OXNARD UNION HIGH SCHOOL DISTRICT RETIREE HEALTH BENEFITS TRUST

CYBERSECURITY POLICY STATEMENT

I. Introduction

The Oxnard Union High School District Retiree Health Benefits Trust ("Trust") adopts this policy to protect the Trust's network from threat activity. Trusts often hold assets and maintain personal data on participants, making the Trust a target for cyber threats. Trustees and plan fiduciaries have an obligation to ensure proper mitigation of cybersecurity risks.

II. Purpose

The purpose of this policy is to identify and assess any cybersecurity risks related to stored nonpublic information, including appropriate actions if a cybersecurity breach occurs and strong data access control procedures. Trustees should also understand how any Trust service providers handle and protect the Trust's data.

III. Cyber Security Program

The purpose of a cybersecurity program is to identify and asses internal and external cybersecurity risks that may threaten the confidentiality, integrity, and availability of stored nonpublic information. The Trusts will adopt and implement document information security policies, procedures, guidelines, and standards to protect the security of the IT infrastructure and data stored on the system.

The Cybersecurity program will:

- Identify the risks to assets, information and systems.
- Protect each of the necessary assets, data and systems.
- Detect and response to cybersecurity events.
- Recover from the event.
- Disclose the event as appropriate.
- Restore normal operations and services..

IV. Risk Assessments

The Trust will conduct periodic risk assessments to identify, estimate, and prioritize information system risks. This risk assessment will:

- Identify, assess, and document how identified cybersecurity risks or threats are evaluated and categorized.

- Establish criteria to evaluate the confidentiality, integrity, and availability of the information systems and nonpublic information, and document how existing controls address the identified risks.
- Describe how the cybersecurity program will mitigate or accept the risks identified.
- Facilitate the revision of controls resulting from changed in technology and emerging threats.
- Be kept current to account for changes to information systems, nonpublic information, or business operations.

V. Annual Third Party Audit of Security Controls

The Trust will annually have an independent auditor assess the Trust's security control to provide a clear report of existing risks, vulnerabilities, and weaknesses.

As part of the audit program, the third party will produce:

- Audit reports, audit files, penetration test reports and supporting documents, and any other analysis or review of the Trust's cybersecurity policies.
- Audit reports prepared and conducted in accordance with appropriate standards.
- Documented corrections of any weaknesses identified by the third party analyses.

VI. Access Control Procedures

Access control refers to the method of guaranteeing that users have appropriate access to IT systems and data. The Trust adopts the following security practices for access control:

- Access to systems, assets and associated facilities is limited to authorized users, processes, devices, activities, and transactions.

- Access privileges (e.g., general user, third party administrators, plan administrators, and IT administrators) are limited based on the role of the individual and adhere to the need-to-access principle.

- Access privileges are reviewed at least every three months and accounts are disabled and/or deleted in accordance with policy.

- All employees must use unique, complex passwords.

- Multi-factor authentication is used wherever possible, especially to access the internal networks from an external network, unless a documented exception exists based on the use of a similarly effective access control methodology.

- Policies, procedures, and controls are implemented to monitor the activity of authorized users and detect unauthorized access, use of, or tampering with, nonpublic information

- Procedures are implemented to ensure that any sensitive information about a participant or beneficiary in the service providers records matches the information that the plan maintains about the participant.

- Procedures to confirm the identity of the authorized recipient of the funds.

VII. Response to Cybersecurity Incident and Breaches

When a cybersecurity breach or incident occurs, appropriate action will be taken to protect the Trust and plan participants including:

- Informing law enforcement.
- Notifying the appropriate insurer.
- Conducting an investigation of the incident.
- Providing affected plan participants information necessary to prevent and/or reduce injury.
- Honoring any contractual or legal obligations with respect to the breach.
- Addressing and solving the problem that caused the breach to prevent its recurrence.

VIII. Assets or Data Stored in a Cloud or Third Party Service Provider

Assets and data stored in a cloud with a third party provider and accessed over the internet will be subject to appropriate security reviews and independent security assessment. The Trust adopts the following measures to protect the security of data stored on a cloud service provider:

- Require a risk assessment of third party service produces.
- Define minimum cybersecurity practices for third party service providers.
- Periodically assess third party service providers based on potential risks.

Any contracts and guidelines between the Trust and the third party service provider will, at minimum include:

- Guidelines regarding the third party service provider's access control policies and procedures including the use of multi-factor authentication.
- The third party service provider's encryption policies and procedures
- The third party service provider's notification protocol for a cybersecurity event which directly impacts a customer's information systems or nonpublic information.

IX. Cybersecurity Awareness Training

Trustees, administrators, plan staff, and any other personnel of the Trust will be required to participate in cybersecurity awareness training conducted at least annually. The purpose of this training is to set clear cybersecurity expectations for all employees and to educate personnel to recognize attack vectors, help prevent cyber-related incidents, respond to potential threats, and recognize and prevent identify theft which may result in unauthorized access to systems.

X. Secure System Development Life Cycle Program (SDLC)

The purpose of a SDLC process is to ensure that security assurance activities such as penetration testing, code review, and architecture analysis are an integral part of the system development effort. The Trust will include adopt the following practices related to SDLC:

- Procedures, guidelines, and standards which ensure any in-house applications are developed securely. This would include such protections as:
    - Configuring system alerts to trigger when an individual's account information has been changed.
    - Requiring additional validation if personal information has been changed prior to request for a distribution from the plan account.
    - Requiring additional validation for distributions (other than a rollover) of the entire balance of the participant's account.
- Procedures for evaluating or testing the security of externally developed applications including periodic reviews and updates.
- A vulnerability management plan, including regular vulnerability scans.
- Annual penetration tests, particularly with respect to customer-facing applications.

XI. Business Continuity Plan, Disaster Recovery Plan, and Incident Response Plan

The Trust will adapt a business resiliency program to adapt to disruptions while maintaining continuous business operations of the Trust while safeguarding assets and data. The components of the program will include the Business Continuity Plan, Disaster Recovery Plan, and Incident Response Plan.

A. Business Continuity Plan

The Trust will establish a Business Continuity Plan for the Trust to recover, resume, and maintain Trust functions following a disruption.

B. Disaster Recovery Plan

The Disaster Recovery Plan is the process to recover and resume the Trust's IT infrastructure, business applications, and data services in the event of a major disruption.

C. Incident Response Plan

The Trust will create a set of instructions to assist IT personnel to detect, respond to, and recover from security incident.

XII. Encryption of Sensitive Data

The purpose of data encryption is to protect nonpublic information. The Trust will implement standards for encryption keys, message authentication and hashing to protect the confidentiality and integrity of the data of the Trust.

XIII. Technical Controls

Technical security solutions are implemented through hardware, software, and firmware mechanisms. The Trust will develop security practices for technical security.