



Policy Title:	Confidentiality (Non-Disclosure) and Integrity of Data	
Doc Ref Number:	DTI-0065.02	
Policy Type:	Internal Only	Page: 1 of 8
Synopsis:	<p>Employees and contractors working for the Delaware Department of Technology & Information (DTI) have unique access to citizen, customer and employee records, communications and data storage equipment. This policy establishes expectations and standards of behavior in safeguarding information that others entrust to us. Employees and contractors are required to take all necessary precautions not only to prevent unauthorized disclosure or modification of State computer files, but will bring to the attention of their immediate supervisor any situation which might result in, or create the appearance of, unauthorized disclosure or modification of State data.</p>	
Authority:	<p>Delaware Title 29, Chapter 90C, § 9002C. Establishment of the Department of Technology and Information.</p> <p>A Department of Technology and Information is established to replace the Office of Information Services within the Executive Department, and shall have the powers, duties and functions vested in the Department by this chapter. (73 Del. Laws, c. 86, § 1; 74 Del. Laws, c. 128, § 11.)</p>	
Applicability:	<p>All organizational elements of the Department of Technology and Information, including but not limited to:</p> <ul style="list-style-type: none"> - DTI Employees - Any consolidated staff from other organizations - State Employees working within DTI - Contractors and private organizations providing products, services and/or support. 	
Effective Date:	December 7, 2005	
POC for Change:	Chief Security Officer	

POLICY

A Message to All DTI Employees/Contractors

Our jobs at the Delaware Department of Technology & Information (DTI) give us unique access to citizen, customer and employee records, communications and data storage equipment. We are trusted to use their information with care. We will carefully handle both DTI information and information that others entrust to us. Each of us is responsible for upholding the DTI's commitment to the highest standards of business conduct.

DTI employees/contractors will take all necessary precautions not only to prevent unauthorized disclosure or modification of State computer files, but will bring to the attention of their immediate supervisor any situation which might result in, or create the appearance of, unauthorized disclosure or modification of State data.



STATE OF DELAWARE
DEPARTMENT OF TECHNOLOGY AND INFORMATION
801 SILVER LAKE BLVD.
DOVER, DELAWARE 19904

Because this agreement cannot address every situation and issues continue to evolve in our rapidly changing environment, you can seek assistance; discuss concerns or report violations through numerous channels, including your supervisor or Team Leader. You are accountable for familiarizing yourself with this agreement:

Read: the agreement and give careful attention to those subjects that most pertain to your job duties.

Understand: the purpose of this Confidentiality and Non-disclosure Agreement and your overall responsibilities for DTI's standards of business conduct.

Consult Related Documents: employees/contractors should review and understand related DTI policies, including those governing "Acceptable Use", "FOIA", "e-Records Request", "Data & UserID Security", "Data Classification Policy" and "Disposal of Electronic Equipment/Storage Media."

Acknowledgement: employees/contractors must attest to their compliance by signing the Confidentiality and Non-disclosure acknowledgement form. See appendices 1 & 2.

Introduction

DTI employees are responsible for safeguarding the confidentiality and integrity of data in State computer files regardless of the source of those data or the medium on which they are stored; e.g., printed page, photocopies, or tape or disk. Computer programs developed to process State Agency data will not be modified without the knowledge and written authorization of that State Agency's Representative. All source data submitted by any State Agency to the Department of Technology and Information, and all data generated from the original source data, shall be the property of the State of Delaware. The control of the disclosure of those data shall be retained by the State Agency and DTI.

Note: References to "customers" in this document include the agencies/organizations we serve, citizens, and DTI employees

Applicability

DTI's expectations for responsible conduct are applicable to all parties who work on behalf of DTI, including, but not limited to, its employees, consultants, in-house contractors, and employees of vendors completing work on behalf of DTI.

Corrective Action and Discipline

Employees who violate DTI policies and standards may be disciplined up to and including dismissal, as well as be subject to civil and criminal charges. If misconduct occurs, DTI is committed to taking prompt and responsive action to correct the situation and discipline responsible individuals.

Management employees may be disciplined if they condone misconduct, do not report misconduct, do not take reasonable measures to detect misconduct, or do not demonstrate the appropriate leadership to ensure compliance.

DTI has no authority to discipline consultants, in-house contractors, and employees of vendors completing work on behalf of DTI, but expects the same level of compliance and will take the appropriate steps to ensure any misconduct is appropriately addressed.



STATE OF DELAWARE
DEPARTMENT OF TECHNOLOGY AND INFORMATION
801 SILVER LAKE BLVD.
DOVER, DELAWARE 19904

Compliance with Privacy Laws

We have a responsibility to our customers (agencies, citizens, employees) to comply with all applicable privacy laws and regulations. We should not listen -nor allow others- to customer conversations or monitor data transmissions unless it is part of our job responsibilities, and even then, only in compliance with applicable law. We should not tamper with or intrude upon conversations using wiretaps or other methods, except when authorized by law. We will neither confirm nor deny to customers or to any unauthorized person the existence of, or any information concerning, a subpoena, warrant or court order for communications, wiretaps and/or records, unless authorized by law. **During the course of employment, employees may receive a subpoena or similar inquiries from law enforcement or the government requesting or directing them to furnish records or information in the possession of DTI, including records or other customer-specific data. Employees should provide these requests immediately to their Team Leader or directly to DTI's FOIA Coordinator (Office of the CIO Executive Secretary).**

Question – A neighbor is working on a committee to help elect a new state representative. Her committee needs voter registration information for the communities in our area. She has asked me to help out by providing that information. Is it OK to try to get this information for my neighbor?

