



**State of Delaware
Department of Transportation**

**National Electric Vehicle
Infrastructure (NEVI)**

Request For Proposals

Contract No. DOT2317-NEVI

APPENDIX A

SCOPE OF WORK

TABLE OF CONTENTS

1	SCOPE SUMMARY	1
1.1	BACKGROUND	1
1.2	SITE REQUIREMENTS	1
1.3	MAINTENANCE & OPERATIONS	2
1.3.1	<i>Equipment Ownership.....</i>	<i>2</i>
1.3.2	<i>Five-Year Operations and Maintenance Obligation.....</i>	<i>2</i>
1.3.3	<i>Transfer After or During the Performance Period.....</i>	<i>3</i>
1.3.4	<i>Up Time Requirement</i>	<i>3</i>
1.3.5	<i>Data Sharing/Interoperability Requirements.....</i>	<i>3</i>
1.3.6	<i>Proposed Modifications to System Specifications.....</i>	<i>3</i>
1.3.7	<i>Testing Requirements</i>	<i>3</i>
1.3.8	<i>Customer Service.....</i>	<i>4</i>
1.3.9	<i>Privacy & Cybersecurity</i>	<i>4</i>

1 Scope Summary

1.1 Background

Competitive funding is available to businesses and other eligible applicants for design and installation of publicly accessible DC fast charging equipment in Delaware that complies with the NEVI Program requirements. Charging stations funded through this opportunity must be maintained and operated for public use by vendor for a minimum of five (5) years with no less than 97.00 percent uptime throughout the entire performance period.

Vendors must follow all NEVI Program requirements, including those set forth in the following FHWA documents:

- [NEVI Formula Program Guidance](#)
- [NEVI Program Frequently Asked Questions](#)
- [NEVI Standards and Requirements Final Rule](#)
- [NEVI Formula Program Guidance \(Update\)](#)

In general, proposals for public charging stations at multiple locations are accepted; however, each location shall have no less than four (4) 150kW or greater DCFC charging ports configured with no less than one (1) Society of Automotive Engineers Combined Charging System (SAE CCS) connection and no less than one (1) Charge de Move (CHAdeMO) connection. Projects funded under this opportunity will provide DCFC stations for public use along FHWA-designated AFCs with Delaware. All DC fast charging stations must be networked and comply the NEVI Program Guidance and Final Rule.

The following subsections include additional DelDOT specific considerations. Proposing vendors shall review the approved [DelDOT NEVI Plan](#) before submitting proposals and follow any applicable EV standards adopted by Delaware and/or the federal government.

1.2 Site Requirements

Projects funded under this opportunity will provide DCFC stations for public use along FHWA-designated AFCs within Delaware. All sites are required to have at least four DCFC charging ports capable of simultaneous delivery of 150kw of charge, with each site having a minimum capacity of 600kw. Proposals for public charging stations at multiple locations are acceptable; however, each location shall meet the minimum NEVI program requirements for site charging capacity and interoperability. All DC fast charging stations must be networked and comply with the NEVI Program Guidance and Final Rules.

Site design and layout is to be provided and shall accommodate for both access and safety of the equipment and users. While no formal standards for site layout have been established, design recommendations from the U.S. Access Board are available in their July 22, 2022, document, "Design Recommendations for Accessible Electric Vehicle Charging Stations." Sites should consider

flood plain locations and applicable site conditions. If a site is proposed in an active flood plain, the Operation & Maintenance (O&M) Plan must take flood plain maintenance into consideration.

DelDOT will obtain, at its expense, environmental review clearances for the site work related to EV installation as required by the National Environmental Policy Act (NEPA) once the vendor has finalized a site design. Any amendments or supplements required to the obtained NEPA review clearances shall be the responsibility of the vendor. It is anticipated NEPA clearance would be obtained by DelDOT within 60 days following finalized site design, but actual length is subject to specific site conditions and FHWA approval so therefore subject to change.

Proposing vendors shall be responsible for all permitting responsibilities and third-party agreements for the site. Contingent agreements or memorandums of understanding (MOU) with site owners and utility companies are sufficient prior to award, but fully executed site host agreements must be obtained within 30 days after notice of conditional award. Each Vendor must have or be able to secure necessary property rights, easements, rights-of-way, and access to the property for the proposed DC fast charging station. Documentation of site control (e.g., a letter of commitment, lease, or property title) must be included in the application.

1.3 Maintenance & Operations

1. Equipment Ownership

Upon completion of construction and installation and written acceptance by DelDOT of fully operational EVSE (including power and data service), the vendor shall own the EVSE equipment. Vendors shall ensure there is a separate and distinct meter for the EVSE system.

2. Five-Year Operations and Maintenance Obligation

The selected vendor shall be required to ensure the operations and maintenance of the EVSE at the site for a period of at least five years from the date identified on the Notice of Acceptance letter. Compliance with the at least 97.00 percent uptime requirement throughout the five-year performance period is essential, and vendors may satisfy this requirement one of two ways:

