

CYBERSECURITY POLICY

*The State of Delaware Deferred Compensation Plans
Under IRC§§ 457(b), 403(b) and 401(a)*

*The State of Delaware College Investment Plan under
IRC§ 529*

The State of Delaware ABLE Plan under IRC§ 529A

Approved on December 5, 2023

By the Delaware Plans Management Board

I. THE PLANS MANAGEMENT BOARD AND ITS COMMITTEES

The Plans Management Board (the “Board”) oversees the State's deferred compensation program authorized under chapter 60A of title 29 of the Delaware Code (the “DC Program”).¹ The DC Program encompasses three distinct deferred compensation plans authorized under the Internal Revenue Code (“IRC”): (a) the State's deferred compensation plan under IRC § 457(b); (b) the State's tax-sheltered annuity plan for certain education employees under IRC § 403(b); and (c) the State's employer match plan under IRC § 401(a) (the “DC Plans”). The Board also oversees and administers the State's college investment plan under IRC § 529, authorized by subchapter XII, chapter 34 of title 14 of the Delaware Code, and the State's "Achieving a Better Life Experience Program," authorized by chapter 96A of title 16 of the Delaware Code (the “ABLE Plan,” and together with the DC Plans, the “Plans”).

In February 2018, as memorialized in Resolution No. 2018-1, the Board created the Audit and Governance Committee (the “AGC”) and vested it with initial responsibility for all audits-related matters, potential Plan amendments, Plan-related cybersecurity issues, and such other audit or governance matters pertaining to the DC Plans and ABLE Plan as may be referred by the Board.

II. OFFICE OF THE STATE TREASURER

The Office of the State Treasurer (“OST”) provides administrative support to the Board and its committees. OST, in addition to performing certain administrative/operational functions for the Plans, is primarily responsible for procuring recordkeepers and other Plan vendors. OST’s Director of Contributions and Plan Management (the “Director”) leads the procurement processes. The Director is charged with forming and overseeing procurement evaluation teams (“Evaluation Teams”), which typically consist of other OST staff and other State employees who have subject matter expertise (“SMEs”). Evaluation Teams make award recommendations to the appropriate committee, which committee then makes a recommendation to the full Board. The Director works with OST’s assigned Deputy Attorney General (the “DAG”) to negotiate contracts (the “Vendor Agreements”) with the vendors approved by the Board. The Director is responsible for monitoring the performance of awarded vendors and reporting material issues to the appropriate committee or the full Board.

III. SCOPE

This policy governs OST’s duties and responsibilities concerning cybersecurity for the Plans. OST and vendors performing Plan-related services may have additional duties and responsibilities under the Board’s vendor management policy.

OST relies on the Department of Technology and Information (“DTI”) for development, implementation, monitoring, employee education, and testing of adequate safeguards to State-managed networks, computer systems, and related hardware/software used by OST. DTI is

¹ See 29 Del. C. § 2722.

responsible for promptly notifying OST of any breach or other cybersecurity issue, including those that may affect Plan participants.

This policy shall not apply to vendors with whom OST, or the Board do not have direct contractual relationships – *e.g.*, 403(b) “legacy” vendors.

IV. OST DUTIES

OST, with oversight from the AGC and the Board, shall have and perform the following duties to guard against cybersecurity threats, including those related to use of and reliance on vendor’s systems:

A. Coordination with DTI

No less than annually, OST will meet with DTI to discuss DTI’s services, any significant cybersecurity issues that arose and how DTI addressed them, emerging cybersecurity threats and DTI’s planning for those threats, and other relevant cybersecurity topics.

B. Plan Administrative Functions

OST shall, when performing administrative/operational functions for the Plans, ensure the protection of participant information. Dissemination of confidential participant information shall be restricted to OST staff with a need to access the information to perform official duties. OST shall not view or use participant information for any purpose other than to perform official functions.

OST staff shall use encrypted email, secured fax, or similar secure methods when communicating internally or externally participant personal or financial information. Hard copies of documents containing participant information shall be handled securely and, when not in active use, maintained in locked offices or filing cabinets. OST staff will timely complete all cybersecurity training assigned by DTI.

C. Procurement

Prior to initiating any procurement process, OST shall assess any Plan-related services for cybersecurity risks where a breach of the vendor’s system could lead to the inability to access or use the vendor’s system, the unauthorized disclosure of confidential participant information, or result in the loss of participant or Plan assets, or where vendor-provided software or data files could contain a virus or malware. For any service presenting a cybersecurity risk:

- OST shall ensure that any Request for Proposal (“RFP”) for such services includes a detailed questionnaire containing questions designed to identify and assess cybersecurity risk, including -
 - Whether the vendor has a process for managing cybersecurity risks as part of the vendor’s overall risk management system.
 - Whether the vendor engages assessors, consultants, auditors or other third parties in connection with such process.