Answer - NO. You should never use your position at DTI to access information that is not available directly to the public. You should direct your neighbor to the Department of Elections who ensures all requests for voting information complies with Delaware law.

We Safeguard Customer Information

DTI possesses sensitive, detailed information about customers who trust us to safeguard that information. Any inappropriate use of confidential customer information violates that trust and weakens our relationship with our customers. For these reasons, it is a serious breach of our policies, and in some cases of the law, to use customer information for anything other than DTI business purposes. Accessing customer records, unless there is a valid business purpose, or divulging this information to any other persons, including friends, co-workers or former employees, is inappropriate. Unless we have a supervisor's express approval, we should never access our own accounts, or those of our relatives, friends, or co-workers.

Question - A friend of mine in the real estate business has asked me for some confidential information on a renter who skipped out owing three months' rent. Through my job, I have access to the information my friend needs. Can I give it to my friend?

Answer - Absolutely not. You should refuse to provide that information to your friend. Our policies prohibit using confidential information for anything other than legitimate DTI business purposes. Even requests from law enforcement or governmental agencies must always be referred to the DTI FOIA Coordinator.

U.S. Government Classified and National Security

Some of our employees have access to information covered under the U.S. Espionage Act and other regulations that govern our work with U.S. classified and national security information and impose stringent penalties for misuse of this information.

We will protect U.S. Government classified and national security information by:

- Ensuring that access to this information is restricted only to employees with proper clearance and a "need to know".
- Safeguarding this information and other assets related to national defense from others, whether such items are classified or unclassified.



STATE OF DELAWARE
DEPARTMENT OF TECHNOLOGY AND INFORMATION
801 SILVER LAKE BLVD.
DOVER, DELAWARE 19904

- Coordinating all activities related to this information, such as proper clearance and contracts, with DTI Security.

Protecting Information

We will safeguard information in the possession of DTI by:

- Following DTI policies and procedures for identifying, using, protecting and disclosing this information.
- Properly returning, destroying or otherwise disposing of Information when it is no longer of use.
- Utilizing a "confidential" marking as appropriate for Information classified as "confidential, secret, or top secret", and ensuring that this information retains its labeling when reproducing any portion of it.
- Keeping "confidential, secret, or top secret" Information in protected places (such as secured offices, locked drawers, and password-protected computer systems).
- Taking appropriate precautions when transmitting "confidential, secret, or top secret" Information, either within or outside the DTI. In general, we should ensure that Information is not transmitted through unsecured e-mail, posted onto the Internet or sent to unattended fax machines.
- Complying with any agreements regarding the use and protection of Information.
- Protecting information owned by others. We are responsible for knowing what these agreements require of us.
- Only disclosing Information according to agreed-upon terms, generally as outlined in non-disclosure agreements between the DTI and others, or according to directives from DTI representatives authorized to permit disclosure of Information.
- Informing our Supervisor or Team Leader if we believe that any Information has been or is being used or disclosed improperly.

Question - Because I work for the State, sometimes my family or friends ask me to get information about someone's vehicle tag number. Is this appropriate?

Answer - No. You should never use your job with DTI to obtain information that isn't available to the public.

Releases of and Requests for DTI Information

We will only release DTI Information under the following conditions:

- To employees who have a legitimate, business-related need to know the DTI Information, and who have been advised of the applicable confidentiality requirements.
- To outside parties, whom we expect will treat the information appropriately, (for example, consultants, suppliers, joint venture partners) to whom disclosure has been specifically authorized and who have entered into a written agreement to receive DTI Information under terms and conditions that restrict use and disclosure of the DTI Information.
- In such a way that we are assured of the security of that disclosure. For example, we will avoid sending DTI Information to unattended fax machines or across unsecured e-mail.

We never release DTI Information or information that could be perceived as DTI Information:

- In public Internet forums, such as in chat rooms or on electronic bulletin boards;



STATE OF DELAWARE
DEPARTMENT OF TECHNOLOGY AND INFORMATION
801 SILVER LAKE BLVD.
DOVER, DELAWARE 19904

- **When outside parties, such as the media, or outside attorneys request DTI Information, we will not respond to this request but will inform our Supervisor or Team Leader about the request and take a call back with the requesting party.**

Employee Separation

When leaving the DTI's employment, we must understand our responsibilities to:

- Return any DTI Information in our possession.
- Not take any DTI Information or copies with us.
- Continue safeguarding DTI Information and not disclose it to or use it for the benefit of other parties, including future employers, without DTI's specific prior written authorization.

Reporting Improper Disclosures and Use

We will report any improper disclosures or unauthorized use of DTI Information. Timely reporting of improper disclosures or unauthorized use can assist us in minimizing any damages; including informing certain parties of their duties to protect the DTI Information or taking other measures that protect our interests.

Privacy Principles

DTI has adopted ten "Privacy Principles" which reflect the DTI's commitment to safeguarding customer privacy in an era of rapidly changing communications technology and applications. We should be aware of these Principles and how they impact our jobs.

General Privacy Principles

1. DTI obtains and uses individual customer information for business purposes only.
2. DTI will only disclose information with the permission of the customer or as directed by a court order.
3. DTI complies with all applicable privacy laws and regulations.
4. DTI will safeguard all information and assets related to national defense.
5. DTI strives to ensure the integrity of all data and information entrusted to us.
6. DTI considers privacy implications as new services are planned and introduced and informs customers of the privacy implications of these services.
7. All DTI employees are responsible for safeguarding individual customer communications and information.
8. DTI participates in and supports consumer, government and industry efforts to identify and resolve privacy issues.
9. DTI will properly return, dispose of, or destroy information when it is no longer of use.