- Option 1—Full-Coverage Service Contract: The Vendor shall comply with a five-year maintenance and operation plan and a five-year networking plan. The Vendor shall have a five-year service contract providing 100 percent coverage of labor, parts, and materials as well as emergency service. This contract shall include comprehensive preventive maintenance for the covered equipment and systems and repair and replacement coverage (sometimes called a “breakdown” insurance policy) for the covered equipment.
- Option 2—In-House Operations and Maintenance: DelDOT will not fund in-house operation and maintenance programs with NEVI program grant funds and thus Vendors will have to use other funding sources. In-house operation and maintenance programs will comply with the Vendor’s Operations and Maintenance Plan. If DelDOT receives information that the Vendor is not providing comprehensive preventive maintenance or system repair or replacement, DelDOT will have the right to enter the property to inspect. If necessary, DelDOT will also have the right to hire a contractor to perform the needed operations and maintenance, at the Vendor’s cost. If DelDOT incurs costs, it may deduct those costs from performance payments as noted in Section **Error! Reference source not found.**

3. Transfer After or During the Performance Period

If the vendor decides to retain and operate the equipment following the expiration of the five-year period, the vendor will be responsible for management of, receipt, and disbursement of fees charged. If the vendor sells the site, closes the business, or otherwise is unable to fulfill the five-year obligation, the vendor must either work with DeIDOT to assign a new operator at the site or pay back project funds prorated for the portion of the remaining five years. The O&M Plan should acknowledge the Vendor's anticipated plan at the end of the five-year O&M Plan and whether the Vendor plans to retain the infrastructure to transfer.

4. Up Time Requirement

Other than allowable downtime for maintenance and repairs, equipment must be up and running equal to or greater than 97.00 percent of the time. Uptime shall be self-monitored by the vendor and reported to DeIDOT if uptime is less than 97.00 percent for a continuous window exceeding twelve hours. DeIDOT may notify the vendor if it has reason to believe the uptime requirement is not being met and require the vendor to develop an action plan to bring the equipment back to working condition. DeIDOT also reserves the right to have third party monitoring of uptime to validate vendor reporting. DeIDOT reserves the right to retain a contractor of its own choosing to repair or replace it, at the vendor's cost.

If DeIDOT determines the vendor is not in compliance with the uptime requirements for two consecutive quarters, DeIDOT may require the vendor to submit an action plan. Material or repeated non-compliance with the uptime requirements may be considered an event of default.

Notwithstanding anything to the contrary contained in this Notice of Funding Opportunity (NOFO) (including its terms and conditions and applicable appendices) or the Vendor Agreement, if the vendor is in default of the uptime requirement, DeIDOT may terminate the Vendor Agreement, and if the default occurs within five years following the disbursement of any part of the Grant, require the vendor to repay to DeIDOT the amount of financial assistance provided, prorated for the portion of the remaining five years.

5. Data Sharing/Interoperability Requirements

DeIDOT is required to provide both quarterly and annual data submittals for similar evaluation at the national level. Data must be transferred or made available using methods authorized under the Vendor Agreement and as agreed upon between the contracted parties. The submitted data will be maintained in a secure manner and will not be used for any purposes other than those required to fulfill the requirements of the Vendor Agreement. The proposing vendor must also disclose, via the Data Management Plan the location of the data and security processes and systems governing it while under the vendor's control. The Data Management Plan shall also include contingency plans for when internet service is out and other information technology (IT) requirements

6. Proposed Modifications to System Specifications

If the proposing vendor seek to use EVSE that deviate from the NOFO minimum requirements, the vendor shall fully explain the deviation from the requirements as part of the application for DeIDOT review. DeIDOT will review the request, evaluate compliance with program requirements, and approve or reject the proposed modifications.

7. Testing Requirements

Vendors shall conduct standard factory testing and post-installation system testing for each charging unit to verify functionality of the EVSE, as well as access and/or integration into the DeIDOT or other prescribed data sharing system. Factory test results shall be provided for each unit as verified by the

vendor's quality assurance or test manager. Similar test results for the installed system shall be provided with the test manager's approval. DelDOT will also have the right to test the EVSE and any data sharing connections (DelDOT systems and/or vendor provided portal). For data sharing, DelDOT will participate in the testing through verification of receipt of the specified data. For the charging unit, DelDOT or its representative may run on-site testing at its own expense.

8. Customer Service

Vendors shall ensure that customer service is provided and available 24 hours per day, 7 days a week, 365 days a year. The customer service shall provide support and responses to inquiries and comments from EVSE users who are using or attempting to use the EVSE charging equipment. The proposing vendor shall submit a plan detailing how such service shall be provided which is accessible by all users.

9. Privacy And Cybersecurity

Vendors shall be responsible for cybersecurity as it relates to owning, operating, maintaining, and data sharing for the EVSE. After selection, the vendor shall participate in a privacy impact assessment with DelDOT, including their Data Governance and Security team. After agreement execution, vendors shall share the following:

- How cybersecurity will be assessed throughout the Agreement term,
- Results of third-party cybersecurity testing (not proprietary information that would make the overall system vulnerable),
- How system updates will affect end users, and
- Proposed protocols for notifying DelDOT of any security breach.

Vendors shall develop a Data Management Plan that incorporates this information and guidance on risk assessments for personnel involved with the charging network, including contractors and service providers. Vendors shall submit the Data Management Plan to DelDOT for approval. Vendors shall comply with local, state, or federal laws as they relate to cybersecurity and privacy. Vendors shall provide an updated Data Management Plan annually along with the annual report for approval by DelDOT. Vendors shall specifically identify the need for the changes and changes to the Data management Plan as part of the annual updates. Vendors can update and submit the Data Management Plan more frequently, if required.

The O&M Plan should address physical security and protection against vandalism as it is the responsibility of the Vendor and/or site host to ensure protection against vandalism and related security issues.



