Complete i.t.
TECHNOLOGY ASSURANCE

# Cybersecurity Overview

Version 1.0
(512) 674-4134
service@completeit.com

Microsoft
Cloud Solution Provider

Complete IT recommends that customers adhere to best-practices as defined by the Center for Internet Security (CIS). This list of controls represents a minimum standard of information security for all enterprises and is designed to protect organizations from common cyber-attack vectors. 56 cyber defense safeguards are organized below according to the following categories:

| |
|---|
| Standard (included with every Complete IT Managed Services Agreement) |
| Optional (requires recommended, but optional services) |
| Shared (requires cooperation and agreement between Complete IT and its customer) |
| Customer (outside of our scope of services) |

This information is provided freely in accordance with the Creative Commons public license found here. For additional information, please refer to https://www.cisecurity.org/controls.

| Inventory and Control of Enterprise Assets | | | |
|---|---|---|---|
| 1.1 | Establish and Maintain Detailed Enterprise Asset Inventory | Establish and maintain an accurate, detailed, and up-to-date inventory of all enterprise assets with the potential to store or process data, to include: end-user devices (including portable and mobile), network devices, non-computing/IoT devices, and servers. Ensure the inventory records the network address (if static), hardware address, machine name, enterprise asset owner, department for each asset, and whether the asset has been approved to connect to the network. For mobile end-user devices, MDM type tools can support this process, where appropriate. This inventory includes assets connected to the infrastructure physically, virtually, remotely, and those within cloud environments. Additionally, it includes assets that are regularly connected to the enterprise's network infrastructure, even if they are not under control of the enterprise. Review and update the inventory of all enterprise assets bi-annually, or more frequently. | Optional (Microsoft 365) |
| 1.2 | Address Unauthorized Assets | Ensure that a process exists to address unauthorized assets on a weekly basis. The enterprise may choose to remove the asset from the network, deny the asset from connecting remotely to the network, or quarantine the asset. | Shared |

|  |  |  |  |
|---|---|---|---|
| **Inventory and Control of Software Assets** |  |  |  |
| 2.1 | Establish and Maintain a Software Inventory | Establish and maintain a detailed inventory of all licensed software installed on enterprise assets. The software inventory must document the title, publisher, initial install/use date, and business purpose for each entry; where appropriate, include the Uniform Resource Locator (URL), app store(s), version(s), deployment mechanism, and decommission date. Review and update the software inventory bi-annually, or more frequently. | Shared |
| 2.2 | Ensure Authorized Software is Currently Supported | Ensure that only currently supported software is designated as authorized in the software inventory for enterprise assets. If software is unsupported, yet necessary for the fulfillment of the enterprise's mission, document an exception detailing mitigating controls and residual risk acceptance. For any unsupported software without an exception documentation, designate as unauthorized. Review the software list to verify software support at least monthly, or more frequently. | Shared |
| 2.3 | Address Unauthorized Software | Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently. | Shared |
| **Data Protection** |  |  |  |
| 3.1 | Establish and Maintain a Data Management Process | Establish and maintain a data management process. In the process, address data sensitivity, data owner, handling of data, data retention limits, and disposal requirements, based on sensitivity and retention standards for the enterprise. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard. | Shared |
| 3.2 | Establish and Maintain a Data Inventory | Establish and maintain a data inventory, based on the enterprise's data management process. Inventory sensitive data, at a minimum. Review and update inventory annually, at a minimum, with a priority on sensitive data. | Shared |
| 3.3 | Configure Data Access Control Lists | Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. | Shared |
| 3.4 | Enforce Data Retention | Retain data according to the enterprise's data management process. Data retention must include both minimum and maximum timelines. | Shared |
| 3.5 | Securely Dispose of Data | Securely dispose of data as outlined in the enterprise's data management process. Ensure the disposal process and method are commensurate with the data sensitivity. | Optional (Microsoft 365) |
| 3.6 | Encrypt Data on End-User Devices | Encrypt data on end-user devices containing sensitive data. Example implementations can include: Windows BitLocker®, Apple FileVault®, Linux® dm-crypt. | Optional (Microsoft 365) |

