



State of Wisconsin
Department of Employee Trust Funds
4822 Madison Yards Way
Madison, WI 53705-9100
P. O. Box 7931
Madison, WI 53707-7931

Contract by Authorized Board

Commodity or Service:

Third Party Administration of Uniform Dental Benefits

Contract No./Request for Proposal No:

ETJ0045 Contract Amendment 1 dated January 9, 2025



Authorized Board: Group Insurance Board (GIB)

Contract Period: January 1, 2022 – December 31, 2028 with the option for renewal for one (1) additional two (2)-year term.

1. This Contract Amendment 1 is entered into by the State of Wisconsin Department of Employee Trust Funds (Department) on behalf of the State of Wisconsin Group Insurance Board (Board), and Delta Dental of Wisconsin, Inc. (Contractor). Contractor's address and principal officer appear below. The Department is the sole point of contact for this Contract.
2. Whereby the Department agrees to direct the purchase and Contractor agrees to supply the Contract requirements in accordance with the documents specified in the order of precedence below, which are hereby made a part of this Contract by reference.
3. **ARTIFICIAL INTELLIGENCE:** Contractor use of Artificial Intelligence (AI) models shall at all times comply with and observe the terms of the Contract. "AI model" means a system that is designed to process or learn from data entered to conduct cognitive functions that simulate human intelligence. This includes, but is not limited to, search and filtering functionality that collects, tracks, and monitors data whether via sensors, user-entered data, or other sources without a human responsible for verifying the validity and integrity of data inputs and outputs to maintain the system's integrity, including legal due process if the model is allowed to make decisions on issues that impact human or legal rights.
 - (a) Contractor use of AI models shall comply with each of the following:
 - (1) Materially comply with and observe all applicable State and federal laws, administrative rules, and regulations, including but not limited to privacy, intellectual property, and equity requirements.
 - (2) Maintain the integrity of work performed and Services provided under the Contract, including, but not limited to, ensuring that its AI model vendors are required to comply with applicable laws and regulations prohibiting bias and discrimination from being introduced into Services provided pursuant to the Contract by Contractor.
 - (3) Maintain the quality of Department information under Contractor's authority.
 - (4) Maintain the confidentiality, privacy, and security of Confidential Information as defined in Section 24.0 (a) (2).
 - (b) The Contractor shall remove all Department Confidential Information and to the extent possible all other Department Confidential Information from AI models used by Contractor upon the Department's request or, at the latest, upon Contract termination, including removal from AI model training data and learning.
 - (c) The Contractor shall not gain profit from use of Department information, including Confidential Information, that is outside the scope of the Contract.
 - (d) Upon request from the Department the Contractor will disclose within 30 calendar days from the day of the request which Services provided to the Department are using AI models.
4. Delete from Department Terms and Conditions (RFP Appendix 2) Section 28.0 and Add to Department Terms and Conditions (RFP Appendix 2) (for Department reference this is DTC v. 6.24.2024 Section 31.0) as described in the attached Amendment 1A.
5. By executing Contract Amendment 1 dated January 9, 2025, the Department and Contractor hereby agree to extend this contract for two (2) additional years, from January 1, 2027 through December 31, 2028 for the rate of \$1.15 per employee per month (PEPM).
6. For purposes of administering this Contract, the order of precedence is:

- (a) This Contract Amendment 1 dated January 9, 2025;
- (b) The Contract dated July 16, 2021;
- (c) Exhibit A documenting clarifications to the Department Terms and Conditions (RFP Appendix 2) and Program Agreement (RFP Appendix 5);
- (d) Exhibit B documenting additional covered CDT codes and changes to the Program Agreement (RFP Appendix 5);
- (c) Department Terms and Conditions dated May 1, 2019 (RFP Appendix 2);
- (d) Program Agreement (RFP Appendix 5);
- (e) Contractor's Best and Final Offer dated 12.3.2020 Corrected (003);
- (f) Request for Proposal (RFP) ETJ0045 dated April 15, 2020; and
- (g) Contractor's proposal dated October 1, 2020.