**State of Delaware
Department of Transportation**

**National Electric Vehicle
Infrastructure (NEVI)**

Request For Proposals

Contract No. DOT2317-NEVI

APPENDIX B

Project Budget

Please be as detailed as possible when completing your budget. If additional space is needed, please label pages in your application package "<Title of Project>, Project Budget".

The applicant is responsible for detailing the proposed budget associated with the project. This includes "eligible costs" which includes the equipment necessary for the project and the "ineligible costs" which includes the other expenses related to the project.

Total project costs, including eligible and ineligible costs, associated with the entire project. See Section 3 "Definitions" under the Grant RFP for this project for additional information.

Eligible Costs are those costs that qualify for funding under this RFP grant announcement. See page 3 "Eligible Costs" under the Grant RFP for this project for additional information.

Ineligible costs are those costs that do not qualify for funding under this grant announcement. See page 3 "Ineligible Costs" under the Grant RFP for this project for additional information.

Total Project Costs

Total Budget Expenses	Description	Estimated Cost
Total Ineligible Costs		
Total Eligible Costs		
Total Costs (Total Project Costs plus Total Eligible Costs)		

Eligible Costs

Eligible Costs	Description	Number of Each Item (if applicable)	Estimated Costs
Charging station (make and model)			
Required Permits			
Payment and tracking technologies (key pads, credit card readers, etc.)			
Electrical equipment			
Electrical conduit			
Security fencing (fencing around the station only)			
Concrete pad (concrete only)			

Bollards and car stops			
Other necessary equipment for the charging station			
Necessary signage (i.e. directional signage, safety and usage signage, etc.)			
Labor			
Other			
Total Eligible Costs			

Ineligible Costs

Ineligible Costs	Description	Number of Each Item (if applicable)	Estimated Costs
Administration			
Printing and supplies			
Office equipment			
Acquisition of real estate property			
Travel			
Costs of activities required to obtain permits			
Landscaping			
Renewable energy infrastructure (solar, wind, geothermal, etc.)			
(add rows as necessary)			
Total Ineligible Costs			



**State of Delaware
Department of Transportation**

**National Electric Vehicle
Infrastructure (NEVI)**

Request For Proposals

Contract No. DOT2317-NEVI

APPENDIX C

TECHNICAL PROPOSAL

TABLE OF CONTENTS

1	SITE LAYOUT SKETCH	1
2	SITE INFORMATION SHEET	1
3	NARRATIVE RESPONSE BY CATEGORY	3
a.	Existing Site Details.....	3
b.	Project Approach	3
c.	Site Readiness.....	3
d.	Future Proofing.....	3
e.	Sustainability, Equity, Resilience, & Economic Development	4
f.	Safety & Training	4

For each site being proposed, the technical proposal shall include the information listed on this Form and in the format requested. The narrative section must be no longer than 10 pages.

1. Site layout sketch showing the following:

- Ingress/Egress points and surrounding road access to the site
- Existing and proposed EV charging parking spaces
- Locations of all proposed EVSE equipment
- On-premises signage and wayfinding
- Electric service equipment
- Additional space or equipment for future use
- Layout of proposed charging stalls including availability, if applicable, of pull through sites
- Identification of any site amenities including bathrooms, retail, or public transit connectivity
- Point of sale equipment

2. Site information sheet:

Site Location (Short Answer)	Site/Host Name	
	Physical Address	
	Municipality/County	
	Charger Coordinates	
	AFC Corridor Served	
Existing Features on Site (Yes/No)	Existing DCFC station needing upgrades and/or additional ports/power	
	Within a designated FEMA flood zone	
	Lighting at the charging site	
	Cameras covering the charging facility	
	Canopies covering the charging area	
	Emergency call systems	
	Available on-site staff	
	Dedicated Support staff for the chargers	
	Existing retail, prepared, or non-prepared food available at the site	
	Existing retail, prepared, or non-prepared food available within 0.25 miles of the proposed site	
	Availability of open/free wi-fi at the facility	

	Access to restrooms at the facility and availability of the bathrooms	
	Access to public transportation within 0.25 miles of the facility	
Site Layout and Details (Short Answer)	Total number of DC fast charging stalls with dedicated DC fast charging ports	
	Types of connectors	
	Overall power capacity	
	Additional site additions that will be made available when operational (e.g., dedicated staff for EV charging support)	
	Features of the proposed EVSE equipment and compliance with the NEVI NRPM	
	Site compliance with ADA, 42 U.S.C. 12101 et seq., and 49 U.S.C. 322 or modifications proposed to make the site compliant	
	Damage or loss of service proof against weather, transient surge voltages, traffic incidents, vandalism, or other environmental factors	
	ADA compliance for all amenities on site	
Site Readiness (Yes/No with Short Answer)	Project boundary within an existing parking lot, paved area, or maintained (periodically mowed) lawn	
	Any permits or other approvals required to complete this project (such as air/land user, electrical, structural, zoning, local agency, environmental, etc.)	
	Any site contamination/remediation or cleanup activity associated with hazardous materials	

3. Narrative Response By Category [10 page maximum]

a. Existing Site Details

- 1) Identify the risk associated with locating EVSE in flood zone (if applicable) and plans for mitigating this risk.
- 2) Describe EVSE access during times of emergency such as evacuation during natural disasters.
- 3) Identify and describe enhancements to the site that demonstrate site feasibility and comfort.

