting the need for stronger authentication protocols and regular review of user privileges. It is essential that we implement multi-factor authentication and enforce the principle of least privilege to minimize the risk of unauthorized access.

Another critical finding was the lack of robust incident response and recovery procedures. In the event of a security breach, it is crucial that we have a well-defined plan in place to mitigate the impact and restore normal operations promptly. We recommend establishing an incident response team and conducting regular drills to ensure preparedness.

Lastly, the audit highlighted the importance of regular vulnerability assessments and penetration testing. By proactively identifying and addressing vulnerabilities, we can significantly reduce the likelihood of successful attacks.

In conclusion, the security audit has provided valuable insights into the current state of our security measures. It is imperative that we address the identified vulnerabilities and implement the recommended actions to safeguard our systems and data.