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

| | | |
|---|---|---|
| **Doc Ref Number:** | PL-GAS-001 | **Revision Number:** 1 |
| **Document Type:** | Enterprise Policy | **Page:** 1 of 14 |
| **Policy Title:** | Data Management Policy | |

| | | | |
|---|---|---|---|
| **Synopsis:** | The goal of this policy is to improve the integrity, management, storage, transmission, use, availability and security of the State's data. | | |
| **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:** | 10/1/2011 | **Expiration Date:** | None |
| **POC for Changes:** | Greg Lane, Chief Technology Officer | | |
| **Approval By:** | Secretary James Collins, Chief Information Officer | | |
| **Approved On:** | 4/4/2014 | | |

## TABLE OF CONTENTS

**Page**



## I. Policy

**EXECUTIVE SUMMARY**
This policy covers management of data that is owned or acquired by the State of Delaware. There are specific roles and functions for individuals that govern the data management process. Also, this policy primarily addresses structured data only and as a result, it does not provide explicit guidance on the management of documents and files.

**PURPOSE**
The purpose of this policy is to improve the integrity, management, storage, transmission, use, availability and security of the State's data. It also provides instructions and safeguards for managing data stewarded by organizations within the State of Delaware.

## POLICY STATEMENTS

1. All databases (custom or off-the-shelf) must have a current conceptual and physical data model.
2. All data models and associated definitions must be accessible from a central metadata repository. New data models must re-use a subject area, if it exists in the central metadata repository.
3. All acquired data must be documented in appropriate detail including an approved data sharing agreement. (See Data Classification Policy for more details)
4. Data quality applies to business data and data models.
5. Each data element must be associated with a privacy classification and whether its use is subject to limitations.
6. The collection, storage, and access of the State's data are subject to oversight by the State's Data Governance Council. Also, the Council provides guidance and instruction to the individuals, who have been assigned data roles and responsibilities.
7. All transportation schemas must have a documented implementation method such as message, file or table.

## Policy and Standard Compliance

In addition to this policy, State organizations are required to comply with applicable security-related Federal, State, and Local laws, including the following:

- State of Delaware Data Integration Standard
- State of Delaware Reporting and Warehouse Standard
- State of Delaware Metadata and Data Modeling Standard
- State of Delaware Information Security Policy (covers Data Backups, Data Security and Disaster Recovery)
- State of Delaware Data Retention

- Delaware Security Breach Notification (Title 6, Commerce and Trade, Chapter 12B. Computer Security Breaches).
- Health Insurance Portability Accountability Act of 1996 (HIPAA).
- Gramm-Leach Bliley Act (GLB Act), also known as the Financial Modernization Act of 1999.
- The Sarbanes-Oxley Act of 2002 (SOX), also known as the Public Company Accounting Reform and Investor Protection Act of 2002.
- Federal Information Security Management Act of 2002 (FISMA).
- National Security Presidential Directive 38 – National Strategy to Secure Cyberspace.
- National Security Presidential Directive 51 – National Continuity Policy.
- National Security Presidential Directive 54 – Comprehensive National Cyber Security Initiative.
- Federal Preparedness Circular 65 – Continuity of Operations.
- Children's Internet Protection Act (CIPA).
- Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) is a Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education.

## DATA ROLES

**Data Owner State of Delaware Data** – Data in use by State of Delaware organizations, in transit through, or residing within the State's computing infrastructure or in State contracted external hosting facilities are considered State property and owned and controlled by the State of Delaware according to statute.

**Data Steward** – The head of a state organization, or an employee delegated by the head of the organization, with appropriate knowledge and authority to carry out the responsibilities of the Data Steward as defined in this policy. The Data Steward will have a cleared background check.

Acquires, creates, and maintains information about the data within their assigned area of control and reports this to the DTI Data Management Office. All assets must be clearly documented in a single repository and updated at least every six months.

The inventory shall include the type of asset, format, Data Steward, ISO, Data Custodian, data classification, DR criticality level, location, backup information, license information, and a business value.

A current inventory of assets helps to ensure that effective asset protection and risk management takes place, and is required for other business purposes, such as health and safety, insurance or financial asset management reasons.

