# Controls assessment

## 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; prevents abuse of privileges by ensuring that users have the minimum amount of permissions to perform their jobs. | X | High |
| Disaster recovery plans | Corrective; minimizes the effect of incidents on assets and productivity. | X | High |
| Password policies | Preventative; minimizes the likelihood of account compromise through brute force or dictionary attack techniques | X | High |
| Access control policies | Preventative; increase confidentiality and integrity of data | X | High |
| Account management policies | Preventative; reduce attack surface and the impact an insider threat could have | X | High/  Medium |
| Separation of duties | Preventative; reduces the chance of system abuse by involving multiple parties | X | High |

|  |  |  |  |
| --- | --- | --- | --- |
| **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 | NA | NA |
| Intrusion Detection System (IDS) | Detective; enhances security team’s detection and consequently its responsiveness to security incidents | X | High |
| Encryption | Deterrent; ensures confidentiality of data | X | High/  Medium |
| Backups | Corrective; part of the disaster recovery plan to restore systems and productivity | X | High |
| Password management system | Corrective; password recovery, reset, lock out notifications | X | High/  Medium |
| Antivirus (AV) software | Corrective; provides alerts and quarantine steps when malware is detected | X | High |
| Manual monitoring, maintenance, and intervention | Preventative/corrective; mitigates risk to particularly vulnerable assets, such as legacy systems | X | High |

|  |  |  |  |
| --- | --- | --- | --- |
| **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 | Medium/  Low |
| Adequate lighting | Deterrent; provides visibility to detect threats to assets | X | Medium/  Low |
| Closed-circuit television (CCTV) surveillance | Preventative/detective; provides data for security investigation and response | X | High/  Medium |
| Locking cabinets (for network gear) | Preventative; ensures access is limited to authorized staff | X | Medium |
| Signage indicating alarm service provider | Deterrent; prevents some would-be attackers | X | Low |
| Locks | Preventative; limits access to assets | X | High |
| Fire detection and prevention (fire alarm, sprinkler system, etc.) | Detective/Preventative; enhances detection and response of fire-related incidents | X | Medium/  Low |