DELAWARE STATE-WIDE INFORMATION

TECHNOLOGY AND ARCHITECTURE STANDARDS

Guideline ID:	GU-DataClass-001
Title:	**Data Classification Guideline**
Revision Number:	2
Domain:	Information
Discipline:	Data Classification
Effective:	03/01/2006
Reviewed:	02/26/2024
Approved By:	Chief Information Officer
Sponsor:	Chief Technology Officer

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. The Department of Technology and Information (DTI) is an Executive Branch Agency and has no authority over the customers in Legislative and Judicial Branches, as well as Local Education Agencies, and other Federal and Local Government entities that use these resources. However, all users, including these entities, must agree to abide by all policies, standards promulgated by DTI as a condition of funding, access and continued use of these resources.

C. Purpose: This document is a guideline to the Data Classification Policy, and it is noted in that document. If there is any conflict between the Data Classification Policy and this document, the Data Classification Policy shall prevail. This document will be updated from time to time with additional declarations of data classification or examples of context sensitive guidelines.

II. Scope

A. Areas Covered: All locations such as on-premise, cloud, vendor-hosted, etc.

B. Environments: All environments with State of Delaware data.

III. Process

A. <u>**Adoption:**</u> These guidelines have been adopted by the DTI through the Technology and Architecture Standards Committee (TASC) and are applicable to all Information Technology use throughout the State of Delaware.

B. <u>**Revision:**</u> Technology is constantly evolving; therefore, the guidelines will need to be regularly reviewed. It is the intent of the TASC to review this guideline 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. <u>**Contractors:**</u> Contractors or other third parties are required to comply with these guidelines when proposing technology solutions to DTI or other State entities. Failure to do so could result in rejection of the proposed technology solution. For further guidance, or to seek review of a component that is not rated below, contact the TASC at dti_tasc@delaware.gov.

D. <u>**Implementation responsibility:**</u> DTI and/or the organization's technical staff will implement these guidelines during the course of normal business activities, including business case review, architectural review, project execution and the design, development, or support of systems.

E. <u>**Enforcement:**</u> DTI will enforce these guidelines 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. These guidelines may also be enforced by others during the course of their normal business activities, including audits and design reviews.

F. <u>**Contact us:**</u> Any questions or comments should be directed to dti_tasc@delaware.gov.

IV. Definitions/Declarations

A. <u>**Declarations**</u>

1. All data classifications must adhere to all the rules and regulations of the appropriate governing bodies such as federal, state, and local governments.

2. State organizations must consider the characteristics of the data elements individually. If the data elements are part of a dataset, then the dataset must be classified no lower than the highest classification of any data element.

3. State organizations must consider the characteristics of the data elements in context. The combination of multiple data elements may, in some situations, result in the combined rating being higher than the highest individual rating.

V. Guidelines

A. **State of Delaware Public** – Data that should be classified as public.

Context Sensitive Types of Information	Examples
Agency Name	Dept of Transportation
Hours of Operation	8 AM to 4:30 PM Monday thru Friday
Office Address	123 Main St Anywhere DE
Office Phone Number	302 555 1234
Types of Reports or Collections of Data	
Audit Reports	Excluding Data that provides knowledge that could be used to injure the State, its Citizens or Business Partners.
Agency Policies	Excluding Data that provides knowledge that could be used to injure the State, its Citizens or Business Partners.
Computer Usage History	Excluding Data that provides knowledge that could be used to injure the State, its Citizens or Business Partners.
Expenditure Data	Excluding Data that is covered by Agreement or Contract, for example Non-Disclosure Agreements
Revenue Data	Excluding Data that is not Public because of law.

B. **State of Delaware Confidential** – Data that should be minimally classified as confidential.

1. Elections record
2. Payroll record
3. Personnel record
4. Personal Income Tax record

5. Defendant, or Witness PII record

6. Financial institution information on one person or business

7. Facts on Disaster Recovery Plans

8. Information covered by Non-Disclosure Agreements

9. Information about an investigation or audit

10. Passwords giving access to data. (For example, a citizen's password granting access only to their confidential record)

11. Technical documentation, i.e., detailed network port/ip diagrams and system architectures for systems containing public, confidential, or secret data.

C. **State of Delaware Secret** – Data that should be classified as secret.

1. Data that is specifically protected by law: for example, HIPAA, GLB, FERPA or CJIS

2. Expunged court cases

3. Sealed court cases or child support information

4. Information regarding people's health

D. **State of Delaware Top Secret** – Data that should be classified as top secret.

1. Information about investigations, undercover officers, police raids, etc.

2. Information about State or National Homeland Security

VI. Development and Revision History

Date	Revision
3/1/2006	Rev 0 - Initial version
02/26/2024	Rev 1 – Major update with new formatting and removal of specific PII, PFI, and PHI context. The volume of records no longer impacts the classification.