CONFIDENTIAL MEMBER INFORMATION POLICY

PURPOSE

This policy establishes the requirements for using confidential member information in public awareness programs. It describes how the information will be protected and how certain information will be communicated to stakeholders.

SCOPE

This policy applies to information that has been provided to the Pipeline Association for Public Awareness by its Members for use in public awareness programs. It does not address provisions for handling *Sensitive Security Information (SSI) or Protected Critical Infrastructure Information (PCII),* as defined by Federal Regulation. Members must clearly identify any information that is SSI or PCII.

DEFINITIONS

Association – is the Pipeline Association for Public Awareness

Confidential Member Information (CMI) – is information that has been identified as "confidential" by the Member, except this shall not include: information that is publicly available, information that has been provided to the Association through the member registration process, and information that is acquired by the Association from other sources.

Members - are "Pipeline Members" as defined in the bylaws of the organization and their representatives.

Programs – are the public awareness programs executed by the Association on behalf of participating Members, as defined in the program outlines published by the Association.

Stakeholders – are the recipients of communications disseminated through the public awareness programs executed by the Association and include the target audiences identified in the program outlines.

REQUIREMENTS

General

1. These requirements apply to the Associations Directors, Members, employees, contractors, and other representatives.

2. Confidential Member Information (CMI) shall only be used for the purposes of the Programs.

CONFIDENTIAL MEMBER INFORMATION POLICY

Identification

1. When Members provide information to the Association, they should identify which information they consider to be CMI.

2. Association may identify information as CMI even if the Member does not identify the information as confidential information. Digital GIS pipeline centerline information and stakeholder mailing addresses or email addresses will be treated as CMI, unless it has been classified as non-confidential by the member providing the information.

Receipt, Processing and Storage

1. It is the intent of the Association to only retain information that is relevant to the Programs. If the information received by the Association includes additional information that is not relevant to the Programs (e.g., security assessments, vulnerability evaluations, construction information, operating information, business information, other proprietary information), that information shall be deleted, destroyed or returned to the Member.

2. CMI shall be stored in a secure environment which is not accessible to unauthorized personnel.

3. Access to the stored information shall be limited to individuals who are involved in executing the Programs and who are bound by the requirements of this policy.

Use of Information in Programs

1. CMI shall only be used for the purposes of the Programs and may not be used for any other purpose without the written permission of the Member.

2. Any additional information developed from CMI provided by a Member shall be treated in the same manner as CMI provided directly from the Member (i.e. a calculated recommended minimum evacuation distance based on pipeline size and pipeline pressure).

3. Certain CMI may be disclosed to specific Stakeholders through the Programs, including:
    a. General Pipeline Location – to all Stakeholders
    b. Pipeline Size – to Emergency Responders, Schools, and Public Officials
    c. Pipeline Pressure - this information will not be disclosed through any program
    d. Evacuation Distances – to Emergency Responders, Schools, and Public Officials
    e. MSDS sheets – to Emergency Responders, Schools, and Public Officials
    f. Site Specific Emergency Procedures – to Emergency Responders, Schools, and Public Officials

4. Stakeholders who are authorized access to CMI shall be required to obtain a username and password for access to the information and must agree to the terms and conditions applicable to the Programs prior to accessing the information.

5. Members will also have access to the information provided to the Stakeholders through the Programs. Members are also required to obtain a username and password for access to the information and must agree to the terms and conditions applicable to the Programs prior to accessing the information.

Warranties

1. Program materials shall contain appropriate language to inform Stakeholders that no representations or warranties as to the accuracy, completeness, or fitness for a particular purpose of the information are being made by the Association or its participating Members.

Duration

1. The requirements of this Policy shall remain in effect if the Programs using CMI continue or if a Member continues to participate in the Programs using CMI.

2. If the Programs are discontinued or a Member's participation in a Program is discontinued, the associated CMI shall promptly be returned to the Member or securely disposed of in a manner that prevents unauthorized access or disclosure.

Ownership

1. All CMI provided to the Association shall remain the sole property of the Member providing the information. The Association only has the right to use the information in the Programs.

Required Disclosure

1. If the Association is requested or required by subpoena, civil investigation, court order, demand or similar legal process to disclose any CMI, the Association shall promptly notify the appropriate Members, will cooperate with all parties involved and will strive to protect the information to the extent permitted under the law.

Data Security

1. Members can upload data files directly to the Association's secure Sharefile account with the link to the FTP site on the Program Documentation landing page. Only certain individuals have access to the section where incoming files are received and stored. ShareFile provides a full spectrum of measures to protect client authentication,

authorization, and file transfers, including two-factor verification, SAML integration, password policies, bank-level encryption, and TLS protocols with up to 256-bit encryption. Data at rest is protected using AES 256-bit encryption with unique per-file keys. If Members send data files to the Association via email, they will be stored in the Association's Sharefile account.

2. Member data is structured for use by the applications and uploaded to an MS SQL database in the Association's Microsoft Azure account. All sensitive information stored in the database is encrypted using industry best practices and standards, and access to the information in the database is be restricted to only those individuals who require it to perform their job duties. All database passwords, encryption keys, and other credentials are securely stored and managed according to industry best practices and standards.

3. All sensitive information transmitted between the server and client is encrypted using a strong encryption algorithm and key length that meet industry best practices and standards. All cryptographic keys and certificates used in the web application are securely stored and managed according to industry best practices and standards.

4. The web applications use HTTPS (via Secure Sockets Layer (SSL)) to establish a secure connection between the server and client. The use of HTTP is strictly prohibited.

5. Cryptographic controls are periodically reviewed and updated to ensure they continue to meet industry best practices and standards.

6. Any suspected or actual compromise of cryptographic controls or sensitive information is reported immediately to the appropriate personnel and investigated thoroughly.