b. Project Approach

- 1) Describe your team's approach to project planning, design and permitting.
- 2) Describe your teams' duration of commitment to operate charging station, and plan to operate and maintain the facility for the five-year period, and potentially longer.
- 3) Describe your team's approach to meet the 97.00% uptime requirement.
- 4) Describe processes and procedures related to data sharing responsibilities and identify critical cybersecurity and data safety issues with appropriate measures to manage cybersecurity for all parties involved.
- 5) Provide an estimate of the project schedule/timeline along with major project milestones. Discuss plans to ensure the EVSE site will be installed and ready for public use in a reasonable time and how you are working to mitigate supply chain delays, and other potential project delays. For purposes of estimating, assume a notice to proceed date of 10/01/2023.

c. Site Readiness

- 1) Describe the coordination efforts between the applicant or site host and the utility provider for your specific site including how power will be transmitted to the site, and any upgrades that are required.
- 2) Describe the communications networking capabilities at your site.
- 3) Describe the current state of the site and development required to prepare for EVSE installation. Include any applicable site development needs including plans for site acquisition, site construction, or other site preparation other than power-related preparation.
- 4) Describe the current state of the site and development required to prepare for EVSE installation. Include any applicable site development needs including plans for site acquisition, site construction, or other site preparation other than power-related preparation.
- 5) Identify potential risks, issues, challenges, and needs related to the candidate site and plans for mitigating these risks.

d. Future Proofing

- 1) Describe the potential for additional charging ports, stalls, and power to be provided in the future.
- 2) Describe the current and future ability of the site to allow for parking and charging of medium-and/or heavy-duty vehicles, if any.
- 3) Describe any additional equipment that could improve site resiliency and how the site will accommodate that equipment.

e. Sustainability, Equity, Resilience, and Economic Development

- 1) Describe any usage of renewable energy sources in the electric vehicle charging process for this site.
- 2) Describe any innovative technologies used and/or innovative approaches, such as on-site battery storage, to site design or operation being employed on the project.
- 3) Describe your plan for use of local businesses and/or workforce in Planning, Design, Construction and Inspection, and Operations & Maintenance.
- 4) Describe the plan for the site to serve users with disabilities including access to amenities at the site.
- 5) Describe your plan for addressing additional components of the [Justice40 Initiative](#) to allow for a more equitable charging experience for all users.

f. Safety and Training

- 1) Describe all safety considerations at the site, including safety for users and safety equipment (e.g., site lighting, fire extinguisher, Automated External Defibrillator (AED), automatic safety shutoff, etc.)
- 2) Describe the plan for potential EVSE incidents and explain the management approach and strategies to facilitate site safety as well as safety during construction.
- 3) Describe your team's plan for workforce training and meeting EVTIP certification.
- 4) Describe your team's plan for public and/or stakeholder engagement



STATE OF DELAWARE
DEPARTMENT OF TECHNOLOGY AND INFORMATION
801 Silver Lake Blvd., Dover, Delaware 19904

PUBLIC AND NON-PUBLIC DATA OWNED BY THE STATE OF DELAWARE

State of Delaware Cloud and/or Offsite Hosting Specific Terms and Conditions

Contract/Agreement # _____, Appendix _____

between State of Delaware and _____ dated _____

This document shall become part of the final contract.

	Public Data	Non Public Data	
1	✓	✓	Data Ownership: The State of Delaware shall own all right, title and interest in its data that is related to the services provided by this contract. The PROVIDER shall not access State of Delaware user accounts, or State of Delaware data, except (i) in the course of data center operations, (ii) in response to service or technical issues, (iii) as required by the express terms of this contract, or (iv) at State of Delaware's written request. All information obtained or generated by the PROVIDER under this contract shall become and remain property of the State of Delaware.
2	✓	✓	Data Usage: The PROVIDER shall comply with the following conditions. At no time will any information, belonging to or intended for the State of Delaware, be copied, disclosed, or retained by PROVIDER or any party related to PROVIDER for subsequent use in any transaction. The PROVIDER will take reasonable steps to limit the use of, or disclosure of, and requests for, confidential State data to the minimum necessary to accomplish the intended purpose under this agreement. PROVIDER may not use any information collected in connection with the service issued from this proposal for any purpose other than fulfilling the service. Protection of Personally Identifiable Information (PII, as defined in the State's Terms and Conditions Governing Cloud Services and Data Usage Policy), privacy, and sensitive data shall be an integral part of the business activities of the PROVIDER to ensure that there is no inappropriate or unauthorized use of State of Delaware information at any time. The PROVIDER shall safeguard the confidentiality, integrity, and availability of State information. No party related to the PROVIDER or contracted by the PROVIDER may retain any data for subsequent use in any transaction that has not been expressly authorized by the State of Delaware.
3	✓	✓	Termination and Suspension of Service: In the event of termination of the contract, PROVIDER shall implement an orderly return of State of Delaware data in CSV, XML, or another mutually agreeable format. The PROVIDER shall guarantee the subsequent secure disposal of State of Delaware data. a) Suspension of services: During any period of suspension, contract negotiation, or disputes, the PROVIDER shall not take any action to intentionally erase any State of Delaware data. b) Termination of any services or agreement in entirety: In the event of termination of any services or agreement in entirety, the PROVIDER shall not take any action to intentionally erase any State of Delaware data for a period of ninety (90) days after the effective date of the termination. All obligations for protection of State data remain in place and enforceable during this 90-day period. After such 90-day period has expired, the PROVIDER shall have no obligation to maintain or provide any State of Delaware data and shall thereafter, unless legally or contractually prohibited, dispose of all State of Delaware data in its systems or otherwise in its possession. Within this 90-day timeframe, the PROVIDER will continue to secure and back up State of Delaware data covered under the contract. c) Post-Termination Assistance: The State of Delaware shall be entitled to any post-termination assistance generally made available with respect to the Services unless a unique data retrieval arrangement has been established as part of the Service Level Agreement. d) Secure Data Disposal: When non-public data is provided by the State of Delaware, the PROVIDER shall destroy all requested data in all of its forms (e.g., disk, CD/DVD, backup tape, paper). Data shall be permanently deleted, and shall not be recoverable, in accordance with National Institute of Standards and Technology (NIST) approved methods after ninety (90) days of the contract termination. The PROVIDER shall provide written certificates of destruction to the State of Delaware.



