# **Botium Toys Security Audit**

| **Administrative/Managerial Controls** | | | | |
| --- | --- | --- | --- | --- |
| **Control Name** | **Control Type** | **Control Purpose** | **Needs to be implemented (X)** | **Priority** |
| Least Privilege | Preventative | Reduce risk and overall impact of malicious insider or compromised accounts | X | Medium |
| Disaster recovery plans | Corrective | Provide business continuity | X | High |
| Password policies | Preventative | Reduce likelihood of account compromise through brute force or dictionary attack techniques | X  (There is one but needs to be updated for more secure policy) | Mid |
| Access control policies | Preventative | Bolster confidentiality and integrity by defining which groups can access or modify data | X | Medium |
| Account management Policies | Preventative | Managing account lifecycle, reducing attack surface, and limiting overall impact from disgruntled former employees and default account usage | X | Low |
| Separation of duties | Preventative | Reduce risk and overall impact of malicious insider or compromised accounts | X | Low |

| **Technical Controls** | | | | |
| --- | --- | --- | --- | --- |
| **Control Name** | **Control Type** | **Control Purpose** | **Needs to be implemented (X)** | **Priority** |
| Firewall | Preventative | To filter unwanted or malicious traffic from entering the network | - | none |
| IDS/IPS | Detective | To detect and prevent anomalous traffic that matches a signature or rule | X | Low |
| Encryption | Deterrent | Provide confidentiality to sensitive information | X | High |
| Backups | Corrective | Restore/recover from an event | X | High |
| Password management | Preventative | Reduce password fatigue | X | Mid/High |
| Antivirus (AV) software | Preventative | Scans to detect and quarantine known threats | - | none |
| Manual monitoring, maintenance, and intervention | Preventative | Necessary to identify and manage threats, risks, or vulnerabilities to out-of-date systems | - | none |

| **Physical/Operational Controls** | | | | |
| --- | --- | --- | --- | --- |
| **Control Name** | **Control Type** | **Control Purpose** | **Needs to be implemented (X)** | **Priority** |
| Time-controlled safe | Deterrent | Reduce attack surface and overall impact from physical threats | - | none |
| Adequate lighting | Deterrent | Deter threats by limiting “hiding” places | - | none |
| Closed-circuit television (CCTV) | Preventative/Detective | Closed circuit television is both a preventative 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 | - | none |
| Locking cabinets (for network gear) | Preventative | Bolster integrity by preventing unauthorized personnel and other individuals from physically accessing or modifying network infrastructure gear | - | none |
| Signage indicating alarm service provider | Deterrent | Deter certain types of threats by making the likelihood of a successful attack seem low | - | none |
| Locks | Deterrent/Preventative | Bolster integrity by deterring and preventing unauthorized personnel, individuals from physically accessing assets | - | none |
| Fire detection and prevention (fire alarm, sprinkler system, etc.) | Detective/Preventative | Detect fire in physical location and prevent damage to physical assets such as inventory, servers, etc. | - | none |