Contract Number & Service: ETJ0045 Third Party Administration of Uniform Dental Benefits This Contract Amendment 1 shall become effective upon the date of last signature below (the "Effective Date").

State of Wisconsin Department of Employee Trust Funds	Contractor
Authorized Board: Group Insurance Board	Legal Company Name: Delta Dental of Wisconsin, Inc.
By (Name): Herschel Day	Trade Name:
Signature: 	Taxpayer Identification Number: 39-6094742
Date of Signature: 1/10/2025	Contractor Address (Street Address, City, State, Zip): 3100 Business Park Dr. Stevens Point, WI 54482
Contact A. John Voelker, ETF Secretary, if questions arise: (608) 266-9854	Name & Title (print name and title of person authorized to legally sign for and bind Contractor): Kyle Humphrey, Chief Sales & Marketing Officer
	Signature: 
	Date of Signature: 1/10/2025
	Email: khumphrey@deltadentalwi.com Phone: 715-343-7618

Amendment 1A

Delete from Department Terms and Conditions (RFP Appendix 2) Section 28.0.

Add to Department Terms and Conditions (RFP Appendix 2) (for Department reference this is DTC v. 6.24.2024 Section 31.0):

28.0 INFORMATION SECURITY AGREEMENT

- (a) **PURPOSE AND SCOPE OF APPLICATION:** This Information Security Agreement ("Agreement") is designed to protect the Department's Confidential Information (defined above in Section 22.0) and Department Information Resources (defined below). This Agreement describes the information security obligations of Contractor, its employees, contractors, and third-party users that connect to Department Information Resources and/or gain access to Confidential Information.
- (b) **DEFINED TERMS:**
- (1) Department Information Resources. "Department Information Resources" means those devices, networks and related infrastructure that the Department has obtained for use to conduct Department business. Devices include but are not limited to, Department-owned devices; devices managed or used through service agreements; storage, processing, and communications devices and related infrastructure on which Department data is accessed, processed, stored, or communicated; and may include personally owned devices. Data includes, but is not limited to, Confidential Information, other Department-created or managed business and research data, metadata, and credentials created by or issued on behalf of the Department.
 - (2) Subservice Organization: "Subservice Organization" means a subcontractor whose controls, in combination with the Contractor's controls, are necessary to perform Services under the Contract and related system requirements.
- (c) **ACCESS TO DEPARTMENT INFORMATION RESOURCES:** In any circumstance when Contractor is provided access to Department Information Resources, it is solely Contractor's responsibility to ensure that its access does not result in any access by unauthorized individuals to Department Information Resources. Contractors who access the Department's Information Resources from any Department location must at a minimum conform with Department security standards that are in effect at the Department location(s) where the access is provided. Any Contractor technology and/or systems that gain access to Department Information Resources must comply with, at a minimum, the elements in the Information Security Plan Requirements set forth in this Agreement.
- (d) **COMPLIANCE WITH APPLICABLE LAWS:** Contractor agrees to comply with all applicable state and federal laws, as well as industry best practices, governing the collection, access, use, disclosure, safeguarding and destruction of Confidential Information.
- (e) **SAFEGUARD STANDARD:** Contractor agrees to protect the security of Confidential Information according to all applicable laws and regulations by generally accepted information risk management security control frameworks, standards or guidelines such as the ISO/IEC 27000-series, NIST 800-53, CIS Critical Security Controls for Effective Cyber Defense or HIPAA Security Rule – 45 CFR Part 160 and Subparts A and C of Part 164 and no less rigorously than it protects its own confidential information, but in no case less than reasonable care. Contractor will implement, maintain and use appropriate administrative, technical and physical security measures to preserve the confidentiality, integrity and availability of the Confidential Information. Contractor will ensure that Security measures are regularly reviewed including ongoing monitoring, monthly vulnerability testing and annual penetration and security incident response tests, revised, no less than annually, to address evolving threats and vulnerabilities while Contractor has responsibility for the Confidential Information under the terms of this Agreement.
- (f) **INFORMATION SECURITY PLAN:**
- (1) Contractor acknowledges that the Department is required to comply with information security standards for the protection of Confidential Information as required by law, regulation and regulatory guidance, as well as the Department's internal security program for information and systems protection.
 - (2) Contractor shall develop, implement, and maintain a comprehensive Information Security Plan that contains administrative, technical, and physical safeguards designed to ensure the privacy, security, integrity, availability, and confidentiality of the Confidential Information.
 - (3) Annually, if the Contractor is required to provide an independent service auditor's report, such as a SOC 2, Type 2 audit report, Contractor will furnish the Department's designated staff person as directed with a copy of Contractor's required report.
 - (4) Annually, or upon a significant change in risk posture, Contractor will review its Information Security Plan and update and revise it as needed. If at any time there are any material reductions to Contractor's Information Security Plan, Contractor will notify the Department within two weeks of the completion of the review and prior to implementation. In such instances, the Department will require an explanation of the reductions. At the Department's request, Contractor will make

