Doc Ref Number:	SE-CLD-002	**Revision Number:** 0
Document Type:	Enterprise Policy	**Page:** 1 of 6
Policy Title:	Terms and Conditions Governing State Data Usage	

Synopsis:	This policy provides guidance for State of Delaware organizations when State data is utilized or stored offsite through a contract with an offsite facility or Cloud Service Provider, or when State data is used by an entity for audit, research, or other purposes.
Authority:	Title 29, Delaware Code, §9004C, - General powers, duties and functions of DTI "*2) Implement statewide and interagency technology solutions, policies, standards and guidelines as recommended by the Technology Investment Council on an ongoing basis and the CIO, including, but not limited to, statewide technology and information architectures, statewide information technology plans, development life cycle methodologies, transport facilities, communications protocols, data and information sharing considerations, the technique of obtaining grants involving the State's informational resources and the overall coordination of information technology efforts undertaken by and between the various State agencies;*" §9006C – Requirements for agency technology projects "(d) *Management control and policy direction over all aspects of computerized data requirements definition, data acquisition, data storage and dissemination, data retention and data retirement standards shall be the sole province of the Department of Technology and Information."* §90014C – *"(6) Develop minimum technical standards, guidelines, and architectures as required for state technology projects."*
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 School Districts, 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 Date:	6/18/2018 **Expiration Date:** None
POC for Changes:	Elayne Starkey, Chief Security Officer
Approval By:	James Collins, Chief Information Officer
Approved On:	6/18/2018

TABLE OF CONTENTS

Section **Page**

I.	**Policy**	2
II.	**Definitions**	3
III.	**Development and Revision History**	4
IV.	**Approval Signature Block**	5
V.	**Listing of Appendices**	5

I. Policy

EXECUTIVE SUMMARY

It is important for the State of Delaware to ensure proper measures are employed by providers when handling State data in off-site locations either as part of a cloud services engagement, or for audit, research, or other uses.

PURPOSE

This policy establishes the data usage terms and conditions for provider services when State data is utilized in an off-site location. All IT-related RFPs, contracts, etc. must abide by this policy and the related *Terms and Conditions Governing Cloud Services* policy, if applicable. The terms and conditions set forth in these policies will help to protect the State's organizations by mitigating the risks associated with entrusting the State's data to a third party.

POLICY STATEMENT

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

- *Delaware Data Usage Terms and Conditions Agreement* (PDF)
- *Delaware Cloud Services Terms and Conditions 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.

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 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 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, 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).

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

Initial version established **06/18/2018**

IV. Approval Signature Block

Name & Title: James Collins State Chief Information Officer	**Date**

V. 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 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.

Additional Reference Documents

21 Steps to the Cloud – Center for Digital Government's Infographic *Guide to Cloud Procurements* best practices.

Terms and Conditions Governing Cloud Services (PDF)