IPA Policy Manual
Chapter 5 – Association Operations

5.19 Data Security & Cyber Threats

Purpose & Scope

The Illinois Principals Association is committed to preventing theft of data and all other forms of cyber threats. The purpose of this policy is to establish standards for the acceptable use of equipment and any software that is owned and/or operated by IPA or equipment that accesses IPA's internal systems.

This policy applies to equipment owned and/or operated by IPA and to employees connecting to any IPA-owned network domain or cloud applications that are used in the course and scope of IPA business.

For purposes of this policy, the term "Employee" includes employees, consultants, volunteers, and all others acting on behalf of IPA who have: (1) internet access through IPA owned devices; (2) access to IPA networks; and (3) IPA email accounts.

Security-related events must be immediately reported to the Technology Service Specialist or Executive Director so that corrective measures can be prescribed as needed.

Anti-Virus & Malware Protection

All IPA computers and workstations must have approved anti-virus software installed and scheduled to run at regular intervals. In addition, the anti-virus software must be kept up to date. Virus-infected computers must be removed from the network until they are verified as virus-free. Any activities with the intention to create and/or distribute malicious programs into IPA's internal network (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) are prohibited.

All servers must have an approved anti-virus application installed and activated that offers real-time scanning protection to files and applications.

All mail servers must have either an external or internal anti-virus scanning application that scans all mail and file attachments destined to and from the mail server. All anti-virus applications must have automatic updates enabled and the status of automatic updates must be periodically verified.

Workstation Security

The following measures must be taken to ensure that exposure of sensitive information is restricted to authorized users.

- Restricting physical access to workstations to only authorized personnel.

- Configuring screen-locks to automatically lock the screen after a period of inactivity and requiring personnel to manually enable the screen-lock on workstations prior to leaving the area to prevent unauthorized access.
- Verifying personnel compliance said password policies and procedures.
- Ensuring workstations are used for authorized business purposes only.
- Ensuring workstations are rebooted or shut down at least once each week, which will allow software updates to be automatically installed.
- Ensuring that all workstations use a surge protector (not just a power strip) or a UPS (battery backup).

Software Installation

Employees may not install software on IPA's computing devices operated within the IPA internal network without explicit approval from the Technology Service Specialist or Executive Director.

Password Security Requirements

All user passwords (e.g., e-mail, web, desktop computer, etc.) must be kept private and conform to the following standards:

- Contain an upper-case character
- Contain a lower-case character
- Contain a number
- Contain a special character (e.g. @!.',#$%^&*()_+|~-=\`{}[]:";'<>/ etc.)

Multi-factor authentication (MFA) must be enabled on all accounts that provide such a feature, and MFA codes must be stored in an MFA authenticator mobile application. MFA backup codes should also be stored in a password manager to ensure their security, and if MFA backup codes are provided via a downloaded file, that file must be deleted, and purged from the trash-bin of the device.

Wireless & Remote Access

All wireless devices that reside at IPA and connect to an IPA internal network must:

- Be installed, supported, and maintained by the Technical Services Specialist.
- Use IPA approved authentication protocols and infrastructure.

Encryption Standards

All devices containing stored confidential or sensitive data owned by IPA must use an approved method of encryption to protect data.

Data Backup

Backup software shall be scheduled to run nightly to capture all incremental backup data from the previous day. Backup software shall be properly labeled and stored in a secure location other than IPA's premises.

Cyber Hygiene & Cybersecurity Education

IPA employees are required to participate in all scheduled and remedial cyber hygiene and/or cybersecurity training provided by IPA. Training may include, but is not limited to, online training, onsite training, and phishing testing.

Adopted: January 23, 2025