

Coast Guard Auxiliary Association Information Systems Management Policy

Purpose

This policy establishes practices for the management of Association institutional data and the responsibilities for its protection. The policy applies to all institutional data: verbal, printed, electronic, and whether individually controlled, shared, stand alone, or networked.

The policy serves to:

- Ensure establishment, maintenance, and delivery of secure, trustworthy, stable, reliable, and accessible institutional data for shared access by Association users.
- Maximize the value received from this data asset by increasing its use of the data
- Improve direct access to data by end-users.
- Ensure compliance with state, federal, and Association privacy and security laws and regulations.
- Support the Association strategy to incorporate information technology as an integral part of decision-making, competitive positioning, and delivery of services.

Goals

Successful management and protection of information and data is critical to the functions of the Association. Through active planning, organization, and control of these resources, we will:

- Manage information as a strategic asset to improve the quality of services to Association users.
- Implement databases that are consistent, reliable, and accessible to meet requirements.
- Provide data management services which result in the highest quality data to all users.
- Implement and maintain security policies and procedures to protect data resources.

Policy Statement

Physical Security

- Data resources will be guarded and protected.
- Data will be shared based on Association policies, and federal and state law.

Safeguarding Data

- Data will be managed as an Association resource.
- Institutional data will be identified and defined.
- Contingency plans will be developed and implemented.

Data Strategies

- Databases will be developed based on needs of Association.
- Information quality will be actively managed.

Social Media

- Policy, guidance, and tools will be created and maintained to address Association participation in social media such as blogs, social networks, wikis, etc

Passwords, Electronic Mail, Mailing Lists

- Access to data will be authorized and managed.
- Any data collected must be explicitly described in a privacy statement accessible on the web site.
- Any use of the data for purposes not specifically required by the order process must be described.
- Customers must be given the option to disable any reuse of their information.
- Mailing list ownership is limited to two 'owners.'

Responsibilities

Every Director of the Association is responsible for ensuring compliance with this Association policy and must initiate corrective action if needed. Responsibilities include:

- Applying the guidelines included herein to the data under their stewardship
- Communicating this policy to staff
- Actively supporting strong data management through data stewardship
- Providing appropriate levels of privacy and security
- Ensuring training in security awareness and data management principles to workforce members whose jobs require them to access, maintain, or use this data