modifications to its Information Security Plan or to the procedures and practices thereunder to conform to the Department's security requirements as defined herein.

- (5) Annually, Contractor will demonstrate oversight of Subservice Organizations involved in the delivery of Services under the Contract. To demonstrate oversight, the Contractor shall submit one of the following documents to the Department:
 - a. A summary of its vendor management policy and procedure;
 - b. Documentation showing oversight of Contractor's Subservice Organizations' security posture through reviews of Contractor's vendors' independent service auditor's reports at least every three years; corrective action plans; or reviews of information technology controls at least every three years; or
 - c. Letter of attestation assuming the Contractors' liability for its Subservice Organizations.
- (g) **ADDITIONAL INSURANCE:** In addition to the insurance required under the Contract, Contractor, at its sole cost and expense, will obtain, keep in force, and maintain an insurance policy (or policies) that provides coverage for privacy and data security breaches. This specific type of insurance is typically referred to as Privacy, Technology and Data Security Liability, Cyber Liability, or Technology Professional Liability. In some cases, Professional Liability policies may include some coverage for privacy and/or data breaches. Regardless of the type of policy in place, it needs to include coverage for reasonable costs in investigating and responding to privacy and/or data breaches with the following minimum limits unless the Department specifies otherwise: \$1,000,000 each occurrence and \$5,000,000 aggregate. If the Contractor maintains broader coverage and/or higher limits than the minimums shown above, the Department requires and is entitled to the broader coverage and/or higher limits maintained by the Contractor. Any available insurance proceeds in excess of the specified minimum limits of insurance and coverage shall be available to the Department.

(h) INFORMATION SECURITY PLAN REQUIREMENTS:

If Contractor cannot provide evidence of its Information Security Plan as required in Subsection (f)(2) above, Contractor shall provide the following assurances to the Department:

(1) Security Policies:

- a. Contractor's security policy is documented, has obtained management approval, is reviewed no less frequently than annually and is maintained to ensure its continuing suitability, adequacy, and effectiveness; and
- b. Contractor's operational, technical, and administrative policies, standards and guidelines are documented, have obtained management approval, are reviewed no less frequently than annually and are maintained to ensure their continuing suitability, adequacy, and effectiveness.

(2) Security Organization:

- a. The Contractor's security organization is governed and overseen by Contractor's senior leadership;
- b. Contractor's security organization includes representation from across Contractor's organization with defined roles and responsibilities;
- c. Contractor has clearly defined information security responsibilities;
- d. Contractor has confidentiality or non-disclosure agreements in place with the appropriate external entities;
- e. Contractor's management and implementation of information security (i.e., control objectives, controls, policies, processes, and procedures for information security) are reviewed independently at planned intervals, or when significant changes to the implementation of information security occur; and
- f. Contractor's agreements with third parties involving accessing, processing, communicating, or managing the Contractor's information or information processing facilities, cover all relevant security requirements.

(3) Asset Management:

- a. Contractor has identified, inventoried, assigned ownership, and established rules for acceptable use for information and associated assets; and
- b. Contractor has a process in place to classify information in terms of its value, legal requirements, sensitivity, and criticality to Contractor.

