Recommendations for Botium Toys

Objective: strengthen security posture by classifying assets, deploying various security tools such as employee training on cybersecurity and implementing a stronger password criterion. This recommendation will also include suggestions on, training, backing up data, adhering to strong password policies, segmentation and aligning with the standards of NIST and PCI DSS. These recommendations will aid in keeping digital and physical assets safe.

Classification of Assets

Low Risk	Medium Risk	High Risk
None found	● Legacy system maintenance	● On-premise equipment for office and business needs ● Employee equipment and user devices ● Systems, software and services ● Internet access ● Internal network ● Data reputation and storage including customer PII and SPII ● Physical cash

Mandated Training on Security Awareness

Purpose of Training: make employees aware of the typical digital and physical attacks that threat actors usually employ when trying to access sensitive data and assets. This training will cover assets at risk, how employees should try and reduce those risks and how to respond to suspicious persons and emails.

Password Regulation Recommendations

Objective: Reduce probability of breaches and sensitive information being compromised by aligning with a strong password policy

- Password Policy should include changing user login passwords to systems every 90 days.
- Passwords shall be in compliance with policy regarding the complexity requirements.
- Passwords shall be at least 15 characters long and will include upper- and lower-case letters, one special character and passwords will not include names; in accordance with NIST frameworks
- Password management software shall be deployed on designed computers and devices to change or update passwords
- Multi-factor Authentication will be implemented to verify identity via code sent to text message or email.
- Password management system such as Passbolt or Keeper shall be inforce to regulate password policy

Recommendations for the Protection of Physical and Digital Assets

Objective: Reduce the risk of physical and digital data being compromised by employing written protocols. The following includes recommendations for access control, technical and managerial controls.

Access Control Recommendation:

- Limit resources based on role or attribute of the employee when accessing customer data data from database; in cooperation with PCI DDS
- Identify resources that will only be accessed by supervision so that mandatory access controls can be deployed
- Only selected staff will be given key access to store rooms containing cash and data.
- Limited appointed staff will be tasked with monitoring legacy systems.
- least privilege policy shall be implemented

Technical Controls Recommendation:

- All digital data shall be stored in secure databases with the use of encryption method TDE
- Hardware for backing up data shall be installed, and data should be backed up once per day to refrain from losing data and customer information permanently. It is also highly suggested to also back up data in a cloud-based environment to create redundancy and to ensure availability
- SSL/TLS encryption methods should be implemented while customer data is at rest, in transit or in use; this is imperative so that data can not be compromised; this in cooperation with PCI DDS
- The IT department should install an Intrusion detection system so that abnormal network traffic can be identified and proper response will take place
- Implement dual internet access
- Internet facing resources shall be segmented from internal network
- A Data Loss Prevention System is highly recommended as well as a File Integrity Management system to monitor exfiltration and alteration of data

Managerial Control Recommendation:

- Both IT and Stakeholders should collaborate to create a disaster recovery plan and policies.
  - A cold site should be deployed that will include some employee work stations and internet

    - Insurance should also be considered in case of a catastrophe that may include water, weather or fire damage.
    - utilize Iaas with a CSP along with on premise servers to create redundancy; this will allow for Botium toys to scale up if needed during a disaster
- It is highly suggested that data be classified by sensitive, confidential and critical so that the appropriate security and access controls be implemented
- Legacy Systems: Legacy systems shall be segmented from the rest of the internal network to reduce vulnerabilities due to the inability for legacy systems to be patched. It is recommended that automated continuous scanning of the systems be implemented so that IT will be alerted for any anomalies