



**DELAWARE CLOUD SERVICES TERMS AND CONDITIONS AGREEMENT**

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

XaaS Contract # \_\_\_\_\_, Appendix \_\_\_\_\_  
 between State of Delaware and \_\_\_\_\_ dated \_\_\_\_\_

	Public Data	Non Public Data	Cloud Services (CS) Terms
			<p><b>PROVIDER must satisfy Clause CS1-A OR Clauses CS1-B and CS1-C, AND Clause CS4.</b>  <b>Clause CS2 is mandatory for all engagements involving non-public data.</b>  <b>Clause CS3 is only mandatory for SaaS or PaaS engagements involving non-public data.</b></p>
CS1-A		✓	<p><b>Security Standard Compliance Certifications:</b> The PROVIDER<sup>1</sup> shall meet, and provide proof of, one or more of the following Security Certifications.</p> <ul style="list-style-type: none"> <li>• CSA STAR – Cloud Security Alliance – Security, Trust &amp; Assurance Registry (Level Two or above)</li> <li>• FedRAMP - Federal Risk and Authorization Management Program</li> </ul>
CS1-B		✓	<p><b>Background Checks:</b> The PROVIDER must warrant that they will only assign employees and subcontractors who have passed a state-approved criminal background checks. The background checks must demonstrate that staff, including subcontractors, utilized to fulfill the obligations of the contract, have no convictions, pending criminal charges, or civil suits related to any crime 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 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 Service 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.</p>
CS1-C		✓	<p><b>Sub-contractor Flowdown:</b> The PROVIDER shall be responsible for ensuring its subcontractors' compliance with the security requirements stated herein.</p>
CS2		✓	<p><b>Breach Notification and Recovery:</b> The PROVIDER must notify the State of Delaware immediately of any incident resulting in the destruction, loss, unauthorized disclosure, or alteration of State of Delaware data. If data is not encrypted (see CS 3, 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 <i>Terms and Conditions Governing Cloud Services</i> policy<sup>2</sup>) by PROVIDER or its subcontractors. The PROVIDER will provide notification to persons whose information was breached without unreasonable delay but not later than 60 days after determination of the breach, except 1) when a shorter time is required under</p>

<sup>1</sup> Provider is the contractor, company or vendor as defined in the contract.

<sup>2</sup> This includes Personal Health Information (PHI): <https://webfiles.dti.gov/pdfs/pp/dataclassificationguideline.pdf>



**DELAWARE CLOUD SERVICES TERMS AND CONDITIONS AGREEMENT**

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

XaaS Contract # \_\_\_\_\_, Appendix \_\_\_\_\_  
 between State of Delaware and \_\_\_\_\_ dated \_\_\_\_\_

	Public Data	Non Public Data	Cloud Services (CS) Terms
			<p><b>PROVIDER must satisfy Clause CS1-A OR Clauses CS1-B and CS1-C, AND Clause CS4.</b>  <b>Clause CS2 is mandatory for all engagements involving non-public data.</b>  <b>Clause CS3 is only mandatory for SaaS or PaaS engagements involving non-public data.</b></p>
			<p>federal law; 2) when law enforcement requests a delay; 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<sup>3</sup>, mailing costs, website, and toll-free telephone call center services. 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.</p>
<b>CS3</b>		✓	<p><b>Data Encryption:</b> The PROVIDER shall encrypt all non-public data in transit, regardless of transit mechanism.<sup>4</sup> For engagements where the PROVIDER stores Personally Identifiable Information (PII) or other sensitive, confidential information, it shall encrypt this non-public data at rest. The PROVIDER’s encryption shall meet validated cryptography standards as specified by the National Institute of Standards and Technology in FIPS140-2 and subsequent security requirements guidelines. The PROVIDER and State of Delaware will negotiate mutually acceptable key location and key management details. Should the PROVIDER not be able to provide encryption at rest, it must maintain cyber security liability insurance coverage for the duration of the contract. Coverage must meet the State of Delaware’s standard in accordance with the <i>Terms and Conditions Governing Cloud Services</i> policy.<sup>5</sup></p>

<sup>3</sup> A minimum of three years is non-negotiable.

<sup>4</sup> For the requirements for secure email transmission, please see <http://dti.delaware.gov/pdfs/pp/SecureEmail.pdf>. It is the State’s preference that confidential data will not be accessed on mobile devices. If so, for the requirements please see <http://dti.delaware.gov/pdfs/pp/MobileDeviceEncryptionStandard.pdf>.

<sup>5</sup> See the policy at: <https://webfiles.dti.delaware.gov/pdfs/pp/Terms%20and%20Conditions%20Governing%20Cloud%20Services%20Policy.pdf>  
 Records are defined as the number of covered members.



**DELAWARE CLOUD SERVICES TERMS AND CONDITIONS AGREEMENT**

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

XaaS Contract # \_\_\_\_\_, Appendix \_\_\_\_\_  
 between State of Delaware and \_\_\_\_\_ dated \_\_\_\_\_

	Public Data	Non Public Data	Cloud Services (CS) Terms
			<p><b>PROVIDER must satisfy Clause CS1-A OR Clauses CS1-B and CS1-C, AND Clause CS4.</b>  <b>Clause CS2 is mandatory for all engagements involving non-public data.</b>  <b>Clause CS3 is only mandatory for SaaS or PaaS engagements involving non-public data.</b></p>
CS4	✓	✓	<p><b>Notification of Legal Requests:</b> The PROVIDER shall contact the State of Delaware upon receipt of any electronic discovery, litigation holds, discovery searches, and expert testimonies related to, or which in any way might reasonably require access to the data of the State. With regard to State of Delaware data and processes, the PROVIDER shall not respond to subpoenas, service of process, and other legal requests without first notifying the State unless prohibited by law from providing such notice.<sup>6</sup></p>

**(Note: If the Data Usage (DU) Terms also apply to this engagement, DU6, Breach Notification and Recovery, and DU7, Data Encryption, are duplicative of CS2 and CS3, respectively.)**

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 :

FOR OFFICIAL  CS1 A and CS4 OR  CS1-B and CS1-C and CS4  
 USE ONLY  CS2 (Non-public Data)  CS3 (SaaS, PaaS – Non-public Data)

PROVIDER Name/Address (*print*): \_\_\_\_\_

PROVIDER Authorizing Official Name (*print*): \_\_\_\_\_

PROVIDER Authorizing Official Signature: \_\_\_\_\_ Date: \_\_\_\_\_

<sup>6</sup> This includes Freedom of Information Act (FOIA) requests.