STATE OF DELAWARE
DEPARTMENT OF TECHNOLOGY AND INFORMATION
801 SILVER LAKE BLVD.
DOVER, DELAWARE 19904

10. Each DTI employee and contractor is responsible for implementing these Principles.

DEFINITIONS

Information

For purposes of this policy, Information is:

- any and all data/information that has been entrusted to us by other agencies and organizations. Control of the disclosure of this data remains with the agency/organization.
- any and all data/information owned by DTI but not previously released to the public.

DEVELOPMENT AND REVISION HISTORY

Initial version established December 07, 2005.

Revision 1 published March 21, 2007 & July 16, 2007.

Revision 2 dated 11/1/2016 (Logo & formatting)

APPROVAL SIGNATURE BLOCK

On File	
James Collins	
Name & Title: Cabinet Secretary – State Chief Information Officer	Date: January 3, 2006

LISTING OF APPENDICES

Appendix 1 – Employee Acknowledgement Certification

Appendix 2 – Contractor Acknowledgement Certification



STATE OF DELAWARE
DEPARTMENT OF TECHNOLOGY AND INFORMATION
801 SILVER LAKE BLVD.
DOVER, DELAWARE 19904

Appendix 1 – Employee Acknowledgement Certification



State of Delaware
DEPARTMENT OF TECHNOLOGY AND INFORMATION
William Penn Building
801 Silver Lake Boulevard
Dover, Delaware 19904

DTI Employee Confidentiality (Non-Disclosure) and Integrity of Data Agreement

This is to certify that I have read and agree to abide by the guidelines set forth within the DTI Confidentiality (Non-Disclosure) and Integrity of Data Policy. As an employee of the State of Delaware, I fully intend to comply with this policy realizing that I am personally liable for safeguarding information in the possession of the State of Delaware and subject to the corrective action and/or discipline described in this agreement, up to and including dismissal for just cause. If I have any questions about this agreement, I understand that I need to ask my supervisor for clarification.

Name: _____

Signature: _____

Date: _____



STATE OF DELAWARE
DEPARTMENT OF TECHNOLOGY AND INFORMATION
801 SILVER LAKE BLVD.
DOVER, DELAWARE 19904

Appendix 2 – Contractor Acknowledgement Certification



State of Delaware
DEPARTMENT OF TECHNOLOGY AND INFORMATION
William Penn Building
801 Silver Lake Boulevard
Dover, Delaware 19904

Contractor Confidentiality (Non-Disclosure) and Integrity of Data Agreement

The Department of Technology and Information is responsible for safeguarding the confidentiality and integrity of data in State computer files regardless of the source of those data or medium on which they are stored; e.g., electronic data, computer output microfilm (COM), tape, or disk. Computer programs developed to process State Agency data will not be modified without the knowledge and written authorization of the Department of Technology and Information. All data generated from the original source data, shall be the property of the State of Delaware. The control of the disclosure of those data shall be retained by the State of Delaware and the Department of Technology and Information.

I/we, as an employee(s) of _____ or officer of my firm, when performing work for the Department of Technology and Information, understand that I/we act as an extension of DTI and therefore I/we are responsible for safeguarding the States' data and computer files as indicated above. I/we will not use, disclose, or modify State data or State computer files without the written knowledge and written authorization of DTI. Furthermore, I/we understand that I/we are to take all necessary precautions to prevent unauthorized use, disclosure, or modification of State computer files, and I/we should alert my immediate supervisor of any situation which might result in, or create the appearance of, unauthorized use, disclosure or modification of State data. Penalty for unauthorized use, unauthorized modification of data files, or disclosure of any confidential information may mean the loss of my position and benefits, and prosecution under applicable State or Federal law.

This statement applies to the undersigned Contractor and to any others working under the Contractor's direction.

I, the Undersigned, hereby affirm that I have read DTI's Policy On Confidentiality (Non-Disclosure) and Integrity of Data and understood the terms of the above Confidentiality (Non-Disclosure) and Integrity of Data Agreement, and that I/we agree to abide by the terms above.

Contractor Signature _____

Date: _____

Contractor Name: _____



DELAWARE STATE-WIDE INFORMATION TECHNOLOGY AND ARCHITECTURE STANDARDS

Standard ID:	IN-DAT-003
Title:	Data Modeling
Domain:	Information
Discipline:	Modeling
Effective Date:	5/15/2013
Revision no.:	2
Original date:	11/10/2011

I. Authority, Applicability and Purpose

- A. 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.
- B. Applicability** – Applies to all 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 funding, access and continued use of these resources.
- C. Purpose** – Due to the importance of the information managed by the State’s technology solutions, it is necessary to establish common guidelines for Data Modeling. This document provides approaches and best practices for Data Modeling.

II. Scope

- A. State of Delaware** – All communications and computing resources involved with data owned by the State of Delaware
- B. Areas Covered** – This standard covers all data and data modeling technologies whether they were developed in-house or purchased as a complete solution.
- C. Environments** – This standard addresses all environments that contain State of Delaware data, managed by State of Delaware Data Stewards.

III. Process

These standards are adopted by the Department of Technology and Information (DTI), through the Technology and Architecture Standards Committee (TASC), and are applicable to all Information Technology use throughout the State of Delaware. Any questions or comments should be directed to dti_tasc@delaware.gov.



