BEST PRACTICES

Reasonable Security Practices

43 security best practices that all Illinois districts should implement to comply with the Student Online Personal Protection Act.

Beginning July 1, 2021, Illinois public schools must "implement and maintain reasonable security procedures and practices that otherwise meet or exceed industry standards designed to protect covered information from unauthorized access, destruction, use, modification, or disclosure" (105 ILCS 85/15). The Learning Technology Center selected 43 security best practices that all districts should implement to comply with legislation. The practices align with CIS Controls, a globally recognized cybersecurity standard, and are vetted by Illinois school district technology leaders.

HARDWARE ASSETS

Maintain Detailed Asset Inventory

Maintain an accurate and up-to-date inventory of all technology assets with the potential to store or process information. This inventory shall include all hardware assets, whether connected to the organization's network or not (CIS 1.4).

Address Unauthorized Assets

Ensure that unauthorized assets are either removed from the network, quarantined or the inventory is updated in a timely manner (CIS 1.6).

SOFTWARE ASSETS

Maintain Inventory of Authorized Software

Maintain an up-to-date list of all authorized software that is required in the enterprise for any business purpose on any business system (CIS 2.1).

Ensure Software is Supported by Vendor

Ensure that only software applications or operating systems currently supported by the software's vendor are added to the organization's authorized software inventory. Unsupported software should be tagged as unsupported in the inventory system (CIS 2.2).

Address unapproved software

Ensure that unauthorized software is either removed or the inventory is updated in a timely manner (CIS 2.6).

VULNERABILITY MANAGEMENT

Deploy Automated Operating System Patch Management Tools

Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor (CIS 3.4).

Deploy Automated Software Patch Management Tools

Deploy automated software update tools in order to ensure that third-party software on all systems is running the most recent security updates provided by the software vendor (CIS 3.5).

ADMIN PRIVILEGES

Change Default Passwords

Before deploying any new asset, change all default passwords to have values consistent with administrative level accounts (CIS 4.2).

Ensure the Use of Dedicated Administrative Accounts

Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities (CIS 4.3).

SECURE CONFIGURATION

Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software (CIS 5.1).

MAINTENANCE, MONITORING AND AUDITING LOGS

Activate audit logging

Ensure that local logging has been enabled on all systems and networking devices (CIS 6.2).

EMAIL AND BROWSERS

Ensure Use of Only Fully Supported Browsers and Email Clients

Ensure that only fully supported web browsers and email clients are allowed to execute in the organization, ideally only using the latest version of the browsers and email clients provided by the vendor (CIS 7.1).

Use of DNS Filtering Services

Use DNS filtering services to help block access to known malicious domains (CIS 7.7).

MALWARE

Ensure Anti-Malware Software and Signatures are Updated

Ensure that the organization's anti-malware software updates its scanning engine and signature database on a regular basis (CIS 8.2).

Configure Anti-Malware Scanning of Removable Devices

Configure devices so that they automatically conduct an anti-malware scan of removable media when inserted or connected (CIS 8.4).

Configure Devices Not To Auto-Run Content

Configure devices to not auto-run content from removable media (CIS 8.5).

NETWORK PORTS, PROTOCOLS, AND SERVICES

Apply Host-Based Firewalls or Port Filtering

Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed (CIS 9.4).

DATA RECOVERY

Ensure Regular Automated BackUps

Ensure that all system data is automatically backed up on a regular basis (CIS 10.1).

Perform Complete System Backups

Ensure that all of the organization's key systems are backed up as a complete system, through processes such as imaging, to enable the quick recovery of an entire system (CIS 10.2).

Ensure Protection of Backups

Ensure that backups are properly protected via physical security or encryption when they are stored, as well as when they are moved across the network. This includes remote backups and cloud services (CIS 10.4).

Ensure Backups Have At least One Non-Continuously Addressable Destination

Ensure that all backups have at least one backup destination that is not continuously addressable through operating system calls (CIS 10.5).

SECURE CONFIGURATION OF NETWORK DEVICES

Install the Latest Stable Version of Any Security-Related Updates on All Network Devices

Install the latest stable version of any security-related updates on all network devices (CIS 11.4).

