# Controls assessment

To review control categories, types, and the purposes of each, read the [control categories](https://docs.google.com/document/d/1HsIw5HNDbRXzW7pmhPLsK06B7HF-KMifENO_TlccbSU/template/preview) document.

## Current assets

Assets managed by the IT Department include:

* On-premises equipment for in-office business needs
* Employee equipment: end-user devices (desktops/laptops, smartphones), remote workstations, headsets, cables, keyboards, mice, docking stations, surveillance cameras, etc.
* Management of systems, software, and services: accounting, telecommunication, database, security, ecommerce, and inventory management
* Internet access
* Internal network
* Vendor access management
* Data center hosting services
* Data retention and storage
* Badge readers
* Legacy system maintenance: end-of-life systems that require human monitoring

| **Administrative Controls** | | | |
| --- | --- | --- | --- |
| **Control Name** | **Control type and explanation** | **Needs to be implemented (X)** | **Priority** |
| Least Privilege | Preventative; reduces risk by making sure vendors and non-authorized staff only have access to the assets/data they need to do their jobs | **x** | High: Insures that only the people working on data need to work on that data. |
| Disaster recovery plans | Corrective; business continuity to ensure systems are able to run in the event of an incident/there is limited to no loss of productivity downtime/impact to system components, including: computer room environment (air conditioning, power supply, etc.); hardware (servers, employee equipment); connectivity (internal network, wireless); applications (email, electronic data); data and restoration | **x** | High: This will insure that the loss of data is minimized, customer and user data is protected and business operations remain as unaffected as possible. |
| Password policies | Preventative; establish password strength rules to improve security/reduce likelihood of account compromise through brute force or dictionary attack techniques | **x** | High: This will link back to user and data safety. By implementing a strong password policy we reduce the risk of user accounts and customer data being compromised |
| Access control policies | Preventative; increase confidentiality and integrity of data | **x** | High: Botium Toys should make it a priority to insure that data is secured from within and from without the company. This links to the principle of least privilege, but it has more to do with what files and data can be accessed and by who. Implementing a good Access control Policy will enable and insure customer data protection as well as user security. |
| Account management policies | Preventative; reduce attack surface and limit overall impact from disgruntled/former employees | **x** | High: As soon as an individual leaves the company, their access to company files and customer data should be revoked. Employees should also not be able to store any company data or customer information on personal devices. |
| Separation of duties | Preventative; ensure no one has so much access that they can abuse the system for personal gain | **x** | Medium: Setting out decent Identity Management Policies is vital. For example there should be no reason why a sales representative has access to the payroll system. |

|  |  |  |  |
| --- | --- | --- | --- |
| **Technical Controls** | | | |
| **Control Name** | **Control type and explanation** | **Needs to be implemented**  **(X)** | **Priority** |
| Firewall | Preventative; firewalls are already in place to filter unwanted/malicious traffic from entering internal network | **x** | High: Controlling incoming and outgoing data and monitoring it for threats is of utmost importance. Having a decent firewall in place to prevent threats from the outside affecting business data and continuity should be treated as a priority. |
| Intrusion Detection System (IDS) | Detective; allows IT team to identify possible intrusions (e.g., anomalous traffic) quickly | **x** | High: As the company expands the amount of customer data increases. This may also be true for employee data. Notification and identification of threats in a timely manner will help align the company with regulations and codes of best practice. |
| Encryption | Deterrent; makes confidential information/data more secure (e.g., website payment transactions) | **x** | High: Encrypting sensitive data may be seen as a priority because it minimizes the risk of a data breach along with other risks of the organization. For example, when storing customer payment details such as credit cards, the PCI DSS 4 should be implemented as standard. |
| Backups | Corrective; supports ongoing productivity in the case of an event; aligns to the disaster recovery plan | **x** | Medium: Ongoing backups of data can aid in disaster recovery processes. It is advisable that this. Please note that any retention and preservation of customer and employee data should adhere to various laws such as the GDPR (Where Applicable) This process should also be automated and ran at frequent intervals. |
| Password management system | Corrective; password recovery, reset, lock out notifications | **x** | Medium: As the customer and employee base expands, a password management system would need to be implemented to insure that the customer and employee’s data is safe. Rotating passwords, minimum lengths and complexity requirements will minimize the risk of passwords being compromised both on site and for customers. |
| Antivirus (AV) software | Corrective; detect and quarantine known threats | **x** | High: Links IDS, Antivirus software is vital for employee workstations and any servers. This should be treated as a priority. |
| Manual monitoring, maintenance, and intervention | Preventative/corrective; required for legacy systems to identify and mitigate potential threats, risks, and vulnerabilities | **x** | High: The IT department may have to manually update, backup and decommission or otherwise manage legacy systems that may no longer qualify for vendor specific support. |

|  |  |  |  |
| --- | --- | --- | --- |
| **Physical Controls** | | | |
| **Control Name** | **Control type and explanation** | **Needs to be implemented**  **(X)** | **Priority** |
| Time-controlled safe | Deterrent; reduce attack surface/impact of physical threats | **x** | Low: Implementing safes for physical devices which may pose a risk of theft is good practice. Having these safes automatically lock after a time period has elapsed reduces the risk of onsight thefts |
| Adequate lighting | Deterrent; limit “hiding” places to deter threats | **x** | Medium: Personal safety and onsight identification is important for any business |
| Closed-circuit television (CCTV) surveillance | Preventative/detective; can reduce risk of certain events; can be used after event for investigation | **x** | High: Should be implemented in high risk areas. Server rooms, till areas etc. |
| Locking cabinets (for network gear) | Preventative; increase integrity by preventing unauthorized personnel/individuals from physically accessing/modifying network infrastructure gear | **x** | High: Securing network apparatus correctly is not just a security issue but a safety one as well. |
| Signage indicating alarm service provider | Deterrent; makes the likelihood of a successful attack seem low | **x** | Low: This is may be a decent practice to implement in more public areas of the business. |
| Locks | Preventative; physical and digital assets are more secure | **x** | High: This can be achieved by physical door locks or MFA tokens for digital assets. |
| Fire detection and prevention (fire alarm, sprinkler system, etc.) | Detective/Preventative; detect fire in the toy store’s physical location to prevent damage to inventory, servers, etc. | **x** | High: This links back to disaster recovery and is needed by any business. |