Approved by the AYBS Board on 3-13-25

IT Policy

Acceptable Use Policy

The Acceptable Use Policy (AUP) outlines the acceptable use of computer equipment and managed software. It is used for organizational purposes in serving the interests of the Organization, its members and fostering community baseball and softball. All members of the organization are to strictly use the organizational technology and information in the performance of their assigned roles and duties within the organization and within the Code of Conduct. All other uses are strictly prohibited.

Incident Response Policy

The incident response policy is part of an organization's Business Continuity Plan. It outlines an organization's response to an information security incident. The incident response policy should be documented separately from the Disaster Recovery Plan, as it focuses on procedures following a breach of data or other security incident.

All data breach and compromise of private data not limited to financial, or health must be immediately reported to the President and Vice President of Technology.

Vendor Management Policy

The vendor management policy validates a vendor's compliance and information security abilities. The policy should address the process to acquire vendors and how to manage all of an organization's vendors. The organization should trust that the third party vendor will appropriately safeguard the information that it is given. It is critical that the organization keeps a list of their vendors, and contacts for the vendors.

Password Creation and Management Policy

The password creation and management policy provides guidance on developing, implementing, and reviewing a documented process for appropriately creating, changing, and safeguarding strong and secure passwords used to verify user identities and obtain access for company systems or information. The policy should touch on training and awareness as to why it is so important to choose a strong password. It should include rules for changing temporary passwords and risks of reusing old passwords.

Passwords should not be shared, and upon turnover of accounts, new passwords must be created by the VP of Technology for new account members.

IT Policy

Access Authorization, Modification, and Identity Access (Account) Management

Using access authorization requires organizations to implement the Principle of Least Privilege. This is the idea that users and systems should only be given access to information needed to complete their job. The organization should create and document a process for establishing, documenting, reviewing, and modifying access to systems and sensitive information. This process usually involves IT, who allow access upon hiring and termination. Access must be granted based on valid access authorization, intended system usage, and other attributes required by organizations. An access authorization and modification map should be created in accordance with the access authorization policy and password management policy. These policies and procedures must be updated regularly as they are critical in data privacy.

Sports Engine

- As of 11/25/24, the Board voted for and approved: Every Divisional Director role is to be given Sports Engine registration access which includes: add, modify, delete, read all registration lists.
- As of 3/3/2025, Book Keeper Bryce Thompson, or subsequently approved accounting assistance to the Treasurer, is given Financial Access to obtain financial information for the purpose of accounting.

Constant Contact

- As of 11/25/24, the Board voted for and approved: The organizational role of Community Relations and Communication, and Club Baseball Divisional Director be given the Account Manager access.

Google Work Space - Restricted

Go Daddy - Restricted

Data Retention Policy

The data retention policy specifies the types of data the business must retain and for how long. The policy also states how the data will be stored and destroyed. This policy will help to remove outdated and duplicated data and create more storage space. A data retention policy will also help organize data so it can be used at a later date. Types of data include documents, customer records, transactional information, email messages, and contracts. This policy is essential to businesses that store sensitive information. Organizations should reference regulatory standards for their data retention requirements.

Approved by the AYBS Board on 3-13-25

IT Policy

Transition Policy - Surrender of Account Password Upon Resignation or Termination of Role from Organization

In order to facilitate the transition and onboarding of new board members or transitioning of responsibilities, all members are to surrender accounts, account information including vendor contacts, passwords, authentication, verification, reset codes and all related matters of control to the VP of Technology, Secretary or President within a 72 hour period upon request. This includes all subscriptions, software licenses, privileges, memberships and rights belonging to the organization.