STATE OF DELAWARE
DEPARTMENT OF TECHNOLOGY AND INFORMATION
801 Silver Lake Blvd., Dover, Delaware 19904

PUBLIC AND NON-PUBLIC DATA OWNED BY THE STATE OF DELAWARE

State of Delaware Cloud and/or Offsite Hosting Specific Terms and Conditions

Contract/Agreement # _____, Appendix _____

between State of Delaware and _____ dated _____

This document shall become part of the final contract.

	Public Data	Non Public Data	
4		✓	Data Location: The PROVIDER shall not store, process, or transfer any non-public State of Delaware data outside of the United States, including for back-up and disaster recovery purposes. The PROVIDER will permit its personnel and subcontractors to access State of Delaware data remotely only as required to provide technical or call center support.
5		✓	Encryption: The PROVIDER shall encrypt all non-public data in transit regardless of the transit mechanism. For engagements where the PROVIDER stores sensitive personally identifiable or otherwise confidential information, this data shall be encrypted at rest . The PROVIDER's encryption shall be consistent with validated cryptography standards as specified in National Institute of Standards and Technology FIPS140-2 , Security Requirements. The key location and other key management details will be discussed and negotiated by both parties. When the PROVIDER cannot offer encryption at rest, they must maintain, for the duration of the contract, cyber security liability insurance coverage for any loss resulting from a data breach in accordance with the Terms and Conditions Governing Cloud Services and Data Usage Policy .
6		✓	Breach Notification and Recovery: The PROVIDER must notify the State of Delaware at eSecurity@delaware.gov immediately or within 24 hours of any determination of the breach of security as defined in 6 Del. C. §12B-101(2) resulting in the destruction, loss, unauthorized disclosure, or alteration of State of Delaware data. The PROVIDER shall send a preliminary written report detailing the nature, extent, and root cause of any such data breach no later than two (2) business days following notice of such a breach. The PROVIDER will continue to send any and all reports subsequent to the preliminary written report. The PROVIDER shall meet and confer with representatives of DTI regarding required remedial action in relation to any such data breach without unreasonable delay. If data is not encrypted (see CS3, below), Delaware Code (6 Del. C. §12B-100 et seq.) requires public breach notification of any incident resulting in the loss or unauthorized disclosure of Delawareans' Personally Identifiable Information (PII, as defined in Delaware's Terms and Conditions Governing Cloud Services and Data Usage Policy) by PROVIDER or its subcontractors. The PROVIDER will assist and be responsible for all costs to provide notification to persons whose information was breached without unreasonable delay but not later than sixty (60) days after determination of the breach, except 1) when a shorter time is required under federal law; 2) when law enforcement requests a delay; or 3) reasonable diligence did not identify certain residents, in which case notice will be delivered as soon as practicable. All such communication shall be coordinated with the State of Delaware. Should the PROVIDER or its contractors be liable for the breach, the PROVIDER shall bear all costs associated with investigation, response, and recovery from the breach. This includes, but is not limited to, credit monitoring services with a term of at least three (3) years, mailing costs, website, and toll-free telephone call center services. The State will retain all determining authority for breach accountability and responsibility. The State of Delaware shall not agree to any limitation on liability that relieves the PROVIDER or its subcontractors from its own negligence, or to the extent that it creates an obligation on the part of the State to hold a PROVIDER harmless. The PROVIDER shall not issue a media notice without the approval of the State.
7		✓	Background Checks: The PROVIDER must warrant that they will only assign employees and subcontractors who have passed a federally compliant (IRS Pub 1075 2.C.3) criminal background check. The background checks must demonstrate that staff, including subcontractors, utilized to fulfill the obligations of the contract,



STATE OF DELAWARE
DEPARTMENT OF TECHNOLOGY AND INFORMATION
801 Silver Lake Blvd., Dover, Delaware 19904

PUBLIC AND NON-PUBLIC DATA OWNED BY THE STATE OF DELAWARE

State of Delaware Cloud and/or Offsite Hosting Specific Terms and Conditions

Contract/Agreement # _____, Appendix _____

between State of Delaware and _____ dated _____

This document shall become part of the final contract.