BOUNDARY DEFENSE

Maintain an Inventory of Network Boundaries

Maintain an up-to-date inventory of all of the organization's network boundaries (CIS 12.1).

Deny Communication over Unauthorized Ports

Deny communication over unauthorized TCP or UDP ports or application traffic to ensure that only authorized protocols are allowed to cross the network boundary in or out of the network at each of the organization's network boundaries (CIS 12.4).

DATA PROTECTION

Maintain an Inventory of Sensitive Information

Maintain an inventory of all sensitive information stored, processed, or transmitted by the organization's technology systems, including those located on-site or at a remote service provider (CIS 13.1).

Remove Sensitive Data or Systems Not Regularly Accessed by Organization

Remove sensitive data or systems not regularly accessed by the organization from the network. These systems shall only be used as stand alone systems (disconnected from the network) by the business unit needing to occasionally use the system or completely virtualized and powered off until needed (CIS 13.2).

Encrypt the Hard Drive of All Mobile Devices.

Utilize approved whole disk encryption software to encrypt the hard drive of all mobile devices (CIS 13.6).

CONTROLLED ACCESS

Protect Information through Access Control Lists

Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities (CIS 14.6).

WIRELESS ACCESS CONTROL

Create Separate Wireless Network for Personal and Untrusted Devices

Create a separate wireless network for personal or untrusted devices. Enterprise access from this network should be treated as untrusted and filtered and audited accordingly (CIS 15.1).

Leverage the Advanced Encryption Standard (AES) to Encrypt Wireless Data

Leverage the Advanced Encryption Standard (AES) to encrypt wireless data in transit (CIS 15.7).

ACCOUNT MONITORING AND CONTROL

Lock Workstation Sessions After Inactivity

Automatically lock workstation sessions after a standard period of inactivity (CIS 16.11).

Disable Any Unassociated Accounts

Disable any account that cannot be associated with a business process or business owner (CIS 16.8)

Disable Dormant Accounts

Automatically disable dormant accounts after a set period of inactivity (CIS 16.9).

TRAINING

Implement a Security Awareness Program

Create a security awareness program for all workforce members to complete on a regular basis to ensure they understand and exhibit the necessary behaviors and skills to help ensure the security of the organization. The organization's security awareness program should be communicated in a continuous and engaging manner (CIS 17.3).

Train Workforce on Secure Authentication

Train workforce members on the importance of enabling and utilizing secure authentication (CIS 17.5).

Train Workforce on Identifying Social Engineering Attacks

Train the workforce on how to identify different forms of social engineering attacks, such as phishing, phone scams and impersonation calls (CIS 17.6).

Train Workforce on Sensitive Data Handling

Train workforce on how to identify and properly store, transfer, archive and destroy sensitive information (CIS 17.7).

Train Workforce on Causes of Unintentional Data Exposure

Train workforce members to be aware of causes for unintentional data exposures, such as losing their mobile devices or emailing the wrong person due to autocomplete in email (CIS 17.8).

Train Workforce Members on Identifying and Reporting Incidents

Train employees to be able to identify the most common indicators of an incident and be able to report such an incident (CIS 17.9).

Incident Response and Management

Document Incident Response Procedures

Ensure that there are written incident response plans that define roles of personnel as well as phases of incident handling/management (CIS 19.1).

Designate Management Personnel to Support Incident Handling

Designate management personnel, as well as backups, who will support the incident handling process by acting in key decision-making roles (CIS 19.3).

Maintain Contact Information For Reporting Security Incidents

Assemble and maintain information on third-party contact information to be used to report a security incident, such as Law Enforcement, relevant government departments, vendors, and ISAC partners (CIS 19.5).

Publish Information Regarding Reporting Computer Anomalies and Incidents

Publish information for all workforce members, regarding reporting computer anomalies and incidents to the incident handling team. Such information should be included in routine employee awareness activities (CIS 19.6).

LEARNING
TECHNOLOGY
CENTER of ILLINOIS

The Learning Technology Center is a statewide program that supports all public K-12 districts, schools, and educators through technology initiatives, services, and professional learning opportunities.

Email: support@ltcillinois.org
Web: ltcillinois.org