DELAWARE STATE-WIDE INFORMATION TECHNOLOGY AND ARCHITECTURE STANDARDS

- A. **Adoption** – These standards have been adopted by the Department of Technology and Information (DTI) through the Technology and Architecture Standards Committee (TASC) and are applicable to all Information Technology use throughout the state of Delaware.
- B. **Revision** – Technology is constantly evolving; therefore the standards will need to be regularly reviewed. It is the intent of the TASC to review this standard annually. The TASC is open to suggestions and comments from knowledgeable individuals within the state, although we ask that they be channeled through your Information Resource Manager (IRM).
- C. **Contractors** – Contractors or other third parties are required to comply with these standards when proposing technology solutions to DTI or other state entities. Failure to do so could result in rejection by the Delaware Technology Investment Council. For further guidance, or to seek review of a component that is not rated below, contact the TASC at dti_tasc@delaware.gov.
- D. **Implementation responsibility** – DTI and/or the organization's technical staff will implement this standard during the course of normal business activities, including business case review, architectural review, project execution and the design, development, or support of systems.
- E. **Enforcement** – DTI will enforce this standard during the course of normal business activities, including business case and architectural review of proposed projects and during the design, development, or support of systems. This standard may also be enforced by others during the course of their normal business activities, including audits and design reviews.
- F. **Contact us** – Any questions or comments should be directed to dti_tasc@delaware.gov.

IV. Definitions/Declarations

A. Definitions

1. **Attribute** – An attribute is another name for a column in a database schema.
2. **Data Dictionary** – It contains the non-technical (business terminology) definitions of fields.
3. **Data Modeling** – Method used to define and analyze data and the requirements needed to support the business process. The final product will be a true and current representation of the production database. The Data Model is a living document and will change in response to the business. The Data Model also, defines the structure and relationship between the data elements. The three main types of Data Models are Conceptual Data Model, Logical Data Model and Physical Data Model. The preferred sequence for doing Data Modeling is:
 - ✓ Conceptual Data Model
 - ✓ Logical Data Model
 - ✓ Physical Data Model
 - **Conceptual Data Model** – This Data Model describes data requirements from a business point of view without the burden of technical details. Models at this level are about understanding the data requirements of the business.
 - **Logical Data Model** – This Data Model refines the conceptual models by documenting the entities, their attributes and their relationships. These models are technology oriented designs, although they are database-independent.

These standards are adopted by the Department of Technology and Information (DTI), through the Technology and Architecture Standards Committee (TASC), and are applicable to all Information Technology use throughout the State of Delaware. Any questions or comments should be directed to dti_tasc@delaware.gov.



DELAWARE STATE-WIDE INFORMATION TECHNOLOGY AND ARCHITECTURE STANDARDS

- **Physical Data Model** – This Data Model represents the detailed specification of what is physically implemented using specific technology. Physical design considerations include performance, size and growth, availability, recovery from failure, and use of specific technology features.
4. **Metadata** – Data that describes the data. A Metadata record consists of a set of elements that describe the characteristics of an information asset or resource. The more detailed the metadata (especially the business explanations) the better it will be for system implementation, usage and maintenance.

Consistency in the metadata is necessary to keep information organized. Consistent terminology helps communicate metadata, and it helps applications process the metadata. The Categories of Metadata are:

- **Analytical** - Analytic Metadata describes the derivations and display of reporting environments. Primary sources of analytic metadata include OLAP and reporting packages metadata environments.
- **Business** - This category of metadata defines in a business context the information that the data provides. Examples of business metadata are business attribute names, business attribute definitions, business attribute valid values, data quality rules, data models and business rules. Primary sources of business metadata include logical data models and data quality.
- **Navigational** – Navigational metadata describes the data linkage and data movement within the environments. Examples of navigational metadata are derived fields, business hierarchies, source columns & fields, transformations, data quality checkpoints, target columns & fields and source & target locations.
- **Operational** – Operational metadata describes the data integration applications and jobs through statistics giving a full technical view of the environment. Examples of Operational metadata include jobs statistics and data quality check results. Primary sources of Operational metadata include data integration job logs and data quality checks.
- **Structural** - Structural metadata provides the description of data within the IT infrastructure For Example, where the data is located, the names under which it can be accessed, what kinds of data types are being stored, data lineage and data integration within Client's IT environment. Examples for Structural Metadata are:
 - Databases / File groups
 - Tables / Views / Files
 - Keys
 - Indices
 - Columns/fields
 - Source columns/fields
 - Target columns/fields



DELAWARE STATE-WIDE INFORMATION TECHNOLOGY AND ARCHITECTURE STANDARDS

B. Declarations

Data Model Tool must:

- Be able to export the metadata to common format (XML, Text and Microsoft Excel) which would help in repository sharing.
- Have a central repository.
- Be able to search objects (tables, columns, constraints) across the entire model.
- Generate code for multiple types of databases.
- Able to import or export data models created or consumed by other data model tools.
- Provide the ability to re-use objects across models and automatically create linkage for object use.
- Be able to provide impact analysis within and across models.
- Provide the ability to create connections, mappings, and dependencies between models.
- Be able to export data models to a common viewable format where users can see the data model without the Data Model tool.
- Have an entry in the central repository that consists of its model type, name, definition, and applicable characteristics such as a data type for database columns.

Data Model must:

- At minimum, a data model or data dictionary must be submitted to DTI once the application design has been finalized or prior to production implementation of the application. DTI will preserve the data model in a central repository and apply the data model to the enterprise data model based on the fit. The data model or data dictionary must be submitted to DTI in either PowerDesigner, Erwin, Excel in a single worksheet with each item listed below in a separate column. The data model or data dictionary submitted to DTI must include at least the following items:
 - Field Name
 - Description
 - Field Type/Data Type
 - Length



DELAWARE STATE-WIDE INFORMATION TECHNOLOGY AND ARCHITECTURE STANDARDS

- Data dictionaries or data models for vendor solutions must contain information about the core entities, tables or fields that house state-owned business data. To protect the proprietary information of vendor solutions the information submitted only needs to contain the core objects that house state-owned business data. Examples of core state-owned business data are citizen, address, company, etc. The submitted data dictionary or data model does not need to include objects for the data that is not owned by the state. Examples of non-state data are the objects that exist to maintain the database or control the inner workings of the application. To further protect the proprietary information about the database, the data dictionary or data model is not expected to have the actual physical object names.
- The data models/dictionaries that are submitted to DTI via the Architecture Review Board (ARB) process are stored in a secure repository where only the agency who is the steward of the data and the DTI Data Management Team can access the information for purposes of data governance. Contents of the data model or data dictionaries may be shared with the Chief Security Officer for data security purposes. The data models/dictionaries will only be shared with others if approved by the data steward.