	Public Data	Non Public Data																						
			have no convictions, pending criminal charges, or civil suits related to any crimes of dishonesty. This includes but is not limited to criminal fraud, or any conviction for any felony or misdemeanor offense for which incarceration for a minimum of one (1) year is an authorized penalty. The PROVIDER shall promote and maintain an awareness of the importance of securing the State's information among the PROVIDER's employees and agents. Failure to obtain and maintain all required criminal history may be deemed a material breach of the contract and grounds for immediate termination and denial of further work with the State of Delaware.																					
8		✓	Security Logs and Reports: The PROVIDER shall allow the State of Delaware access to system security logs that affect this engagement, its data, and or processes. This includes the ability for the State of Delaware to request a report of the records that a specific user accessed over a specified period of time.																					
9		✓	Sub-contractor Flowdown: The PROVIDER shall be responsible for ensuring its subcontractors' compliance with the security requirements stated herein.																					
10		✓	Contract Audit: The PROVIDER shall allow the State of Delaware to audit conformance including contract terms, system security, and data centers, as appropriate. The State of Delaware may perform this audit or contract with a third party at its discretion at the State's expense. Such reviews shall be conducted with at least thirty (30) days advance written notice and shall not unreasonably interfere with the PROVIDER's. business. In lieu of performing its own audit, the State may request the results of a third party audit from the PROVIDER or an attestation of compliance.																					
11		✓	Cyber Liability Insurance: An awarded vendor unable to meet the DTI Cloud and Offsite Hosting Policy requirement of encrypting PII at rest shall, prior to execution of a contract, present a valid certificate of cyber liability insurance at the levels indicated below. Further, the awarded vendor shall ensure the insurance remains valid for the entire term of the contract, inclusive of any term extension(s). Levels of cyber liability insurance required are based on the number of PII records anticipated to be housed within the solution at any given point in the term of the contract. The level applicable to this contract is: [insert appropriate level from the table below]. Should the actual number of PII records exceed the anticipated number, it is the vendor's responsibility to ensure that sufficient coverage is obtained (see table below). In the event that vendor fails to obtain sufficient coverage, vendor shall be liable to cover damages up to the required coverage amount. <table><tr><th>Level</th><th>Number of PII records</th><th>Level of cyber liability insurance required (occurrence = data breach)</th></tr><tr><td>1</td><td>1-10,000</td><td>\$2,000,000 per occurrence</td></tr><tr><td>2</td><td>10,001 – 50,000</td><td>\$3,000,000 per occurrence</td></tr><tr><td>3</td><td>50,001 – 100,000</td><td>\$4,000,000 per occurrence</td></tr><tr><td>4</td><td>100,001 – 500,000</td><td>\$15,000,000 per occurrence</td></tr><tr><td>5</td><td>500,001 – 1,000,000</td><td>\$30,000,000 per occurrence</td></tr><tr><td>6</td><td>1,000,001 – 10,000,000</td><td>\$100,000,000 per occurrence</td></tr></table>	Level	Number of PII records	Level of cyber liability insurance required (occurrence = data breach)	1	1-10,000	\$2,000,000 per occurrence	2	10,001 – 50,000	\$3,000,000 per occurrence	3	50,001 – 100,000	\$4,000,000 per occurrence	4	100,001 – 500,000	\$15,000,000 per occurrence	5	500,001 – 1,000,000	\$30,000,000 per occurrence	6	1,000,001 – 10,000,000	\$100,000,000 per occurrence
Level	Number of PII records	Level of cyber liability insurance required (occurrence = data breach)																						
1	1-10,000	\$2,000,000 per occurrence																						
2	10,001 – 50,000	\$3,000,000 per occurrence																						
3	50,001 – 100,000	\$4,000,000 per occurrence																						
4	100,001 – 500,000	\$15,000,000 per occurrence																						
5	500,001 – 1,000,000	\$30,000,000 per occurrence																						
6	1,000,001 – 10,000,000	\$100,000,000 per occurrence																						



PUBLIC AND NON-PUBLIC DATA OWNED BY THE STATE OF DELAWARE

State of Delaware Cloud and/or Offsite Hosting Specific Terms and Conditions

Contract/Agreement # _____, Appendix _____

between State of Delaware and _____ dated _____

This document shall become part of the final contract.

The terms of this Agreement shall be incorporated into the aforementioned contract. Any conflict between this Agreement and the aforementioned contract shall be resolved by giving priority to this Agreement. By signing this Agreement, the PROVIDER agrees to abide by the following applicable Terms and Conditions [check one]:

FOR OFFICIAL ☐ **1-3 (Public Data)**
USE ONLY ☐ **1-11 (Non-Public Data)**

Provider Name/Address (print): _____

Provider Authorizing Official Name (print): _____

Provider Authorizing Official Signature: _____

Date: _____



STATE OF DELAWARE
DEPARTMENT OF TECHNOLOGY AND INFORMATION
801 Silver Lake Blvd.
Dover, Delaware 19904

Doc Ref Number:	SE-CLD-001	Revision Number: 7
Document Type:	Enterprise Policy	Page: 1 of 7
Policy Title:	Terms and Conditions Governing Cloud Services and Data Usage	

Synopsis:	This policy provides guidance for State of Delaware organizations to utilize offsite or cloud facilities and services, including hosting and computing (XaaS: e.g, Software-, Infrastructure-, Platform-, etc., as-a-Service). Additionally, it addresses situations when State data is used by an entity for audit, research, or other purposes.
Authority:	Title 29 Chapter 90C Delaware Code, §9004C – General Powers, duties and functions of DTI “2) Create, implement and enforce statewide and agency technology solutions, policies, standards and guidelines, including as recommended by the Technology Investment Council on an ongoing basis and the CIO”
Applicability:	This policy is applicable to all users of the State of Delaware communications and computing resources. DTI is an Executive Branch Agency and has no authority over the customers in Legislative and Judicial Branches, as well as Local Education Agencies, and other Federal and Local Government entities that use these resources. However, all users, including these entities, must agree to abide by all policies, standards promulgated by DTI as a condition of access and continued use of these resources.
Effective:	5/15/2013
Reviewed:	4/14/2023
Approved By:	Chief Information Officer
Sponsor:	Chief Security Officer