Data Stewards should be aware that data classification applies to all copies of the data regardless of form or media, especially backups. Full compliance will require a thorough examination of retention periods, numbers of copies, and proliferation of data.

**Sending and Receiving Data:**

The following definitions apply when an organization sends data to or receives data from another entity within the State or outside the State.

- **Sending Data Steward** – The Data Steward (or equivalent if outside the State) of the source data being sent.
- **Receiving Data Steward** – The Data Steward (or equivalent if outside the State) of the data being received.

1. Analyze all computerized data for appropriate data classification at regular intervals as the data/databases are updated or changed. The Data Steward maintains a working knowledge of the data under their care and aligns the organization's data classification selections with it.
2. Establishes Data Privacy rules as appropriate.
3. Notifies the DTI Data Management Office in advance of any planned changes in the type of data (new data base, new interface, decommissioned or archived databases, for example) in their area of control.

4. Evaluates and approves requests for data transfers to or from another party. These parties may be State organizations or external partners or hosting providers.

5. The Sending Data Steward is to clearly communicate to the Receiving Data Steward the classification of the data to be transferred,

6. Obtains written or otherwise binding documentation whereby the Receiving Data Steward agrees to treat the transmitted data according to the classification as declared by the Sending Data Steward. (Upon transfer of the data, the Receiving Data Steward bears the responsibility for properly protecting that data.)

7. The Sending Data Steward must take into consideration any issues involved in releasing this data outside of the State and, if deemed appropriate, may increase the data classification rating.

8. Ensures appropriate data retention periods according to State and Federal laws and organization policies.

9. Ensures appropriate backups are taken and tested.

10. Restricts computer applications and data access to authorized persons in coordination with the Data Custodian.

11. Attends classes or takes Computer Based Training in accordance with DTI Data Management Office requirements.

12. Ensures, in conjunction with the organization's Information Security Officer (ISO) and the Data Custodian, the implementation and enforcement of appropriate security control procedures to protect the data against unauthorized modification, destruction, or disclosure.

13. Reviews and recommends changes to the handling of data with respect to integrity, security and privacy.

14. Authorizes appropriate data access to Data Users. This process is coordinated through the Information Security Officer (ISO) and the use of the Statewide Security Request System

    - The data classification hierarchy is implemented and adhered to for the types of data processed for their particular business unit/department. See Data Classification Policy.

    - Data is categorized for the area that the business unit/department manager (Data Steward) has been designated as a Steward using classifications defined in the Data Classification Policy.

15. Ensures appropriate continuity of operations planning efforts exists including a defined State organization liaison to work with authorities.

16. Ensures the planning and testing of COOP efforts at least annually with the appropriate State of Delaware BC/DR criticality recovery requirements.

17. Categorizes data application systems according to a criticality scale defined by the business unit/department according to the Disaster Recovery/Continuity of Operations Plan (DR/COOP) criticality levels.

18. Ensures that user and system administrator access to data is on a need-to-know basis rather than by rank, position, or affiliation-based. Personnel must undergo appropriate screening relevant to the classification of the data.

19. Adheres to appropriate Federal and State privacy regulations in the classification of data.

20. Checks are periodically made to ensure that data classifications are appropriate and that safeguards remain valid and operative.

21. Reports and coordinates all requests for deviations or clarifications to any Data Policy with the DTI Data Management Office.

22. Documents and coordinates such with the DTI Data Management Office all delegated responsibilities, including the submission of security access requests to specific Data Custodians as needed.

**Data Custodian**

A Data Custodian is an IT individual who works with the Data Steward to oversee and implement the necessary safeguards to protect the information assets in compliance with the policies, rules, and regulations governing the types and classification of the data. Data Custodians must remain current with applicable certifications, available training and data management best practices.