DELAWARE STATE-WIDE INFORMATION TECHNOLOGY AND ARCHITECTURE STANDARDS

V. Definition of Ratings

Individual components within a Standard will be rated in one of the following categories. COMPONENT RATING	USAGE NOTES
<ul style="list-style-type: none"> STANDARD – DTI offers internal support and/or has arranged for external vendor support as well (where applicable). DTI believes the component is robust and solidly positioned in its product life cycle. 	<p>These components can be used without explicit DTI approval for both <u>new projects</u> and <u>enhancement</u> of existing systems.</p>
<ul style="list-style-type: none"> DECLINING – Deprecated – DTI considers the component to be a likely candidate to have support discontinued in the near future. A deprecated element is one becoming invalid or obsolete. 	<p>Via the State’s waiver process, these components must be explicitly approved by DTI for <u>all projects</u>. They must not be used for <u>minor enhancement</u> and <u>system maintenance</u> without explicit DTI approval via the State’s waiver process.</p>
<ul style="list-style-type: none"> DISALLOWED – DTI declares the component to be unacceptable for use and will actively intervene to disallow its use when discovered. 	<p>No waiver requests for new solutions with this component rating will be considered.</p>

- A. Applicability of Ratings** – The ratings and usage notes are intended to encourage technology decisions to move toward components that enjoy the full support of DTI. However, acknowledging that mass replacement of lower rated components is not feasible, DTI will allow continued maintenance, enhancement, and possibly limited new development using these components. In making such determinations, DTI may require that the requestor demonstrate that they have adequate support arrangements in place.
- B. Missing Components** – No conclusions should be inferred if a specific component is not listed. Instead, contact the TASC to obtain further information.

These standards are adopted by the Department of Technology and Information (DTI), through the Technology and Architecture Standards Committee (TASC), and are applicable to all Information Technology use throughout the State of Delaware. Any questions or comments should be directed to dti_tasc@delaware.gov.



DELAWARE STATE-WIDE INFORMATION TECHNOLOGY AND ARCHITECTURE STANDARDS

VI. Component Assessments

All implementations of the following components much adhere to the [State of Delaware's standards and policies](#). Of particular note are [State of Delaware Information Security Policy](#), [State of Delaware Data Classification Policy](#) and [Retention Schedules](#).

#	Component	Rating	Comments
<u>1</u>			
a)	Sybase PowerDesigner	Standard	
b)	CA ERwin	Standard	
c)	Visio	Disallowed	Not for use for official ARB submitted data model. Use for other purposes permitted.



CLOUD SECURITY TERMS AND CONDITIONS

FREQUENTLY ASKED QUESTIONS

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.



CLOUD SECURITY TERMS AND CONDITIONS

FREQUENTLY ASKED QUESTIONS

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.



CLOUD SECURITY TERMS AND CONDITIONS
FREQUENTLY ASKED QUESTIONS

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.



CLOUD SECURITY TERMS AND CONDITIONS

FREQUENTLY ASKED QUESTIONS

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 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.



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

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 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 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:	Solomon Adote, Chief Security Officer		
Approval By:	James Collins, Chief Information Officer		
Approved On:	6/18/2018		

2018-06-18



		STATE OF DELAWARE DEPARTMENT OF TECHNOLOGY AND INFORMATION 801 Silver Lake Blvd., Dover, Delaware 19904	
		Doc Ref Number:	SE-CLD-002
Document Type:	Enterprise Policy	Page:	2 of 6
Policy Title:	Terms and Conditions Governing State Data Usage		

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.

		STATE OF DELAWARE DEPARTMENT OF TECHNOLOGY AND INFORMATION 801 Silver Lake Blvd., Dover, Delaware 19904	
		Doc Ref Number: SE-CLD-002	Revision Number: 0
Document Type: Enterprise Policy	Page: 3 of 6		
Policy Title: Terms and Conditions Governing State Data Usage			

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.

2018-06-18

		STATE OF DELAWARE DEPARTMENT OF TECHNOLOGY AND INFORMATION 801 Silver Lake Blvd., Dover, Delaware 19904	
		Doc Ref Number:	SE-CLD-002
Document Type:	Enterprise Policy	Page:	4 of 6
Policy Title:	Terms and Conditions Governing State Data Usage		

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.

2018-06-18

			STATE OF DELAWARE DEPARTMENT OF TECHNOLOGY AND INFORMATION 801 Silver Lake Blvd., Dover, Delaware 19904		
Doc Ref Number:	SE-CLD-002	Revision Number: 0			
Document Type:	Enterprise Policy	Page: 5 of 6			
Policy Title:	Terms and Conditions Governing State Data Usage				

- 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.

