

Appendix Q – DTI Technology Policies

Digital Accessibility Policy

Terms and Conditions Governing Cloud Services and Data Usage Policy

Terms and Conditions Governing Cloud Services and Data Usage Agreement



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

Doc Ref Number:	AC-DIG-001	Revision Number:	0
Document Type:	Enterprise Policy	Page:	1 of 6
Policy Title:	Digital Accessibility Policy		

Synopsis:	This policy contains scope and technical requirements for State of Delaware agencies to ensure accessibility and usability for all digital information by individuals with disabilities.
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. The Department of Technology and Information (DTI) is an Executive Branch Agency and has no authority over the users 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:	1/30/2023
Reviewed:	1/30/2023
Approved By:	Chief Information Officer
Sponsor:	Chief Technology Officer





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

Doc Ref Number:	AC-DIG-001	Revision Number:	0
Document Type:	Enterprise Policy	Page:	2 of 6
Policy Title:	Digital Accessibility Policy		

Table of Contents

Policy	3
Definitions.....	5
Development and Revision History	6
Approval Signature Block.....	6
Listing of Appendices	6
Related Policies and Standards	6





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

Doc Ref Number:	AC-DIG-001	Revision Number:	0
Document Type:	Enterprise Policy	Page:	3 of 6
Policy Title:	Digital Accessibility Policy		

Policy

POLICY SCOPE

This Policy applies to all State of Delaware public-facing digital assets that are developed, procured, maintained, or used while offering products, services, and online information to users. This includes any accompanying support documentation and services associated with the public-facing digital channel. Employees of the State of Delaware and third-party vendors shall comply with this Policy.

EXECUTIVE SUMMARY

The State of Delaware is committed to providing the most enjoyable and informative experience to all. This includes a commitment to accessibility, diversity, and inclusion. We are working to ensure that all State of Delaware Information and Communication Technology (ICT) is accessible to and usable by individuals with disabilities, in accordance with federal, state, and local law.

POLICY STATEMENT

We have policies and procedures in place to help guarantee that we comply with the World Wide Web Consortium (W3C) Web Content Accessibility Guidelines (WCAG) 2.1 Level A and AA guidelines for websites and mobile applications. We also have made a commitment to follow the W3C [Web Content Accessibility Guidelines 2.1](#) (WCAG 2.1 levels A and AA) standards. We are firmly dedicated to complying with the [Americans with Disabilities Act \(ADA\) Titles I, II and III](#), [Section 504 and Section 508](#) of the Rehabilitation Act of 1973, the [21st Century Communications and Video Accessibility Act of 2010](#) (CVAA), and [Title 6 Delaware Code 4504](#).

POLICY PROVISIONS

General Procedures

1. [External communication](#) - The State of Delaware will maintain a publicly available Accessibility Statement in support of the State's Digital Accessibility Policy. This statement should be available directly from the [State of Delaware homepage](#). Each



"Delivering Technology that Innovates"



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

Doc Ref Number:	AC-DIG-001	Revision Number:	0
Document Type:	Enterprise Policy	Page:	4 of 6
Policy Title:	Digital Accessibility Policy		

department will maintain relevant information about the accessibility of public-facing websites, mobile apps, or other digital communications should be provided, as well as an accessible means by which individuals with disabilities can get further assistance. The information should be kept up to date with any new developments.

2. Training - This Policy will be communicated to all State of Delaware departments responsible for public-facing digital assets, including, but not limited to service representatives, product managers, project managers, designers, developers, engineers, content authors, QA analysts, and compliance/risk managers. The Policy will also be communicated to external vendors and contractors who develop public-facing digital assets for State of Delaware. Training will be offered through the Delaware Learning Center to help identified staff implement the Policy. Training will be coordinated and facilitated by the [State of Delaware Digital Accessibility Program Senior Manager or their designate](#).