- Whether the vendor has a process to oversee and identify cybersecurity risks associated with its use of any third-party service provider.
- Whether the vendor had any previous cybersecurity incidents that materially affected, or which reasonably could have materially affected, the vendor's business strategy, operations, or financial condition.
- Whether the vendor's board of directors, or any board committee or subcommittee, has responsibility for overseeing the prevention, detection, mitigation, and remediation of cybersecurity incidents, and whether such body includes members or has retained consultants with the level of expertise needed to perform those tasks.

While the foregoing questions are posed as eliciting "Yes/No" responses, OST shall require vendors to provide supporting details sufficient to assess cybersecurity risks.

- OST shall consult with internal IT resources or SMEs within DTI when developing the questionnaire for a particular RFP.
- The Director shall select an OST staff member or other State employee or outside consultant with IT expertise to serve as the SME for cybersecurity issues, either as a scoring member of the Evaluation Team or as a non-scoring advisor for the Evaluation Team. In either role, the SME, at a minimum, shall assess each prospective vendor's answers to the questionnaire and other aspects of a proposal bearing on cybersecurity risk and report all issues or concerns to the Director and members of the Evaluation Team.

When negotiating contract terms with vendors who have been approved by the Board, OST, in consultation with the DAG, shall ensure that any resulting Vendor Agreement for services involving cybersecurity risks:

- Requires the vendor to maintain all participant personal and financial information on a secure and confidential basis.
- Requires the vendor to use encrypted email or similar secure means when communicating confidential participant information, internally or externally.
- Requires the vendor to adhere to all applicable DTI policies and procedures and all applicable guidance issued by the National Institute of Standards and Technology and certify compliance with the foregoing on an annual basis.² Vendors shall be notified of all official DTI policy changes and shall be obligated to achieve compliance with within a reasonable period of time. The annual cybersecurity certificate shall be signed by a senior-level executive.
- Requires the vendor to notify OST, without undue delay, of any incident resulting in the destruction, loss (including loss of access through ransomware), unauthorized disclosure, or alteration of Plan participant data, which notice shall identify the type and amount of data that was compromised or disclosed.

² This policy acknowledges that OST does not have unlimited bargaining power with respect to vendors. In circumstances where it is necessary to procure a vendor that is unable or unwilling to adhere to all applicable DTI policies and procedures, OST shall seek to mitigate cyber risk to the fullest extent possible.

- Requires the vendor to provide timely periodic updates and otherwise keep OST informed of the vendor’s efforts to address a security breach.
- Requires the vendor to provide, if requested, a copy of its most recent System and Organization Controls 2 report (“SOC 2”) or similar independent review.
- Requires the vendor to provide periodic reports on the vendor’s cybersecurity practices and, if requested, present same to the Board at a public meeting.
- Requires the vendor to maintain cyber liability insurance in the coverage amount required by the State’s Insurance Coverage Office.
- Requires the vendor to indemnify the State for all costs and expenses related to any cybersecurity breach attributable to the negligence of the vendor or a vendor’s subcontractor or agent.
- Permits OST to audit the vendor’s performance and compliance with the foregoing requirements and requires the vendor to cooperate with such audit.

OST shall have discretion to tailor this list of requirements to fit the specific facts and circumstances of each vendor relationship. Vendor Agreements shall specify the consequences of material non-compliance with the foregoing requirements.

D. Compliance Monitoring

OST shall monitor OST’s and the vendor’s compliance with the foregoing contractual requirements and promptly report any issues to the chair of the AGC. OST shall document its monitoring activities and shall utilize an SME if and as needed in connection with such monitoring.

OST shall promptly review with an SME any SOC 2 or similar independent review provided by a vendor and promptly report any areas of concern to the Chair of the AGC.

V. MISCELLANEOUS PROVISIONS

This policy shall be binding on OST and shall remain in effect until amended by the Board. The Board shall have full and complete discretion as to the interpretation of this document and its application to a specific situation. Nothing contained herein shall provide to any participant, beneficiary, or any other party the right to enforce or assert claims or defenses based on the terms of this policy.

Adopted by the Delaware Plans Management Board this 5th day of December 2023, as evidenced by the signature of the Board Chair, as attested below.

Donna Viera, Chair

ATTEST: _____

Colleen Davis, State Treasurer

DRAFT