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

| | | |
|---|---|---|
| **Doc Ref Number:** | IN-DataClass-001 | **Revision Number:** 2 |
| **Document Type:** | Enterprise Policy | **Page:** 1 of 9 |
| **Policy Title:** | **Data Classification Policy** | |

| | | | |
|---|---|---|---|
| **Synopsis:** | The goal of this policy is to enhance the State's ability to protect data and information through data classification. | | |
| **Authority:** | Title 29, Delaware Code, §9004C - General powers, duties and functions of DTI "2) Implement statewide and interagency technology solutions, policies, standards and guidelines as recommended by the Technology Investment Council on an ongoing basis and the CIO, including, but not limited to, statewide technology and information architectures, statewide information technology plans, development life cycle methodologies, transport facilities, communications protocols, data and information sharing considerations, the technique of obtaining grants involving the State's informational resources and the overall coordination of information technology efforts undertaken by and between the various State agencies;" | | |
| **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:** | 03/01/2006 | **Expiration Date:** | None |
| **POC for Changes:** | Elayne Starkey - Chief Security Officer | | |
| **Approval By:** | Secretary Jim Sills, Chief Information Officer | | |
| **Approved On:** | 4/4/2014 | | |

## TABLE OF CONTENTS



## I. Policy

### EXECUTIVE SUMMARY

This policy requires Data Stewards to classify all of the data used by their organization. It describes the roles and responsibilities of a Data Steward, the four types of data classifications and the minimum set of classifications. Generally, it lays the groundwork for the proper classification and handling of data used by the State. Further insight into this policy may be obtained through the organization's IRM (Information Resource Manager) or the DTI CES (Customer Engagement Specialist) assigned to the organization.

This policy does not limit or redefine FOIA (Freedom of Information Act) laws or regulations. In case of any conflict, the law shall prevail.

### PURPOSE

This policy provides instruction for State organizations to better handle, secure, access, and use data. Sound business judgment and practices must be applied, and the State must comply with applicable Federal, State and Local laws and regulations, as well as any agency-specific guidelines then in effect. Examples of such are HIPAA and Gramm-Leach-Bliley (GLB), Federal Information Security Management Act

(FSMA), Privacy Act, PCI DSS, Federal Tax Data Safeguards (IRS Publication 1075), etc.[1] This policy will be reviewed and revised periodically. However, the State is obligated to comply with new laws or regulations coming into effect between revisions.

This policy is expected to be referenced by other State policies and standards that will further define the implications of the data classification. As such, the actual data classification designations will have far-reaching effects on various aspects of Information Technology throughout the State.

The National Institute of Standards and Technology (NIST) has drafted a comprehensive approach to data classification and the risks that are associated with different levels of data classification. Specifically, it addresses the integrity and availability of data as well as confidentiality, which is the focal point of this policy. Over time, this policy will be influenced by NIST standards. The reading of the NIST draft 'Guide for Mapping Types of Information and Information Systems to Security Categories – SP 800-60' is encouraged.

## DATA OWNER and DATA STEWARD

**Consult the Data Management Policy for these definitions**

## DATA CLASSIFICATIONS

The Data Steward is responsible for classifying all data under the organization's control into one of the following classes.

**State of Delaware Public** – Information available to the general public; eligible for public access.

**State of Delaware Confidential** – Information covered by one or more laws. The disclosure of this information could endanger citizens, corporations,

[1] HIPAA is the United States Health Insurance Portability and Accountability Act of 1996, PL 104-191. The Financial Modernization Act of 1999, also known as the "Gramm-Leach-Bliley Act" or GLB Act.

business partners and others. The types of information might be covered under non-disclosure agreements; or safeguarded by a general reference in law or best practices.

**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).

**State of Delaware Top Secret –** Information that could, if divulged, expose the State's citizens and assets to great risk.

The classifications stated herein are to be considered as **minimum classification levels** for the data. The Data Steward may not specify a lower classification.