1. Provides information technology services that are consistent with the instructions of the Data Steward, including information security measures such as data access controls. Using physical and logical access control and audit/monitoring systems, the Data Custodians must protection of the data in their possession from unauthorized access, alteration, destruction, or usage. Data Custodians are individuals who have the administrative rights to access, modify, delete, and/or utilize data as authorized in writing by the Data Steward.
2. Oversees the operation of information systems to ensure the confidentiality, integrity, and availability of data in their careis maintained as directed by Federal and State law, State Policies and Standards and organization management.
3. Responsible for viewing/amending/updating the information metadata.
4. Reports any violation of this policy to the Data Steward, the DTI Data Management Team, The DTI IT Security Team, DTI Chief Security Officer, and their organizations's supervisor/manager. This includes violations by employees, casual seasonal employees, temporary personnel, contractors, vendors and all State third party associates.

5. All State of Delaware data must have a designated Data Custodian who is responsible for implements and maintains requisite security controls prescribed in relevant policies, procedures, guidelines, and standards.

6. Approves security access requests as needed at the appointment of the Data Steward.

7. Data Custodians must ensures that the information is used only for the purposes specifically approved by the Data Steward. Data Custodians must also comply with all security measures defined by the Data Steward and the DTI Chief Security Office and Data Management Team. Additionally, Data Custodians must refrain from disclosing data in their possession (unless it is designated as State of Delaware Public) without first obtaining permission from the Data Steward.

8. Reports to their manager, ISO, IRM, DTI Chief Security Officer and DTI Data Management Office all situations where they believe an information security vulnerability or violation may exist. Local management must also provide Data Custodians with sufficient time and materials to receive periodic information security training.

**Data User**

Data Users are authorized users who access information assets and use the State's data. This also includes the use of data on an individual's State issued computer and any related files shares. A Data User can be an employee, casual seasonal employee, temporary personnel, contractor, vendors, outsourcers, and/or all others who have access to the State's data.

**Database Administrator**

A database administrator (DBA) is a person responsible for monitoring, coordinating and managing the selection, physical design, development, security, operation, processing, performance and maintenance of relational and/or other databases, data storage and retrieval systems.

**Data Administrator**

A Data Administrator is an IT person responsible for analyzing, organizing and managing data as an asset and promoting data-sharing throughout systems statewide. They maintain data dictionaries, data integration systems, reporting/business intelligence, and data warehousing. They work with the business user and technical staff to improve the management and usage of data statewide.

**IMPLEMENTATION RESPONSIBILITY**

DTI and/or the organization's technical staff will implement this policy during the course of normal business activities, including business case review, architectural review, project execution and the design, development, or support of systems.

**ENFORCEMENT and WAIVER**

DTI will enforce this policy 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 policy may also be enforced by others during the course of their normal business activities, including audits and design reviews.

If there is ambiguity or confusion regarding any part of this policy, contact the point of contact defined in the header of this policy.

## II. Definitions

1. **Acquired Data –** It is data that originates outside of the application. It is a way to describe data that crosses an application, system or managerial border.

2. **Business Intelligence –** Is a set of concepts and methodologies to improve business decision making typically through use of reporting tools accessing data marts, operational data stores, and data warehouses.

3. **Data** – Referred to as a qualitative or quantitative attributes of a variable or set of variables and contains factual information used as a basis for reasoning, discussion, or calculation.

4. **Data Cleansing** – The process of detecting data errors and correcting those errors so that the data quality is at an acceptable level in order for the organization to properly and effectively operate their business and make valid business decisions.

5. **Data Dictionary -** It contains the non-technical definitions of fields.

6. **Data Governance -** boards or committees create and enforce policies and procedures for data usage and management.

7. **Data Integration -** acquires data from one or more sources and transforms as needed by business or functional or technical specifications.

8. **Data Integrity –** Data Integrity is assurance that information is authentic and complete. Ensuring that information can be relied upon to be sufficiently accurate for its purpose. The term 'integrity' is used frequently when considering Information Security as it represents one (1) of the primary indicators of security (or lack of it). The integrity of data is not only whether the data is 'correct', but whether it can be trusted and relied upon. For example, making copies (e.g., by emailing a file) of a sensitive document threatens both confidentiality and the integrity of the information.

9. **Data Management –** encompasses techniques for data analysis, data design, data quality, integration, and governance. It includes all the practices necessary to manage data as a critical enterprise asset.

