Botium Toys Security Audit

Table 1: **Administrative/Managerial Controls**

Control Name	**Implemented (Y/N)**	**Control Purpose**
Least Privilege	N	Reduce risk and overall impact of malicious insider or compromised accounts.
Disaster recovery plans	N	Provide business continuity.
Password policies	N	Reduce likelihood of account compromise through brute force or dictionary attack techniques.
Access control policies	N	Bolster confidentiality and integrity by defining which groups can access or modify data.
Account management policies	N	Managing account lifecycle, reducing attack surface, and limiting overall impact from disgruntled former employees and default account usage.
Separation of duties	N	Reduce risk and overall impact of malicious insider or compromised accounts.

Table 2: **Technical Controls**

Control Name	**Implemented (Y/N)**	**Control Purpose**
Firewall	Y	To filter unwanted or malicious traffic from entering the network
IDS/IPS	N	To detect and prevent anomalous traffic that matches a signature or rule
Encryption	N	Provide confidentiality to sensitive information
Backups	N	Restore/recover from an event
Password management	N	Reduce password fatigue
Antivirus (AV) software	Y	Detect and quarantine known threats
Manual monitoring, maintenance, and intervention	N	Necessary to identify and manage threats, risks, or vulnerabilities to out-of-date systems

Table 3: **Physical/Operational Controls**

Control Name	**Implemented (Y/N)**	**Control Purpose**
Time-controlled safe	Unknown	Reduce attack surface and overall impact from physical threats
Adequate lighting	Unknown	Deter threats by limiting "hiding" places
Closed-circuit television (CCTV)	Y	Closed circuit television is both a preentative and detective control because it's presence can reduce risk of certain types of events from occurring, and can be used after an event to inform on event conditions.
Locking cabinets (for network gear)	Y	Deter certain types of threats by making the likelihood of a successful attack seem low
Locks	Y	Bolster integrity by deterring and preventing unauthorized personnel, individuals from physically accessing assets.
Fire detection and prevention (fire alarm, sprinkler system, etc.)	Y	Detect fire in physical location and prevent damage to physical assets such as inventory, servers, etc.