2018-06-18



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

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

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)





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

DELAWARE DATA USAGE TERMS AND CONDITIONS AGREEMENT

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

Contract/Agreement #/name _____, Appendix _____

between State of Delaware and _____ dated _____

	Public Data	Non Public Data		DATA USAGE (DU) TERMS
DU1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	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) 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.
DU2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Data Usage	<p>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 <i>Terms & Conditions Governing Cloud Services</i> 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.</p> <p>Only duly authorized PROVIDER staff will have access to the State of Delaware data and may be required to obtain security clearance from the State. No party related to the PROVIDER may retain any data for subsequent use in any transaction that has not been expressly authorized by the State of Delaware.</p>



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

DELAWARE DATA USAGE TERMS AND CONDITIONS AGREEMENT

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

Contract/Agreement #/name _____, Appendix _____

between State of Delaware and _____ dated _____

	Public Data	Non Public Data		DATA USAGE (DU) TERMS
DU3	✓	✓	Termination and Suspension of Service	<p>In the event of termination of the contract, the PROVIDER shall implement an orderly return (in CSV or XML or another mutually agreeable format), or shall guarantee secure disposal of State of Delaware data.</p> <p><i>Suspension of services:</i> During any period of suspension or contract negotiation or disputes, the PROVIDER shall not take any action to intentionally alter, erase, or otherwise render inaccessible any State of Delaware data.</p> <p><i>Termination of any services or agreement in entirety:</i> In the event of termination of any services or agreement in entirety, the PROVIDER shall not take any action to intentionally alter, erase, or otherwise render inaccessible any State of Delaware data for a period of 90 days after the effective date of the termination. Within this 90-day timeframe, vendor will continue to secure and back up State of Delaware data covered under the contract. After such 90-day period, the PROVIDER shall have no obligation to maintain or provide any State of Delaware data. Thereafter, unless legally prohibited, the PROVIDER shall dispose securely of all State of Delaware data in its systems or otherwise in its possession or control, as specified herein.</p> <p>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.</p>
DU4		✓	Data Disposition	<p>At the end of this engagement, PROVIDER will account for and return all State data in all of its forms, disk, CD / DVD, tape, paper, for example. At no time shall any data or processes that either belong to or are intended for the use of State of Delaware or its officers, agents, or employees, be copied, disclosed, or retained by the PROVIDER.</p> <p>When required 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. The PROVIDER shall provide written certificates of destruction to the State of Delaware.</p>



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

DELAWARE DATA USAGE TERMS AND CONDITIONS AGREEMENT

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

Contract/Agreement #/name _____, Appendix _____

between State of Delaware and _____ dated _____

	Public Data	Non Public Data		DATA USAGE (DU) TERMS
DU5		✓	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.
DU6		✓	Breach Notification and Recovery	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 (<i>see</i> DU7, 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) 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 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, 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.



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

DELAWARE DATA USAGE TERMS AND CONDITIONS AGREEMENT

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

Contract/Agreement #/name _____, Appendix _____

between State of Delaware and _____ dated _____

	Public Data	Non Public Data		DATA USAGE (DU) TERMS
DU7		✓	Data Encryption	The PROVIDER shall encrypt all non-public data in transit, regardless of transit mechanism. 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.

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 USE ONLY **DU 1 - DU 3 (Public Data Only)** OR **DU 1 - DU 7 (Non-public Data)**

PROVIDER Name/Address (*print*): _____

PROVIDER Authorizing Official Name (*print*): _____

PROVIDER Authorizing Official Signature: _____ Date: _____



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

Doc Ref Number:	SE-CLD-001	Revision Number: 6
Document Type:	Enterprise Policy	Page: 1 of 7
Policy Title:	Terms and Conditions Governing Cloud Services	

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).		
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 applies 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:	5/15/2013	Expiration Date:	None
POC for Changes:	Solomon Adote, Chief Security Officer		
Approval By:	James Collins, Chief Information Officer		
Approved On:	6/18/2018		

2018-06-18



			STATE OF DELAWARE DEPARTMENT OF TECHNOLOGY AND INFORMATION 801 Silver Lake Blvd. Dover, Delaware 19904		
Doc Ref Number:	SE-CLD-001	Revision Number: 6			
Document Type:	Enterprise Policy	Page: 2 of 7			
Policy Title:	Terms and Conditions Governing Cloud Services				

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

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. All IT-related RFPs, Contracts, etc. must abide by this policy and the related *Terms and Conditions Governing State Data Usage* policy. 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 computing operations and data to a third party.

		STATE OF DELAWARE DEPARTMENT OF TECHNOLOGY AND INFORMATION 801 Silver Lake Blvd. Dover, Delaware 19904	
		Doc Ref Number:	SE-CLD-001
Document Type:	Enterprise Policy	Page:	3 of 7
Policy Title:	Terms and Conditions Governing Cloud Services		

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 data usage and/or cloud services signed agreements, as applicable, approved by DTI. 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*. 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 requiring service provider or other (including but not limited to audit, research, etc.) access to, or use of, state data. 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 agreements are available:

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

			STATE OF DELAWARE DEPARTMENT OF TECHNOLOGY AND INFORMATION 801 Silver Lake Blvd. Dover, Delaware 19904		
Doc Ref Number:	SE-CLD-001	Revision Number: 6			
Document Type:	Enterprise Policy	Page: 4 of 7			
Policy Title:	Terms and Conditions Governing Cloud Services				

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 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.



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

Doc Ref Number:	SE-CLD-001	Revision Number: 6
Document Type:	Enterprise Policy	Page: 5 of 7
Policy Title:	Terms and Conditions Governing Cloud Services	

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 **5/15/2013**

First revision established **8/27/2014**

Second revision establish **11/17/2014**

Third revision established **11/23/2015:**

Removed language regarding the State's inclusion on the insured list.

Fourth revision established **03/01/2016:**

Added Tiered Coverage Schedule. Added PII definition. Adjusted Ponemon value.

