ALPHA DELTA STATE OHIO EDUCATIONAL FOUNDATION (ADSOEF)

CYBERSECURITY POLICY AND AGREEMENT

Operating Policy

Effective Date: 06/17/2024

Review Date(s):

Revision Date(s):

Number of Pages: 4

I. Purpose

ADSOEF collects, manages and stores information on a regular basis in order to support its mission and purposes. ADSOEF is committed to preserving the confidentiality, integrity and availability of its information and assets.

ADSOEF must protect its information assets, provide for the integrity of business processes and records, and comply with applicable laws and regulations.

ADSOEF must protect all sensitive data and digital assets from malicious attack and protect the confidentiality, integrity and availability of sensitive information, systems, and data.

This policy reinforces the commitment, establishes high-level functions of an information security program, and outlines information security requirements to safeguard information assets.

II. Scope

This document applies to the use of information, information systems, electronic and computing devices, applications, and network resources used to conduct business on behalf of ADSOEF. The document applies to all board members, officers, committee members and volunteers. Other entities that voluntarily use or participate in services must agree to comply with this document, with respect to those services, as a condition.

III. Responsibility

The Board of Directors (BOD) is responsible for the development and ongoing maintenance of this policy.

IV. Compliance

Compliance with this policy is mandatory.

V. Objectives

The goal of this policy is to manage risk and achieve information security objectives through the establishment of supporting guidelines, processes and functions. The information security objectives are to:

- protect donor data and non-public information;
- comply with applicable laws, regulations and contractual obligations with stakeholders;
- establish a governance structure to effectively and efficiently manage information security risk;
- manage identified security risks to an acceptable (i.e., risk tolerance) level through design, implementation and maintenance risk remediation plans;
- establish a culture of accountability and increase the level of awareness of all personnel in order to meet information security requirements; and
- establish responsibility and accountability for information security policies and governance.

ADSOEF is committed to continual improvement to help ensure that its applicable information security objectives are met and it is able to adapt to changes in the cyber threat landscape and account for evolving organizational, legal and regulatory requirements.

VI. How to Achieve

- ADSOEF members who access internal data and devices must have a password with a minimum length of 12 characters, including at least one capital letter, one number and one special character.
- All members or participants shall have in place on their *bring your own device* (BYOD) personal devices) appropriate and approved security and risk mitigation mechanisms/solutions to reduce the risk of ADSOEF assets and information; i.e., approved antivirus and security software, password manager software, virtual private network (VPN) software, etc. All members need to have appropriate security/antivirus measures on their personal devices to reduce the risk of a security breech.
- Outline and delineate roles and responsibilities of board members and leaders of ADSOEF. Apply Role Based Access Controls (RBAC) to align roles and necessary access to those roles; i.e., Treasurer needs access to A, B, C things but not D, E, F. Board members vs Chairman and Vice Chairman accesses to data and information systems. Include Redundancy in the case of extreme circumstances. This helps with inventory of permissions for oversight and accountability, but also in the event something bad does happen, you can quickly pinpoint the *who* to narrow the search during investigation.

- Users and authoritative personnel should not store critical data on (or only on, as needed) personal devices. Find and implement some form of shared services where critical data elements can be stored and accessed and reduce the risk if someone's personal devices breaks or due to some other unforeseen emergency, you won't lose all the data stored on one person's computer. Using one of these programs adds a layer of protection.
- Implement, where applicable, individual user agreements to physically sign accepting rules of behavior. In parallel and where applicable, implement user login banners on information assets, systems, and data to inform users of consent and acknowledgement of acceptable behavior while conducting official business for ADSOEF (CISA 9-lines reference).

ALPHA DELTA STATE OHIO EDUCATIONAL FOUNDATION (ADSOEF)

Cybersecurity Policy Agreement

Summary

_____ 1. I verify that I have received and read the Cybersecurity Policy.

_____ 2. I verify that my personal computer is password protected.

_____ 3. I verify that my personal computer has appropriate security and antivirus programs to reduce the risk of breech.

_____ 4. In signing this statement, I confirm that I agree to abide by the guidelines in The ADSOEF Cybersecurity Policy.

Signature

Date