Analytical, Life Science & Diagnostics Association (ALDA)
Information Security Policies

As of January, 2023

Introduction

Information security is a holistic discipline, meaning that its application, or lack thereof, affects all facets of an organization or enterprise. The goal of the ALDA Information Security Policies is to protect the Confidentiality, Integrity, and Availability of the data employed within the organization while providing value to the way we conduct business. Protection of the Confidentiality, Integrity, and Availability are basic principles of information security, and can be defined as:

- Confidentiality – Ensuring that information is accessible only to those entities that are authorized to have access.
- Integrity – Protecting the accuracy and completeness of information and the methods that are used to process and manage it.
- Availability – Ensuring that information assets (information, systems, facilities, networks, and computers) are accessible and usable when needed by an authorized entity.

ALDA has recognized that our business information is a critical asset and as such our ability to manage, control, and protect this asset will have a direct and significant impact on our future success.

This document contains the framework to ensure that the enterprise can efficiently and effectively manage, control and protect its business information assets and those information assets entrusted to ALDA by its stakeholders, partners, customers and other third parties.

Purpose

The purpose of the ALDA Information Security Policies is to describe the actions and behaviors required to ensure that due care is taken to avoid inappropriate risks to ALDA, its business partners, and its stakeholders.

Audience

The ALDA Information Security Policies apply equally to any individual, entity, or process that interacts with any ALDA Information Resource.

Responsibilities

Executive Management

- Ensure that appropriate risk-based policies are implemented to protect the confidentiality, integrity, and availability of all Information Resources collected or maintained by or on behalf of ALDA.
- Ensure that information security processes are integrated with strategic and operational planning processes to secure the organization's mission.
- Ensure adequate information security financial and personnel resources are included in the budgeting and/or financial planning process.

All Employees, Contractors, and Other Third-Party Personnel

- Understand their responsibilities for complying with the ALDA Information Security Policies.
- Agree to abide by all applicable policies, standards, and guidelines that have been established.
- Use ALDA Information Resources in compliance with all ALDA Information Security Policies.
- Seek guidance from the CEO for questions or issues related to information security.

Policy Overview

- ALDA maintains and communicates Information Security Policies consisting of topic-specific policies, standards, procedures and guidelines that:
  - Serve to protect the Confidentiality, Integrity, and Availability of the Information Resources maintained within the organization using administrative, physical and technical controls.
  - Provide value to the way we conduct business and support institutional objectives.
  - Comply with all regulatory and legal requirements, including:
    - HIPAA Security Rule,
    - State breach notification laws,
    - PCI Data Security Standard,
    - Contractual agreements,
    - All other applicable federal and state laws or regulations.

Policy Enforcement

Personnel found to have violated these policies may be subject to disciplinary action, up to and including termination of employment, and related civil or criminal penalties.

Any vendor, consultant, or contractor found to have violated this policy may be subject to sanctions up to and including removal of access rights, termination of contract(s), and related civil or criminal penalties.

Policies:

Association Management System Security

ALDA may elect to host its website and/or database on an Association Management System (AMS) managed by a third party. ALDA agrees to follow these policies related to AMS security:

- ALDA will use a secure password manager to keep track of AMS system passwords. Passwords will not be stored unencrypted and without password protection.
- When accessing AMS systems, ALDA agrees that its staff will select strong passwords that meet the latest industry best practices.
- ALDA agrees it will not store credit card information once the initial transaction is complete. ALDA will not store credit card information for the sole purpose of possibly issuing additional charges, credits or refunds and instead rely on your payment gateway to process refunds.
- ALDA agrees to not store sensitive information in text or comments fields. Sensitive information includes credit card numbers, social security numbers, date of birth, or personal health information. If ALDA wishes to store this information, ALDA will contact AMS to determine an appropriate method for collecting and storing sensitive information.
- ALDA will maintain up-to-date anti-virus software on all systems.
- ALDA will not knowingly upload programs or files that contain malicious code, including trojans, viruses and worms.
- ALDA agrees to report any suspicious activity or possible breaches to its IT manager and AMS host.

Access Controls

Only ALDA staff and approved, contracted third party partners will have access to ALDA's data, including the backend of the AMS and the shared drive maintained by staff. The ALDA CEO will approve access for staff, working with our third party IT manager. For any accounting systems, online banking, or other online accounts, the ALDA CEO will approve access for relevant staff, working with the appropriate third party when necessary (our accountants for Sage Intacct, etc.).

