



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 6
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 6
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. The terms and conditions set forth in 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 a cloud services and data usage signed agreement, as applicable, approved by DTI. When it applies, the *Terms and Conditions Governing Cloud Services and Data Usage* policy requires a signed *Terms and Conditions Governing Cloud Services and Data Usage Agreement*. 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 agreement is available:

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

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.



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 6
Policy Title:	Terms and Conditions Governing Cloud Services and Data Usage		

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 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 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 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).



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 6
Policy Title:	Terms and Conditions Governing Cloud Services and Data Usage		

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.





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 6
Policy Title:	Terms and Conditions Governing Cloud Services and Data Usage		

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
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:	Date
State Chief Information Officer	



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 6
Policy Title:	Terms and Conditions Governing Cloud Services and Data Usage		

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.
- 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.

