AWWA INFORMATION SECURITY AND ACCEPTABLE USE POLICY FOR SECTIONS

OVERVIEW

Protecting our members' personal information is a core responsibility of AWWA and its Sections. An effective information security program ensures trust between AWWA, the Sections, and our members. This policy covers all AWWA Section staff, contractors, and volunteers, including temporary staff, and vendors who utilize AWWA confidential data as defined below. AWWA employees are obligated to a separate policy. For more information, please review AWWA's Privacy Policy.

SECTION RESPONSIBILITIES

1. Information security is a responsibility everyone shares when accessing AWWA's proprietary and confidential data. For the purpose of this policy, "confidential data" includes any of the following:
    a. any member's personal information including name, email address, physical address, phone number, activities, or any other data about a specific person,
    b. financial data,
    c. non-public conference and meeting data, and
    d. any other data which, if disclosed, would create a negative impact on AWWA's reputation or competitive advantage.
2. Sections will follow industry best practices for ensuring the security of confidential data:
    a. Confidential data should not be stored or transported on portable storage devices (flash drives, memory cards, etc.).
    b. Confidential data must not be posted on a web site. Any personal information can only be posted on a website with each member's explicit permission in writing.
    c. Confidential data which has exceeded its usefulness or could be considered duplicative will be deleted in a timely manner.
    d. All computer systems storing confidential data must run current anti-virus/ malware software and must install security updates when available from the manufacturer.
    e. Sections will remove former employees' (including volunteers and consultants) access to confidential data immediately upon separation of employment.
    f. All systems containing confidential data must be protected by a complex password.
    g. Passwords should be changed on a regular basis.
    h. Sharing username/password combinations with anyone is discouraged.
3. Sections will establish and follow procedures to remain in compliance with regional cybersecurity and privacy regulations.
4. Sections will include an accurate privacy policy on their website.
5. Sections will notify AWWA Section Services immediately of any information security concerns which result in confidential data becoming available to non-authorized parties.
6. Sections will maintain adequate physical security to protect confidential data.

(continued on next page)

ACCEPTABLE USE POLICY

AWWA allows sections to use AWWA proprietary data and confidential data for the purpose of providing services to AWWA members. Some information may be shared with third-party vendors and volunteers when it adds value to membership. Sections are not permitted to sell membership data under any circumstance.

Data must not be shared when the intended use of the data does not advance the work of the Association and the Sections. For example, contact lists cannot be sold to or shared with marketing agencies for the purpose of promoting a member's business activities.