Data Collection

Data shall be collected in a lawful and appropriate manner in accordance with the requirements of applicable legislation, government mandates and ALDA policies.

Data Use and Disclosure

Data shall be used and disclosed in a lawful and appropriate manner in accordance with the contractual obligations of ALDA, requirements of applicable legislation, government mandates and ALDA policies.

Data Security

Data shall remain protected and secure in accordance with the requirements of applicable legislation, government mandates and ALDA policies.

Data Privacy

Data shall remain private and shall only be disclosed to authorize parties in accordance with the requirements of applicable legislation, government mandates and ALDA policies.

Data Availability

Retention and Disposal. Data shall be retained and disposed of in a lawful and appropriate manner. Appropriate controls shall be applied to ensure that data remains available to bona fide persons within ALDA.

Staff should have access to data in the central repository for the data they generate. Staff should have access to the centrally stored data required to successfully accomplish their job duties.

Data Integrity

Appropriate controls shall be applied to ensure that data remains complete and accurate.

Data Compliance

All Data Sources and Systems shall remain compliant with ALDA following business rules. ALDA maintains a single primary system of record - MatrixMaxx is the single system of record for Membership, individual and company records and all other data entities defined in this policy. It is the first choice to be used to develop or store new data in the future

Historical Data is automatically exempted from this Policy.

ALDA will maintain multiple data collection systems (i.e. Event Espresso). Data from those systems will be synchronized or duplicated in MatrixMaxx either thru an automated or manual interface.

New Data Requirements

All new systems, data tracking, data sources, and data reporting requirements must comply based on the Compliance Section of this document. *Example – A new event hosted by a Council must use MatrixMaxx to track their Event, or they must submit a request with their requirements and a business case to propose taking another approach.*

New Contracts

Any future 3rd Party Agreements should be written to be consistent with this policy and must be reviewed by the President & CEO.

Reviewing Current Contracts

All current contracts will be reviewed by staff and the CEO at least annually, including a review of all IT platforms and partners.

Insurance Policies

ALDA will carry the following insurance:

1. Directors & Officers Insurance
2. General Liability Insurance
3. Cyber Security Insurance

Incident Response & Disaster Recovery Plan

Cybersecurity insurance is in place and a communications plan is in place in the case a breach does happen. Insurance policies are reviewed and renewed annually. The communications plan primarily involves working directly with ALDA's contracted third parties who oversee whatever was breached; if it is the files on our server, we will work with our IT manager. If it pertains to our website, we will work with our AMS provider. If it involves any of our online banking institutions, we will work directly with our client management contact. If it involves any of our benefits, we will work with our benefits broker.

Data Backup and Restoration Plan

Our IT Manager oversees our Google suite/Drive where all of our electronic association data is stored. They ensure it is safe and backed up. Likewise, our contracted AMS provider is responsible for nightly backing up of the data on our AMS.

Data Availability, Retention and Disposal

Data shall be retained and disposed of in a lawful and appropriate manner. Appropriate controls shall be applied to ensure that data remains available to bona fide persons within ALDA.

Data Usage Statement

Data collected through the ALDA website is used to inform decisions and better serve members. Only the personal information that is knowingly provided is collected and stored. If our privacy policy changes, we will notify users through our website.

ALDA does not collect personal information from users browsing our website. Aggregate data are only used for internal and marketing purposes and do not provide any personally identifying information. Members and meeting registrants provide limited information such as name, organization, phone, and email address.

Additionally, we may collect specific information regarding what recipients do with email, such as clicks on the links provided in messages, dates and times, message

numbers, tracking URL numbers, and destination pages. This information is not sold or distributed but may be used to improve web content; to respond to visitors' interests, needs, and preferences; and to develop new products and services. Information about event registrants will not be provided to sponsors and other third parties.

For purposes of the Data Protection Act(s) 1984 and 1998, ALDA and its agents must store, host, and otherwise process the information (including personal data) supplied by users when registering for this website. If you reside in the European Union, please indicate your consent that the personal information you have provided may be transferred and stored in countries outside of the EU, including the United States.

ALDA does not disclose credit card account information. Cookies may be used to facilitate automated activity, store, and track passwords, determine appropriate solicitations, and review navigation patterns. Cookies are not used to analyze information that users have unknowingly provided.

The ALDA website may contain links to other web sites. ALDA has no control over and is not responsible for the privacy policies or content of such sites.

If you have questions or suspect personal information has been used by ALDA in a manner that does not comply with this privacy statement, please contact us via email.