



## Q1 : What is new?

**A1-1:** Updated policy for *Terms and Conditions Governing Cloud Services* for procuring X-a-a-S or Hybrid cloud deployments with a simplified *Delaware Cloud Services Terms & Conditions Agreement*.

**A1-2:** New, separate policy for *Terms and Conditions Governing State Data Usage* simplifies data sharing for audits, research collaboration and other data usage for providers and non-IT staff.

**A1-3:** Fast-Track for providers/vendors holding cloud security certifications. Leveraging these industry standards the State can validate provider/vendor cloud security controls compliance. Currently the Cloud Security Alliance (CSA) Star and Federal Risk Authorization Management Program (FedRAMP) are accepted certifications.

## Q2 : What has been removed?

**A2-1:** The Data Protection term has been removed. Data Protection language was included in the new Data Usage term for clarity.

**A2-2:** The Data Dictionary term has been removed. A Data Dictionary agreement should be negotiated outside of this set of terms since it is not security related.

**A2-3:** The Security Log and Reports term has been removed. The State no longer requires access to logs.

**A2-4:** The Contract Audit term has been removed. If required, Contract audit terms should be negotiated.

**A2-5:** The Operational Metrics term has been removed. Operational Metrics should be negotiated in the Service Level Agreement.

**A2-6:** The Sub-contractor Disclosure term has been replaced. The new Sub-contractor Flowdown term replaces the old term.



---

**Q3 : Why are there now two policies and two agreements?**

**A3:** The revisions recognize that not all engagements require cloud services; some engagements simply revolve around the use of State data. Consequently, a new *Terms and Conditions Governing State Data Usage* policy has been developed, along with its associated agreement. These documents include the terms related to data protection. The *Terms and Conditions Governing Cloud Services* policy now only includes the terms related to cloud provider/vendor responsibilities and accountabilities, and has a separate agreement to match.

**Q4: How will these documents be used in an RFP solicitation?**

**A4:** One or both of these sets of documents will be submitted as part of the RFP package depending on use case(s). When provider/vendor selection is determined the necessary terms must be finalized with the provider/vendor.

**Q5: Has the Delaware Department of Justice reviewed these policies and terms?**

**A5:** Yes.

**Q6: What is the effective date and cutover date for the new policies and agreements?**

**A6:** The current Terms and Conditions will be retired on 6/18/2018. All current engagements and in-flight negotiations will continue to leverage the current *Cloud and Offsite Hosting Policy* terms and conditions. Once the two new policies and their agreements are effective, all new and renewing engagements, contracts, and renewals negotiated after that date will be required to adhere to these. A waiver will only be accepted if engagements adhering to the new policies are deemed impossible to negotiate due to time constraints. A date for bringing the contractual relationship into compliance will be determined at time of waiver.

**Q7: If a vendor has already signed the T&Cs, do they need to re-sign the new ones?**

**A7:** Yes eventually! You may go back and insert the new T&Cs into existing contracts but it is not required. What is required is that the new T&Cs are replaced at the next renewal.



**Q8: When should I inform my providers/vendors of Delaware’s new policies and agreements?**

**A8:** Procurement Officers should inform providers/vendors of this change as of the new policies’ effective dates. Providers/vendors should understand that compliance will be required at the time of a renewal or extension of that contract.

**Q9: Does a blank box in the PUBLIC column on the agreement indicate a term is *not* required?**

**A9:** Yes.

**Q10: If data ownership has been transferred from the State to a provider do we still need Delaware Data Usage Terms and Conditions Agreement signed?**

**A10:** No. If Data Ownership has been passed to the provider/vendor no Terms and Conditions are necessary (e.g., Federal agency request for State data—either a one-time or subscription request—where data becomes the Federal agency’s to use).

**Q11: What terms apply if we are sending data to a provider or other organization for audit, research, aggregation, or analysis with no Cloud involvement?**

**A11:** These transactions include when another organization is taking action on data on behalf of Delaware for Delaware (e.g., UD research using State data that provides outcomes for State programs) qualifies as a simple data usage agreement. Only the *Delaware Data Usage Terms and Conditions Agreement* would be required.