Responsibilities

1. State of Delaware Digital Accessibility Senior Manager - Upon adoption of this policy, the State of Delaware Digital Accessibility Senior Manager will be responsible for the enterprise accessibility program. All State of Delaware departments responsible for public-facing digital assets should contact the [Digital Accessibility Senior Manager](#) to answer any questions about accessibility, address the accessibility of covered digital assets, and assist in handling alternative format requests. The Digital Accessibility Senior Manager will review this policy annually, to ensure both its applicability and compliance with emerging regulations and standards.
2. Compliance - All State of Delaware departments responsible for public-facing digital assets shall collaborate with the State of Delaware Digital Accessibility Senior Manager to understand accessibility requirements, receive accessibility training, address accessibility of covered public-facing digital assets, and document how the public-facing digital assets conform to Technical Standards referenced in this Policy. Departments are responsible for implementing procedures that inform authors, developers, publishers, and procurers about applicable laws, policies, and contractual obligations.
3. Evaluation and Monitoring - All State of Delaware departments responsible for public-facing digital assets shall provide standards conformance reports on an annual basis. Reports will include both components developed by the State of Delaware and components developed by third-party vendors that are deployed on or integrated into State of Delaware managed platforms or applications. The State of Delaware will conduct





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

Doc Ref Number:	AC-DIG-001	Revision Number: 0
Document Type:	Enterprise Policy	Page: 5 of 6
Policy Title:	Digital Accessibility Policy	

automated accessibility tests of its core website, at regularly scheduled intervals mandated by the State of Delaware Digital Accessibility Senior Manager, to identify any instances where the core website or other key digital communications are not in conformance with the Technical Standards referenced in this Policy.

EXCEPTIONS

Where compliance with this Policy is not possible, exceptions to this Policy may be granted by the State of Delaware. Requests for exceptions must be documented and submitted to the State of Delaware Digital Accessibility Program Senior Manager. Exceptions may be granted in scenarios such as not readily achievable, undue burden or fundamental alteration, user generated content, linked sites and resources, external digital content, short term digital content, orphaned digital content, back office, public safety systems, state contracts, ICT functions located in maintenance or monitoring spaces, etc. For more information, visit the following [website](https://accessibility.dti.delaware.gov/) (<https://accessibility.dti.delaware.gov/>).

Definitions

Accessibility – it means the degree to which an environment, service, or product allows access by as many people as possible, in particular, people with disabilities.

Accessibility Standards incorporated by reference – it means conventions, norms or requirements intended to provide access to an environment, product, or service, particularly to people with disabilities. The principle of accessibility may be mandated in law and specified in detail per regulations, standards, or codes.

Alternative Formats – it means information presented in Braille, in large print, via audio recording, or in an electronic format that can be accessed by people with disabilities. The Alternative Format must make the same content available and provide an equivalent level of access to the content by people with disabilities that is available to others who access the original document.

Public-Facing Digital Content - it includes, but is not limited to, electronic or digital content, communications or applications that are:

- In HTML, non-HTML, or mobile platform digital formats
- Public-facing and broadly disseminated, including products and services information, account information, etc.





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

Doc Ref Number:	AC-DIG-001	Revision Number:	0
Document Type:	Enterprise Policy	Page:	6 of 6
Policy Title:	Digital Accessibility Policy		

- Public support mechanisms (e.g., chat, email, etc.)
- Digital marketing and social media content

For the purposes of this Policy – “Public-Facing Digital Content” shall not include Archival documents stored or retained solely for archival purposes to preserve an exact image of a hard copy; or draft versions of documents that are not public-facing, or which are intended for limited distribution.

Readily Achievable - it is defined as easily accomplishable and able to be carried out without much difficulty or expense. Failure to remove accessibility barriers where “readily achievable” might constitute discrimination. Determining what is “readily achievable” often involves analyzing the nature and cost of removing barriers and the overall financial resources of the business organization, among other factors. The analysis seeks to balance the benefit of the barrier’s removal and the harm (e.g., cost) to the business.

Development and Revision History

Date	Revision
1/30/2023	Rev 0 - Initial version

Approval Signature Block

On File	
Name & Title: State Chief Information Officer	Date

Listing of Appendices

Related Policies and Standards



“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: 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.



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 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.



Delivering Technology that Innovates



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

State of Delaware Terms and Conditions Governing Cloud Services and Data Usage Agreement

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 Terms and Conditions Governing Cloud Services and Data Usage Agreement

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 Terms and Conditions Governing Cloud Services and Data Usage Agreement

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 Terms and Conditions Governing Cloud Services and Data Usage 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. 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 Terms and Conditions Governing Cloud Services and Data Usage Agreement

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: _____