TABLE OF CONTENTS

Section	Page
I. Policy	2
II. Definitions	4
III. Development and Revision History	5
IV. Approval Signature Block	6
V. Listing of Appendices	6





STATE OF DELAWARE
DEPARTMENT OF TECHNOLOGY AND INFORMATION
801 Silver Lake Blvd.
Dover, Delaware 19904

Doc Ref Number:	SE-CLD-001	Revision Number: 7
Document Type:	Enterprise Policy	Page: 2 of 7
Policy Title:	Terms and Conditions Governing Cloud Services and Data Usage	

I. Policy

EXECUTIVE SUMMARY

Cloud and offsite hosting and services (contracted XaaS: Infrastructure-, Platform-, Software-as-a-Service) offer credible alternatives to traditional IT delivery models. Contracted XaaS can provide benefits such as rapid delivery, enhanced scalability, development agility and new funding models.

PURPOSE

This policy establishes the terms and conditions for contracted XaaS and establishes terms and conditions for data usage. All IT-related RFPs, Contracts, etc. and data sharing engagements that may involve offsite hosting must abide by this policy and the related ~~Terms and Conditions Governing State Data Usage policy~~. The terms and conditions set forth in these policies this policy will help to protect the State's organizations by mitigating the risks associated with entrusting the State's computing operations and data to a third party.

POLICY STATEMENT

New contracts and amendments to contracts with service providers, as well as agreements regarding others (including but not limited to audit, research, etc.), are expected to include data usage and/or cloud services a cloud services and data usage signed agreements, as applicable, approved by DTI. When it applies, the ~~Terms and Conditions Governing Cloud Services and Data Usage~~ policy requires a signed ~~Delaware Cloud Services Terms and Conditions Agreement~~ Terms and Conditions Governing Cloud Services and Data Usage Agreement, in addition to the signed ~~Delaware Data Usage Terms and Conditions Agreement~~. The ~~Terms and Conditions Governing State Data Usage~~ policy requires a signed ~~Delaware Data Usage Terms and Conditions Agreement~~ for any XaaS engagement or other agreement requiring service provider or other (including but not limited to audit, research, etc.) access to, or use of, state data. Contracts or other agreements already in force will be expected to include the applicable signed agreements approved by DTI at the next renewal or revision date. The following standard agreements are is available:

- [Terms and Conditions Governing Cloud Services and Data Usage Agreement \(PDF\)](#)
- ~~[Delaware Data Usage Terms and Conditions Agreement \(PDF\)](#)~~



Delivering Technology that Innovates



STATE OF DELAWARE
DEPARTMENT OF TECHNOLOGY AND INFORMATION
801 Silver Lake Blvd.
Dover, Delaware 19904

Doc Ref Number:	SE-CLD-001	Revision Number: 7
Document Type:	Enterprise Policy	Page: 3 of 7
Policy Title:	Terms and Conditions Governing Cloud Services and Data Usage	

Nothing in this policy statement or its related agreement precludes state agencies from imposing their own industry-specific terms and conditions as their business might require, above and beyond those promulgated by DTI.

IMPLEMENTATION RESPONSIBILITY

DTI and/or the organization's technical staff will implement this policy during the course of normal business activities, including project execution and the design, development, or support of systems.

Service providers ~~shall~~ **should** be familiar with, and adhere to, security guidelines closely aligned with standardized industry approaches to assessment, documentation, monitoring, and controls for cloud products and services, such as those promulgated by the Federal Risk and Authorization Management Program (FedRAMP), Cloud Security Alliance (CSA), the National Institute of Standards and Technology (NIST), and other accreditation authorities as these become recognized by the industry.

ENFORCEMENT and WAIVER

DTI will enforce this policy during the course of normal business activities, including review of proposed projects and during the design, development, or support of systems. This policy may also be enforced by others during the course of their normal business activities, including contract execution, review or amendment, audits, and design reviews.

Cyber Security Liability Insurance

The State of Delaware places paramount importance on protection of sensitive Personally Identifiable Information (PII) or otherwise confidential information as defined by 6 Del. C. §1202C (15) and §12B-101(7)a, and as noted below under Section II – Definitions.

In accordance with the State's ~~Contracted Computing and Cloud Services Terms and Conditions Agreement Item 4~~ **Terms and Conditions Governing Cloud Services and Data Usage Agreement Item 5**, non-public state data shall be encrypted in transit and, for PII data, at rest. A service provider will employ validated cryptography standards as specified in National Institute of Standards and Technology FIPS140-2 Security Requirements. When the Service Provider cannot offer encryption at rest, they must



Delivering Technology that Innovates



STATE OF DELAWARE
DEPARTMENT OF TECHNOLOGY AND INFORMATION
801 Silver Lake Blvd.
Dover, Delaware 19904

Doc Ref Number:	SE-CLD-001	Revision Number: 7
Document Type:	Enterprise Policy	Page: 4 of 7
Policy Title:	Terms and Conditions Governing Cloud Services and Data Usage	

maintain, for the duration of the contract, cyber security liability insurance coverage for any loss resulting from a data breach. Such a liability protection policy shall comply with the State's requirements, incorporated by addendum to this policy (see Addendum 1: Cyber Security Liability Insurance Requirement).