(4) Human Resources:

- a. Security roles and responsibilities of Contractor's employees, contractors and third-party users have been defined and documented in accordance with Contractor's information security policy;
- b. Contractor performs background verification checks on all candidates for employment, contractors, and third-party users in accordance with relevant laws, regulations, and ethics, and proportional to the business requirements, the classification of the information to be accessed, and the perceived risks;
- c. All Contractor's employees and, where relevant, contractors and third-party users, shall receive appropriate security awareness training and regular updates regarding Contractor's security policies and procedures, as relevant for their job function;
- d. Contractor has a formal disciplinary process in place for employees who have committed a security breach;
- e. Contractor's employees' responsibilities for performing employment terminations and changes of employment status are clearly defined and assigned;
- f. All Contractor's employees, contractors and third-party users shall return all Contractor's and the Department's assets in their possession upon termination of their employment, contract, or agreement; and
- g. The access rights of all Contractor employees, contractors and third-party users to information and information processing facilities are removed upon termination of their employment, contract, or agreement, or adjusted upon a status change.

(5) Physical and Environmental Security:

- a. **Secure Areas**

- i. Contractor has a physical and environmental policy in place, with standards and guidelines that have been documented, approved by Contractor management, reviewed at least annually, and maintained to ensure continuing suitability, adequacy and effectiveness;
 - ii. Contractor's secure areas are protected by appropriate entry controls to ensure that only authorized personnel are allowed access; and
 - iii. Contractor's physical protection and guidelines for working in secure areas have been adequately designed and applied.
- b. Equipment security**
 - i. Contractor's equipment, and the equipment Contractor may utilize in its operations that is owned by a third party, is maintained to ensure its continued availability and integrity; and
 - ii. Contractor's security measures have been applied to off-site equipment to address the risks of working outside the Contractor's premises.
- c. Operations management**
 - i. Contractor's operating procedures have been documented, maintained, and made available to all users who require them;
 - ii. Contractor controls changes to information processing facilities and systems; and
 - iii. Contractor has segregated duties and areas of responsibility to reduce opportunities for unauthorized or unintentional modification or misuse of Contractor's assets.
- d. Third party service delivery management**
 - i. Security controls, service definitions and delivery levels included in Contractor's third-party service delivery agreements are implemented, operated, and maintained by the third party; and
 - ii. The services, reports and records provided by third parties are regularly monitored, reviewed, and audited by Contractor.
- e. Back-up**
 - i. Contractor regularly makes and tests back-up copies of information and software in accordance with Contractor's backup policy.
- f. Network security management**
 - i. Networks are managed and controlled, either by Contractor or a third party under contract with Contractor; and
 - ii. Security features, service levels, and management requirements of all Contractor's network services have been identified and included in any network services agreement, whether these services are provided in-house by Contractor or outsourced.
- g. Media handling**
 - i. Contractor has procedures in place to prevent unauthorized disclosure, modification, misuse, removal or destruction of assets, and interruption to business activities; and
 - ii. Contractor has procedures in place for the management of removable media, including the secure and safe disposal of media when no longer required.
- h. Exchange of information**
 - i. Contractor has established agreements for the secure exchange of information and software between Contractor and appropriate external parties;
 - ii. Contractor shall ensure information involved in electronic messaging is protected;
 - iii. Contractor has developed and implemented policies and procedures to protect the exchange of information; and
 - iv. Contractor shall ensure the integrity of information being made available on a publicly available system is protected to prevent unauthorized modification.
- i. Monitoring**
 - i. Contractor shall produce and keep a rolling twelve (12) consecutive months of audit logs recording user activities, exceptions, and information security events to assist in future investigations and access control monitoring;
 - ii. Contractor's logging facilities and log information are protected against tampering and unauthorized access; and
 - iii. Contractor's system administrator and system operator activities are logged.