Updated link for The Center for Digital Government 2014 study of Cloud Security Procurements.

Fifth revision established **10/10/2016:**

Added language and references to State standards in the Implementation Responsibility section.

Fifth revision established **2/1/2018:**

Added language and references to State standards in the Implementation Responsibility section.

2018-06-18



		STATE OF DELAWARE DEPARTMENT OF TECHNOLOGY AND INFORMATION 801 Silver Lake Blvd. Dover, Delaware 19904	
		Doc Ref Number: SE-CLD-001	Revision Number: 6
Document Type: Enterprise Policy	Page: 6 of 7		
Policy Title: Terms and Conditions Governing Cloud Services			

Sixth revision established **6/18/2018**:

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.

IV. Approval Signature Block

Name & Title: James Collins State Chief Information Officer	Date 10/10/2016

VI. 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.

2018-06-18



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

Doc Ref Number:	SE-CLD-001	Revision Number: 6
Document Type:	Enterprise Policy	Page: 7 of 7
Policy Title:	Terms and Conditions Governing Cloud Services	

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 State Data Usage \(PDF\)](#)

2018-06-18



Delivering Technology that Innovates



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

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>PROVIDER must satisfy Clause CS1-A OR Clauses CS1-B and CS1-C, AND Clause CS4 for all engagements involving non-public data.</p> <p>Clause CS2 is mandatory for all engagements involving non-public data.</p> <p>Clause CS3 is only mandatory for SaaS or PaaS engagements involving non-public data.</p>
CS1-A		✓	<p>Security Standard Compliance Certifications: The PROVIDER shall meet, and provide proof of, one or more of the following Security Certifications.</p> <ul style="list-style-type: none"> • CSA STAR – Cloud Security Alliance – Security, Trust & Assurance Registry (Level Two or higher) • FedRAMP - Federal Risk and Authorization Management Program
CS1-B		✓	<p>Background Checks: 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>Sub-contractor Flowdown: The PROVIDER shall be responsible for ensuring its subcontractors' compliance with the security requirements stated herein.</p>
CS2		✓	<p>Breach Notification and Recovery: 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 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 <i>Terms and Conditions Governing Cloud Services</i> policy) 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 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, 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>



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

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>PROVIDER must satisfy Clause CS1-A OR Clauses CS1-B and CS1-C, AND Clause CS4 for all engagements involving non-public data.</p> <p>Clause CS2 is mandatory for all engagements involving non-public data.</p> <p>Clause CS3 is only mandatory for SaaS or PaaS engagements involving non-public data.</p>
CS3		✓	<p>Data Encryption: The PROVIDER shall encrypt all non-public data in transit, regardless of transit mechanism. 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.</p>
CS4	✓	✓	<p>Notification of Legal Requests: 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.</p>

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

PROVIDER Name/Address (*print*): _____

PROVIDER Authorizing Official Name (*print*): _____

PROVIDER Authorizing Official Signature: _____ Date: _____



DHR049 – Employee Data File

Flat File:**Tab Delimited Flat file format**

Flat File Output		
Output Description and Other Information		
File Name	Delimiter	Retention (Number of Runs to keep)
datadhr049.txt	Tab	2
File Disposition		
Encrypted output will be picked up by the vendor from the SFTP server.		
Header Record		
Field Name	Comments	
SSN	The employee's Social Security Number must be provided in the file;	
POSITION_ID	Employee job record number	
FNAME	Employee first name	
LNAME	Employee last name	
EMAIL	Employee work email address	
ADDRESS1	Employee home address - Street Address 1	
ADDRESS2	Employee home address - Street Address 2	
CITY	Employee home city	
STATE	Employee home state	
ZIP	Employee home zip code (US)	
JOB_TITLE	Employee job title	
EMPLOY_STATUS	The employee's employment status; A or I.	
WORK_STATUS	Employee work status (Full time, part time, temporary, etc.)	
START_DATE	The most recent date the employee started working for the company	
ORIG_START_DATE	If the employee has been hired more than once, the date of the first hire.	
TERMINATION_DATE	If the EMPLOY_STATUS is I (inactive), the date the employee was most recently terminated. If the employee is currently active, leave blank	
BNAME	Employee's current work location name	
BLOCATION	Employees current work location name	
BADDRESS1	Employee's current work location's address	
BADDRESS2	Employee's current work location's address line 2	
BCITY	Employee's current work location's city	
BSTATE	Employee's current work location's state	
BZIP	Employee's current work location's zip code	



DPR063 – YTD Earnings File

Delimited flat file format

Flat File Output		
Output Description and Other Information		
File Name	Delimiter	Retention (Number of Runs to keep)
ytddpr063.txt	Tab	2
File Disposition		
Encrypted output will be picked up by the vendor from the SFTP server.		
Header Record		
Field Name	Comments	
SSN	Employee Social Security Number. No dashes.	
POSITION_ID	Employee job record number	
SALARY_YEAR	The year the overall salary information refers to . This is the primary key for the overall salary data.	
RECORD_DATE	The date this YTD data was tabulated. This is used to prevent overwriting of newer YTD numbers in the event it is necessary to re-import data or import data in an incorrect order.	
PAY_RATE	The employee's pay rate in dollars (no dollar symbol). The pay rate type (period this value is measured in) is specified in the PAY_RATE_TYPE field.	
PAY_RATE_TYPE	The unit of time the PAY_RATE field is specified in. Only one of the 7 string values provided in the example will be accepted as a valid response	
AVG_HOURS_PER_WEEK	The average number of hours the employee works per week.	
BASE	The Gross YTD earnings (in dollars) for the employee for the year specified in the SALARY_YEAR field.	
OVERTIME	The YTD total overtime (in dollars) the employee received for the year specified in the SALARY_YEAR field.	
BONUSES	The YTD total bonuses (in dollars) the employee received for the year specified in the SALARY_YEAR field	
OTHER	The YTD total other pay (in dollars) the employee received for the year specified in the SALARY_YEAR field.	