In the event a service provider fails to keep in effect at all times the insurance coverage required by this provision, the State may, in addition to pursuing any other remedies available, terminate the contract upon the occurrence of such event, subject to the provisions of the contract.

If there is ambiguity or confusion regarding any part of this policy, seek clarification from the point of contact defined in the header of this policy.

II. Definitions

Personally Identifiable Information (PII)

1. Information or data, alone or in combination, that identifies or authenticates a particular individual. Such information or data may include, without limitation, Name, Date of birth, Full address (e.g. house number, city, state, and/or zip code), Phone Number, Passwords, PINs, Federal or state tax information, Biometric data, Unique identification numbers (e.g. driver's license number, social security number, credit or debit account numbers, medical records numbers), Criminal history, Citizenship status, Medical information, Financial Information, Usernames, Answers to security questions or other personal identifiers.
2. Information or data that meets the definition ascribed to the term "Personal Information" under Delaware Code Title 6 § 12B-101 Title 6, §1202C, and Title 29 §9017C or any other applicable State of Delaware or Federal law.

III. Development and Revision History

Date	Revision
5/15/2013	Rev 0 – Initial version
8/27/2014	Rev 1 – Updated version
11/17/2014	Rev 2 – Updated version



Delivering Technology that Innovates



STATE OF DELAWARE
DEPARTMENT OF TECHNOLOGY AND INFORMATION
801 Silver Lake Blvd.
Dover, Delaware 19904

Doc Ref Number:	SE-CLD-001	Revision Number: 7
Document Type:	Enterprise Policy	Page: 5 of 7
Policy Title:	Terms and Conditions Governing Cloud Services and Data Usage	

11/23/2015	Rev 3 - Removed language regarding the State's inclusion on the insured list.
3/1/2016	Rev 4 - Added Tiered Coverage Schedule. Added PII definition. Adjusted Ponemon value. Updated link for The Center for Digital Government 2014 study of Cloud Security Procurements.
10/10/2016	Rev 5 - Added language and references to State standards in the Implementation Responsibility section.
2/1/2018	Rev 5 - Added language and references to State standards in the Implementation Responsibility section.
6/18/2018	Rev 6 - Revised policy titles and agreement references. Added language and references to new Data Usage Terms and Conditions Policy, as well as to State standards in the Implementation Responsibility section; revised DelCode references with respect to definitions of Personally Identifiable Information (PII); moved information regarding Cyber Liability Insurance Requirement to be incorporated by Addendum 1.
4/14/2023	Rev 7 - Revised the wording to reflect the consolidated policy and agreement documents.

IV. Approval Signature Block

Name & Title: State Chief Information Officer	Date



Delivering Technology that Innovates



STATE OF DELAWARE
DEPARTMENT OF TECHNOLOGY AND INFORMATION
801 Silver Lake Blvd.
Dover, Delaware 19904

Doc Ref Number:	SE-CLD-001	Revision Number: 7
Document Type:	Enterprise Policy	Page: 6 of 7
Policy Title:	Terms and Conditions Governing Cloud Services and Data Usage	

VI. Listing of Appendices

APPENDIX 1

CYBER SECURITY LIABILITY INSURANCE REQUIREMENTS

- Issued by an insurance company acceptable to the State of Delaware and valid for the entire term of the contract, inclusive of any term extension(s).
- Liability limits will be calculated based on the maximum system record count over the life of the contract and the **Ponemon Institute** average Public Sector Breach cost per record as published in the most recent *Cost of Breach Study* (e.g., 2017, \$141). Refer to the Tiered Coverage Schedule below.

Tiered Coverage Schedule

Level	Number of PII records	Level of cyber liability insurance required (occurrence = data breach)
1	1-10,000	\$2,000,000 per occurrence
2	10,001 – 50,000	\$3,000,000 per occurrence
3	50,001 – 100,000	\$4,000,000 per occurrence
4	100,001 – 500,000	\$15,000,000 per occurrence
5	500,001 – 1,000,000	\$30,000,000 per occurrence
6	1,000,001 – 10,000,000	\$100,000,000 per occurrence

- Shall include, but not be limited to, coverage for liabilities arising out of premises, operations, independent contractors, products, completed operations, and liability assumed under an insured contract.
- At a minimum, the policy must include third party coverage for credit monitoring; notification costs to data breach victims; and regulatory penalties and fines.
- Shall apply separately to each insured against whom claim is made or suit is brought subject to the Service Provider's limit of liability.
- Shall include a provision requiring that the policy cannot be cancelled without thirty days written notice to the State Chief Information Officer.
- The Service Provider shall be responsible for any deductible or self-insured retention contained in the insurance policy.



Delivering Technology that Innovates



STATE OF DELAWARE
DEPARTMENT OF TECHNOLOGY AND INFORMATION
801 Silver Lake Blvd.
Dover, Delaware 19904

Doc Ref Number:	SE-CLD-001	Revision Number: 7
Document Type:	Enterprise Policy	Page: 7 of 7
Policy Title:	Terms and Conditions Governing Cloud Services and Data Usage	

- The coverage under the policy shall be primary, and not excess, to any other insurance carried by the Service Provider.
- The State of Delaware shall not be a named or additional insured under the policy.

Additional Reference Documents

[21 Steps to the Cloud](#) — Center for Digital Government's Infographic *Guide to Cloud Procurements* best practices.

[Terms and Conditions Governing State Data Usage](#)



Delivering Technology that Innovates