(6) Access Management:

- a. Access control**
 - i. Contractor has an established and documented access control policy that is reviewed at least annually based on business and security requirements for access;
 - ii. Contractor has a formal user registration and de-registration procedure in place for granting and revoking access to all information systems and services;
 - iii. Contractor restricts, controls, and monitors the allocation and use of access to its systems for unauthorized users and data used on the network;
 - iv. Contractor controls the allocation of passwords through an automated or semi-automated password management tool; and
 - v. Contractor's management reviews users' access rights at least annually using a formal process.
- b. User responsibilities**
 - i. Users are required to follow good security practices in the selection and use of passwords;
 - ii. Users shall ensure that unattended equipment is protected; and
 - iii. Users shall adopt a clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities.
- c. Network access control**
 - i. Contractor's users shall adhere to the principle of least privilege;

- ii. Contractor has implemented appropriate authentication methods to control access by remote users;
- iii. Contractor has segregated groups of information services, users, and information systems on networks;
- iv. For shared networks, especially those extending across Contractor's boundaries, Contractor has restricted the capability of users to connect to the network, in line with Contractor's access control policy; and
- v. Contractor has implemented routing controls for networks to ensure that computer connections and information flows do not breach Contractor's access control policy.

(7) Security Requirements of Information Systems:

- a. Correct processing in applications**
 - i. Contractor shall validate data input to applications to ensure the data is correct and appropriate, and incorporate validation checks to detect any corruption of information through processing errors or deliberate acts;
 - ii. Contractor has identified the requirements for ensuring authenticity and protecting message integrity in applications, and identified and implemented appropriate controls; and
 - iii. Contractor has validated the data output from an application to ensure that the processing of stored information is correct and appropriate to the circumstances.
- b. Cryptographic controls**
 - i. Contractor has a cryptographic controls policy in place that is documented, has obtained management approval, is reviewed at least annually and is maintained to ensure its continuing suitability, adequacy, and effectiveness.
- c. Security of system files**
 - i. Contractor has procedures in place to control the installation of software on operational systems;
 - ii. Contractor selects test data carefully, and the test data is protected and controlled; and
 - iii. Contractor restricts access to program source code.
- d. Security in development and support processes**
 - i. Contractor has implemented procedures to maintain the security of application system software and information;
 - ii. Contractor utilizes formal change control procedures to implement changes; and
 - iii. Contractor supervises and monitors outsourced software development.
- e. Technical Vulnerability Management**
 - i. Contractor documents the technical vulnerabilities, the exposure evaluated, and the appropriate measures taken to address the associated risk.

(8) Information Security Incident Management:

- a.** Contractor communicates information security events and weaknesses associated with information systems in a manner allowing timely corrective action to be taken;
- b.** All Contractor's employees, contractors, and third-party users of information systems and services are provided awareness training on reporting an observed or suspected incident; and
- c. Management of information security incidents and improvements**
 - i. The responsibilities and procedures of Contractor's management have been established to ensure timely, effective, and orderly response to information security incidents;
 - ii. Contractor has mechanisms in place to enable the security incidents to be quantified and monitored; and
 - iii. Where a follow-up action against a person or organization after an information security incident involves legal action (either civil or criminal), Contractor shall collect, retain and present evidence in conformance with the rules for evidence established in the relevant jurisdiction(s).

(9) Business Continuity Management:

- i. Contractor has implemented one or more business continuity plans, including an information security plan, to maintain or restore operations and ensure availability of information at the required level and in the required timeframe following interruption to, or failure of, critical business processes;
- ii. Contractor tests and updates its business continuity plans regularly to ensure that they are up to date and effective; and
- iii. Contractor shall include the Department's designated contact in Contractor's business continuity plans for notification concerning any disruption that may impact the Services.

(10) Compliance:

- a. Identification of applicable legislation**
 - i. Contractor understands all relevant statutory, regulatory, and contractual requirements under the Contract, and Contractor's approach to meet these requirements has been explicitly defined, documented, and kept up to date;
 - ii. Contractor has implemented appropriate procedures to ensure compliance with legislative, regulatory, and contractual requirements under the Contract on the use of material which may be afforded intellectual property rights;
 - iii. Contractor shall ensure that important records are protected from loss, destruction and falsification, in accordance with the statutory, regulatory, contractual, and business requirements under the Contract; and
 - iv. Contractor shall ensure the protection and privacy of data as required in relevant legislation, regulations, and, as applicable, the Contract.