| Secure Configuration of Enterprise Assets and Software | | | |
|---|---|---|---|
| 4.1 | Establish and Maintain a Secure Configuration Process | Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard. | Optional (Microsoft 365) |
| 4.2 | Establish and Maintain a Secure Configuration Process for Network Infrastructure | Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard. | Shared |
| 4.3 | Configure Automatic Session Locking on Enterprise Assets | Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes. | Shared |
| 4.4 | Implement and Manage a Firewall on Servers | Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent. | Standard |
| 4.5 | Implement and Manage a Firewall on End-User Devices | Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed. | Standard |
| 4.6 | Securely Manage Enterprise Assets and Software | Securely manage enterprise assets and software. Example implementations include managing configuration through version-controlled-infrastructure-as-code and accessing administrative interfaces over secure network protocols, such as Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS). Do not use insecure management protocols, such as Telnet (Teletype Network) and HTTP, unless operationally essential. | Standard |
| 4.7 | Manage Default Accounts on Enterprise Assets and Software | Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable. | Shared |

| | | | |
|---|---|---|---|
| **Account Management** | | | |
| 5.1 | Establish and Maintain an Inventory of Accounts | Establish and maintain an inventory of all accounts managed in the enterprise. The inventory must include both user and administrator accounts. The inventory, at a minimum, should contain the person's name, username, start/stop dates, and department. Validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently. | Shared |
| 5.2 | Use Unique Passwords | Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA. | Shared |
| 5.3 | Disable Dormant Accounts | Delete or disable any dormant accounts after a period of 45 days of inactivity, where supported. | Shared |
| 5.4 | Restrict Administrator Privileges to Dedicated Administrator Accounts | Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account. | Shared |
| **Access Control Management** | | | |
| 6.1 | Establish an Access Granting Process | Establish and follow a process, preferably automated, for granting access to enterprise assets upon new hire, rights grant, or role change of a user. | Shared |
| 6.2 | Establish an Access Revoking Process | Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails. | Shared |
| 6.3 | Require MFA for Externally-Exposed Applications | Require all externally-exposed enterprise or third-party applications to enforce MFA, where supported. Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this Safeguard. | Shared |
| 6.4 | Require MFA for Remote Network Access | Require MFA for remote network access. | Standard |
| 6.5 | Require MFA for Administrative Access | Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-party provider. | Standard |

| | | | |
|---|---|---|---|
| **Continuous Vulnerability Management** | | | |
| 7.1 | Establish and Maintain a Vulnerability Management Process | Establish and maintain a documented vulnerability management process for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard. | Shared |
| 7.2 | Establish and Maintain a Remediation Process | Establish and maintain a risk-based remediation strategy documented in a remediation process, with monthly, or more frequent, reviews. | Shared |
| 7.3 | Perform Automated Operating System Patch Management | Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis. | Standard |
| 7.4 | Perform Automated Application Patch Management | Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis. | Standard |
| **Audit Log Management** | | | |
| 8.1 | Establish and Maintain an Audit Log Management Process | Establish and maintain an audit log management process that defines the enterprise's logging requirements. At a minimum, address the collection, review, and retention of audit logs for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard. | Optional (Threat Monitoring) |
| 8.2 | Collect Audit Logs | Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets. | Optional (Threat Monitoring) |
| 8.3 | Ensure Adequate Audit Log Storage | Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process. | Optional (Threat Monitoring) |
| **Email and Web Browser Protections** | | | |
| 9.1 | Ensure Use of Only Fully Supported Browsers and Email Clients | Ensure only fully supported browsers and email clients are allowed to execute in the enterprise, only using the latest version of browsers and email clients provided through the vendor. | Shared |
| 9.2 | Use DNS Filtering Services | Use DNS filtering services on all enterprise assets to block access to known malicious domains. | Optional (Firewall Security Suite) |

| | | | |
|---|---|---|---|
| **Malware Defenses** | | | |
| 10.1 | Deploy and Maintain Anti-Malware Software | Deploy and maintain anti-malware software on all enterprise assets. | Optional (Threat Monitoring) |
| 10.2 | Configure Automatic Anti-Malware Signature Updates | Configure automatic updates for anti-malware signature files on all enterprise assets. | Optional (Threat Monitoring) |
| 10.3 | Disable Autorun and Autoplay for Removable Media | Disable autorun and autoplay auto-execute functionality for removable media. | Shared |
| **Data Recovery** | | | |
| 11.1 | Establish and Maintain a Data Recovery Process | Establish and maintain a data recovery process. In the process, address the scope of data recovery activities, recovery prioritization, and the security of backup data. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard. | Standard |
| 11.2 | Perform Automated Backups | Perform automated backups of in-scope enterprise assets. Run backups weekly, or more frequently, based on the sensitivity of the data. | Standard |
| 11.3 | Protect Recovery Data | Protect recovery data with equivalent controls to the original data. Reference encryption or data separation, based on requirements. | Standard |
| 11.4 | Establish and Maintain an Isolated Instance of Recovery Data | Establish and maintain an isolated instance of recovery data. Example implementations include, version controlling backup destinations through offline, cloud, or off-site systems or services. | Standard |
| **Network Infrastructure Management** | | | |
| 12.1 | Ensure Network Infrastructure is Up-to-Date | Ensure network infrastructure is kept up-to-date. Example implementations include running the latest stable release of software and/or using currently supported network-as-a-service (NaaS) offerings. Review software versions monthly, or more frequently, to verify software support. | Shared |

