BOTIUM TOYS SECURITY REVIEW

Current security checklist for Botium

Administrative Controls:

1. **Least Privilege:**
   - Implemented: No
   - **Comments:** All Botium Toys employees have access to internally stored data, indicating that least privilege is not enforced.

2. **Disaster Recovery Plans:**
   - Implemented: No
   - **Comments:** There are no disaster recovery plans in place, and the company lacks backups of critical data.

3. **Password Policies:**
   - Implemented: Partially
   - **Comments:** A password policy exists, but its requirements are nominal and not in line with current standards. Also, there is no centralized password management system.

4. **Access Control Policies:**
   - Implemented: No
   - **Comments:** Access controls pertaining to least privilege and separation of duties have not been implemented.

5. **Account Management Policies:**
   - Implemented: No
   - **Comments:** The status of account management policies is not explicitly mentioned in the provided information.

6. **Separation of Duties:**
   - Implemented: No
   - **Comments:** Separation of duties has not been implemented.

Technical Controls:

1. **Firewall:**
   - Implemented: Yes
   - **Comments:** The IT department has a firewall that blocks traffic based on an appropriately defined set of security rules.

2. **Intrusion Detection System (IDS):**
   - Implemented: No

- **Comments:** The IT department has not installed an intrusion detection system (IDS).

3. **Encryption:**
   - Implemented: No
   - **Comments:** Encryption is not currently used to ensure confidentiality of customers' credit card information.

4. **Backups:**
   - Implemented: No
   - **Comments:** There are no disaster recovery plans currently in place, and the company does not have backups of critical data.

5. **Password Management:**
   - Implemented: Partially
   - **Comments:** There is no centralized password management system.

6. **Antivirus (AV) Software:**
   - Implemented: Yes
   - **Comments:** Antivirus software is installed and monitored regularly by the IT department.

7. **Manual Monitoring, Maintenance, and Intervention:**
   - Implemented: Partially
   - **Comments:** While legacy systems are monitored and maintained, there is no regular schedule in place for these tasks, and intervention methods are unclear.

Physical/Operational Controls:

1. **Time-Controlled Safe:**
   - Implemented: No
   - **Comments:** The status of a time-controlled safe is not explicitly mentioned in the provided information.

2. **Adequate Lighting:**
   - Implemented: Yes
   - **Comments:** Adequate lighting is implemented to deter threats.

3. **Closed-Circuit Television (CCTV):**
   - Implemented: Yes
   - **Comments:** The store's physical location has up-to-date CCTV surveillance.

4. **Locking Cabinets (for Network Gear):**
   - Implemented: No
   - **Comments:** The status of locking cabinets for network gear is not explicitly mentioned.

5. **Signage Indicating Alarm Service Provider:**
   - Implemented: No
   - **Comments:** The status of signage indicating the alarm service provider is not explicitly mentioned.

6. **Locks:**
   - Implemented: Yes
   - **Comments:** Locks are implemented to deter and prevent unauthorized access to assets.

7. **Fire Detection and Prevention (Fire Alarm, Sprinkler System, etc.):**
   - Implemented: Yes
   - **Comments:** Fire detection and prevention systems are in place.

Overall, the company lacks several important security controls, including disaster recovery plans, backups, separation of duties, and strong password policies. Improvements are needed to ensure better data protection and overall security.