**Q12: Can state organizations add more restrictions beyond these policies and terms?**

**A12:** Yes. In certain cases, an agency or school district may require even tighter data security terms.



**Q13: Why require only CSA Star and/or FedRAMP certifications?**

**A13:** These are internationally recognized and provide actual certifications. Certain agencies may require providers/vendors to comply with other recognized cloud security standards (e.g., HIPAA, FISMA, GDPR, etc.)

**Q14: How can I find out if the provider is CSA Star and/or FedRAMP certified?**

**A14:** You can start by asking them. For independent verification, check out [https://cloudsecurityalliance.org/star/#\\_registry](https://cloudsecurityalliance.org/star/#_registry) and <https://marketplace.fedramp.gov/#/products?sort=productName>. The vendor will be required to provide proof of their active certification before the contract is signed.

**Q15: Which terms apply to my project? (See table)**

**A15:** There are three important factors to consider:

1. Is this a SaaS, PaaS, IaaS, or simple data usage agreement?
2. Is the classification of the data PUBLIC or NON-PUBLIC
3. Does the provider/vendor hold a FedRAMP authorization or a Cloud Security Alliance STAR certification? (“Certified” below)

	TYPE OF ENGAGEMENT	REQUIRED CLOUD Ts & Cs	REQUIRED DATA USAGE Ts & Cs
1	Certified, SaaS, PUBLIC	CS1-A, CS4	DU1, DU2, DU3
2	Certified, IaaS, PUBLIC	CS1-A, CS4	DU1, DU2, DU3
3	Certified, PaaS, PUBLIC	CS1-A, CS4	DU1, DU2, DU3
4	Certified, SaaS, NON-PUBLIC	CS1-A, CS2, CS3, CS4	DU1, DU2, DU3, DU4, DU5, DU6, DU7
5	Certified, IaaS, NON-PUBLIC	CS1-A, CS2, CS4	DU1, DU2, DU3, DU4, DU5, DU6, DU7
6	Certified, PaaS, NON-PUBLIC	CS1-A, CS2, CS3, CS4	DU1, DU2, DU3, DU4, DU5, DU6, DU7

CLOUD SECURITY TERMS AND CONDITIONS  
 FREQUENTLY ASKED QUESTIONS



	TYPE OF ENGAGEMENT	REQUIRED CLOUD Ts & Cs	REQUIRED DATA USAGE Ts & Cs
7	Not Certified, SaaS, PUBLIC	CS4	DU1, DU2, DU3
8	Not Certified, IaaS, PUBLIC	CS4	DU1, DU2, DU3
9	Not Certified, PaaS, PUBLIC	CS4	DU1, DU2, DU3
10	Not Certified, SaaS, NON-PUBLIC	CS1-B, CS1-C, CS2, CS3, CS4	DU1, DU2, DU3, DU4, DU5, DU6, DU7
11	Not Certified, IaaS, NON-PUBLIC	CS1-B, CS1-C, CS2, CS4	DU1, DU2, DU3, DU4, DU5, DU6, DU7
12	Not Certified, PaaS, NON-PUBLIC	CS1-B, CS1-C, CS2, CS3, CS4	DU1, DU2, DU3, DU4, DU5, DU6, DU7
13	Data Usage only, PUBLIC	N/A	DU1, DU2, DU3
14	Data Usage only, NON-PUBLIC	N/A	DU1, DU2, DU3, DU4, DU5, DU6, DU7
15	Data Usage when ownership transfers from State to Provider	N/A	N/A

**Q16: Do I need signed agreements for each contract/engagement or each vendor?**

**A16:** Agreements become part of the contract. Each contract needs its own agreement(s).

**Q17: I understand many cloud providers/vendors have signed Delaware’s Terms and Conditions; where is the list?**

**A17:** DTI maintains a log of every contract already including our Cloud Terms and Conditions; we are working to publish this as a reference for our customers. Keep in mind that each contract may be unique to an agency or school district’s needs and/or the specific product offering. Incorporating the applicable terms and conditions agreement document(s) into your contract is still important.