|  |  |  |  |
|---|---|---|---|
| **Security Awareness and Skills Training** |  |  |  |
| 14.1 | Establish and Maintain a Security Awareness Program | Establish and maintain a security awareness program. The purpose of a security awareness program is to educate the enterprise’s workforce on how to interact with enterprise assets and data in a secure manner. Conduct training at hire and, at a minimum, annually. Review and update content annually, or when significant enterprise changes occur that could impact this Safeguard. | Shared |
| 14.2 | Train Workforce Members to Recognize Social Engineering Attacks | Train workforce members to recognize social engineering attacks, such as phishing, pre-texting, and tailgating. | Customer |
| 14.3 | Train Workforce Members on Authentication Best Practices | Train workforce members on authentication best practices. Example topics include MFA, password composition, and credential management. | Customer |
| 14.4 | Train Workforce on Data Handling Best Practices | Train workforce members on how to identify and properly store, transfer, archive, and destroy sensitive data. This also includes training workforce members on clear screen and desk best practices, such as locking their screen when they step away from their enterprise asset, erasing physical and virtual whiteboards at the end of meetings, and storing data and assets securely. | Customer |
| 14.5 | Train Workforce Members on Causes of Unintentional Data Exposure | Train workforce members to be aware of causes for unintentional data exposure. Example topics include mis-delivery of sensitive data, losing a portable end-user device, or publishing data to unintended audiences. | Customer |
| 14.6 | Train Workforce Members on Recognizing and Reporting Security Incidents | Train workforce members to be able to recognize a potential incident and be able to report such an incident. | Customer |
| 14.7 | Train Workforce on How to Identify and Report if Their Enterprise Assets are Missing Security Updates | Train workforce to understand how to verify and report out-of-date software patches or any failures in automated processes and tools. Part of this training should include notifying IT personnel of any failures in automated processes and tools. | Customer |
| 14.8 | Train Workforce on the Dangers of Connecting to and Transmitting Enterprise Data Over Insecure Networks | Train workforce members on the dangers of connecting to, and transmitting data over, insecure networks for enterprise activities. If the enterprise has remote workers, training must include guidance to ensure that all users securely configure their home network infrastructure. | Customer |
| **Service Provider Management** |  |  |  |
| 15.1 | Establish and Maintain an Inventory of Service Providers | Establish and maintain an inventory of service providers. The inventory is to list all known service providers, include classification(s), and designate an enterprise contact for each service provider. Review and update the inventory annually, or when significant enterprise changes occur that could impact this Safeguard. | Shared |

| Incident Response Management | | | |
|---|---|---|---|
| 17.1 | Designate Personnel to Manage Incident Handling | Designate one key person, and at least one backup, who will manage the enterprise’s incident handling process. Management personnel are responsible for the coordination and documentation of incident response and recovery efforts and can consist of employees internal to the enterprise, third-party vendors, or a hybrid approach. If using a third-party vendor, designate at least one person internal to the enterprise to oversee any third-party work. Review annually, or when significant enterprise changes occur that could impact this Safeguard. | Standard |
| 17.2 | Establish and Maintain Contact Information for Reporting Security Incidents | Establish and maintain contact information for parties that need to be informed of security incidents. Contacts may include internal staff, third-party vendors, law enforcement, cyber insurance providers, relevant government agencies, Information Sharing and Analysis Center (ISAC) partners, or other stakeholders. Verify contacts annually to ensure that information is up-to-date. | Standard |
| 17.3 | Establish and Maintain an Enterprise Process for Reporting Incidents | Establish and maintain an enterprise process for the workforce to report security incidents. The process includes reporting timeframe, personnel to report to, mechanism for reporting, and the minimum information to be reported. Ensure the process is publicly available to all of the workforce. Review annually, or when significant enterprise changes occur that could impact this Safeguard. | Standard |