DPR064 – Earnings per pay period

Tab Delimited flat file format

Flat File Output		
Output Description and Other Information		
File Name	Delimiter	Retention (Number of Runs to keep)
ppdpr064.txt	Tab	2
File Disposition		
Encrypted output will be picked up by the vendor from the SFTP server.		
Header Record		
Field Name	Comments	
SSN	Employee Social Security Number. No dashes.	
POSITION_ID	Employee job record number	
PAY_DATE	Pay date for this record. This is the primary key for pay period data.	
PERIOD_DATE	Pay period ending date for this record. This can be the same as PAY_DATE depending on whether or not your organization tracks both dates	
PP_BASE	The base pay (in dollars)—Gross pay check earnings for the employee for the pay period specified in the PAY_DATE field.	
PP_OVERTIME	The overtime (in dollars) the employee received for the pay period specified in the PAY_DATE field	
PP_BONUSES	The bonuses (in dollars) the employee received for the pay period specified in the PAY_DATE field	
PP_OTHER	The total other pay (in dollars) the employee received for the pay period specified in the PAY_DATE field	

Business Associate Agreement

This Business Associate Agreement (“BA Agreement”) is undertaken pursuant to the parties’ performance of a certain contract (“Contract”) dated as of _____, 20__ by and between the State of Delaware by and through Payroll Human Resources Statewide Technology (“PHRST”), on its own behalf and _____ (“Contractor”).

Therefore, in consideration of the mutual covenants contained herein and for other good and valuable consideration, the parties agree as follows:

1. PURPOSE

- a. Provide three PHRST data extracts to _____ in accordance with the schedule contained in the table in Section 6. of this Agreement. The data contained in the files is to be used exclusively to populate the _____ solution. It is not to be used for any other purpose.
- b. Three historical files will be provided one time for the sole purpose of populating State of Delaware employee history as part of the _____ solution. The timeframes of historical data in the one-time files is in the table in Section 6. of this Agreement

2. DEFINITIONS

- a. State of Delaware Secret: Information that, if divulged, could compromise or endanger the people or assets of the State; such as Public Safety Information. Data that is specifically protected by law (e.g. HIPAA)
- b. Personally Identifiable Information (PII): Information which can be used to identify or contact a person uniquely and reliably, or can be used with other sources to uniquely identify an individual. Examples include but are not limited to full name, full social security number, full date of birth, street address, telephone number, email address, and fingerprints or other biometric data.

3. CLASSIFICATION OF DATA

The data being provided under the Agreement shall be classified “State of Delaware Secret” in accordance with the Department of Technology and Information (“DTI”) Data Classification Policy.

The combination of the data elements in the file, name and SSN, at a minimum, meet the definition of Personally Identifiable Information (PII) as defined in the DTI Data Classification guideline.

4. METHOD OF DATA ACCESS AND TRANSFER

- a. The data files will be generated in pre-defined tab delimited text format during the automated Cybermation schedule. As part of this automated process the files will be encrypted using a previously exchanged PGP key and uploaded to a pre-designated directory and folder(s) on the State of Delaware’s SFTP server. The data files will be decrypted and retrieved by _____ directly from the State of Delaware’s server.
- b. During the initial testing phase, files may be generated manually, rather than through the automated Cybermation schedule. However, test files must be encrypted using a previously exchanged PGP key and uploaded to a pre-designated directory and folder(s) on the State of Delaware’s SFTP server. The test files will be

decrypted and retrieved by _____ directly from the State of Delaware's server.

5. FREQUENCY OF DATA EXCHANGE

This Agreement and the table below address the frequency with which the files are exchanged between PHRST and _____. The third column in the table addresses the timeframe of data contained in the one-time historical data files.

File	Frequency of Exchange on a Continued Basis	One-time Historical Data Timeframes
EMPLOYEE DATA	Weekly	Previous 5 years
YEAR TO DATE PER PAY	Bi-weekly in accordance with State of Delaware payroll cycle	2 Calendar Years
PAY PERIOD DATA	Bi-weekly in accordance with State of Delaware payroll cycle	Previous 52 Weeks

6. RETENTION/LIFECYCLE OF DATA

- a. Data transmitted pursuant to this Agreement shall be retained only as long as required to ensure data files were imported successfully by _____. At that time, files provided by PHRST must be deleted from the _____ server(s), database(s) and any other place where _____ stored the files. In the event any portion of the three files was printed, the hard copies must be shredded within the same timeframe.

7. NON-DISCLOSURE OF DATA

Notwithstanding any other provision of this agreement, PHRST shall be considered the custodian of the data it provides to _____ for the purposes of the Delaware Freedom of Information Act, 29 *Del. C. Ch. 100*. All requests pursuant to FOIA for data subject to this agreement in the possession of _____ must be referred to PHRST. To the extent that _____ modifies the form or content of data disclosed by PHRST, _____ shall be considered the custodian of such information for the purposes of the Delaware Freedom of Information Act, 29 *Del. C. Ch. 100*.

8. DATA BREACH

- a. Any breach in the security or confidentiality of the data being shared shall be reported immediately to PHRST and to the DTI Security Office.

State of Delaware		Vendor Name	
Signature		Signature	
Name	Peter Korolyk	Name	
Title	Deputy Director, Government Support Services	Title	
Date		Date	