10. **Data Mart –** Is a set of data tailored to a subject area to support specific analytical requirements of a business unit or a function.

11. **Data Modeling** – Method used to define and analyze data and its requirements needed to support the business process and the final product will be implemented in the 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 main three types of Data Models are Conceptual Data Model, Logical Data Model and Physical Data Model.

- **Conceptual Data Model** – This Data Model describe data requirements from business point of view without the burden of technical details. Models at this level are about understanding the required set of data stores.
- **Logical Data Model** – This Data Model refine conceptual models by documenting entities, their attributes and their relationships. These models are technology oriented designs, although they are platform-independent.
- **Physical Data Model** – This Data Model represent 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.

12. **Data Privacy -** Inappropriate use of data. Based on assigned data classification of the data, the level of data privacy and confidentiality is set. Data collected will be handled in accordance with all appropriate methods to ensure privacy, confidentiality, and compliance with applicable Federal, State, and Local Laws, and State's policies, standards, and procedures. For further information, review the Delaware Information Security Policy, Data Classification Policy, and the Acceptable Use Policy.

13. **Data Quality -** includes techniques for data cleansing, data standardization, verification, profiling, monitoring, matching, and enrichment.

14. **Data Redundancy** – Same Data being stored on two or more systems or tables or databases. The redundancy may create data anomalies among the reporting or analytics as each system / databases updates, unless managed appropriately as these anomalies will lead to inconsistent reporting.

15. **Data Retention –** Data must be retained at the State Organization/School District/Quasi State Organization based upon the organization's retention schedule. The general retention schedules are available at http://archives.delaware.gov/govsvcs/general_records_retention_schedules/index.shtm For State Organization/School District/Quasi State Organization specific

retention schedules, contact that specific entity to arrange review of their data retention schedules.

16. **Data Security -** Unauthorized access to or collection, processing, modification, storage, retention, destruction, or disclosure of business sensitive information, personal information and sensitive personal information.

17. **Data Warehouse –** Typically a decision support system that integrates data from multiple sources into a central location. The integrated data is cleansed, standardized, transformed, and structured to more easily analyze the data for a variety of purposes that may cross multiple business areas. A data warehouse is typically used for historical analysis and, therefore, will contain many years worth of data.

18. **Master Data** – Defined as the commonly shared data elements used by the key business areas of an organization. Master data are the critical areas of a business and fall generally into four groupings: parties, products, financial information, and location data. Further categorizations within those groupings are called subject areas, domain areas, or entity types. Examples of parties are constituents, employees, and other government organizations. Examples of products are licenses, equipment, and services. Examples of financial information are contracts, payroll, fees, and taxes. Finally, examples of places are addresses, office locations and geographic divisions.

19. **Metadata** – Data that describes the data, and is useful to operate, and maintain. A Metadata record consists of a set of elements that describe different characteristics of an information asset or resource.

20. **Operational Data Store –** A repository of transactional data. – Also, an ODS is a subject-oriented, integrated, volatile, real time (or near-real time) and detail operational information. An ODS is designed for performance and numerous queries on small amounts of data such as getting account balance or status of an order.

21. **Operational Warehouse** – A collection of data from multiple sources that is stored centrally for improved data analysis and reporting. The integrated data is cleansed, standardized, transformed, and structured to more easily analyze the data. The data

is typically updated in near real-time and is only stored for a short time period. It may then be moved to the data warehouse for historical analysis.

22. **Reference Data -** Defined as a pre-defined list of domain values, standardized terms, and unique identifiers used across an organization. The domain values are typically coded values used in lookup lists. Reference data provides consistency of the data, its usage, and meaning across all systems.

23. **Transportation Schema –** It is a structure that makes the movement of data easier or convenient. The structure does not have to resemble the source structure or target structure and the structure tends to be for 'transient data' not 'persistent data'.

## III. Development and Revision History

Initial version established on 10/1/2011.

First revision established on 4/4/2014

## IV. Approval Signature Block

| | |
|---|---|
| **Name & Title:**<br>Cabinet Secretary -<br>State Chief Information Officer | **Date** |