These classifications are in line with the Federal Government data classifications found in Executive Order 13292. The exception is that the Federal Government has no consistent designation for Public data. In some cases, the term Unclassified is used to denote non-Confidential, non-Secret and non-Top Secret data. For clarity, the State of Delaware chose to use the term State of Delaware Public data rather than non-Confidential, non-Secret and non-Top Secret data. One core value that distinguishes a classification from another is the Risk of Harm. What is the risk that harm can result from the inappropriate disclosure or use of this information?

**Minimum Classifications**

The following data elements are examples of data that must be classified no lower than as shown regardless of the context in which they are represented.

| Data Element | Classification |
|---|---|
| Social Security Number | State of Delaware Confidential |
| Employee ID | State of Delaware Confidential |
| Bank Account Number | State of Delaware Confidential |
| Credit Card Number | State of Delaware |

| | |
|---|---|
| | Confidential |
| Mother's Name | State of Delaware Confidential |
| Father's Name | State of Delaware Confidential |
| Place of Birth | State of Delaware Confidential |

The statewide policies and standards pertaining to data protection can be found at the DTI website. Local guidelines are established by the state organization itself. For a complete list, please contact the organization's Information Resource Manager (IRM).

**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.

If any dispute arises regarding the minimum classifications of data contained in this policy, the waiver process will resolve the issue. If any disputes or questions arise from the Data Classification Guidelines, the data steward can present them to the State's Chief Security Officer for help in determining the proper classification.

**Failure to Comply**
Failure to comply with the policy is a serious matter whether through intentional act or negligence and may be grounds for discipline up to and including dismissal based on the Just Cause standard set forth by Merit Rules, or collective bargaining agreement, whichever is applicable to the subject employee. Exempt employees shall be subject to appropriate discipline without recourse, except as provided by law. While DTI has no authority to discipline employees of other agencies/organizations in

the Executive, Legislative, or Judicial branches of government, it will take the appropriate steps to ensure any misconduct is appropriately addressed.

## II. Definitions

**Data –** Distinct pieces of information in digital (computer-readable) format that can be stored, read, manipulated, or transmitted.

**Dataset** – A Dataset is a collection of data elements in a structure that is its own unique entity and usually associated with a name. Examples include files, databases, etc. A Dataset's classification must be at least as high as that of the highest data element contained therein (classification by association). This also applies to multiple Datasets when stored or transmitted together; the classification of the combined Datasets must be at least as high as that of the highest Dataset in the combination.

**Data Owner** –
Consult the Data Management Policy for this definition

**Data Steward** –

Consult the Data Management Policy for this definition

**Data User** -
Consult the Data Management Policy for this definition

**Document vs. Data** - A **document** merges data and format together to assist the reader in understanding the context of the data. A document is usually a set of words that form sentences that can be understood in their form and context. **Data** usually does not contain syntax or grammar, leaving the letters and numbers without association beyond the database schema or data dictionary. This policy covers all data, (for example, data entry, document scanning, voice or video recording), regardless of its source, destination or storage medium.

**Federal Tax Information (FTI)** – The IRS defines federal tax information, which is subject to safeguarding requirements, as any tax return-derived information received from the IRS. This includes but is not limited to address information, social security numbers, federal tax filing status, payment source.

**Information Resource Manager (IRM)** – Those assigned the responsibility to act as the primary points of contact for appropriate communications between DTI and the organization.

**Information Security Officer (ISO)** – An individual in the organization designated by the organization's management who is responsible for ensuring the security of the organization's information.

**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.

**Personal Health Information (PHI)** – Individually identifiable health information that is maintained or transmitted in any form or medium.

**Personal Financial Information (PFI)** – Individually identifiable financial information that is maintained or transmitted in any form or medium.

**Privileged Account** – This type of account allows individuals to perform administrator or super-user functions within an IT system or environment.

## III. Development and Revision History

Initial version established **03/01/2006**

Second version established **2/28/2008**

Minor revision established **3/22/2011**

Minor revision established **4/4/2014**

## IV. Approval Signature Block

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

## V. Other Documents

A Data Classification Guideline has been published and it is hereby noted. If there is any conflict between the Data Classification Guideline and this policy, the policy shall prevail. To obtain more information, please reference the Enterprise Standards and Policies and notably the Delaware Information Security Policy for further insight.