# Data Classification Guidelines

## Document No: CDO-004
## Issued by: Chief Data Officer

## 1.0 Purpose

The purpose of the Data Classification Guidelines is to establish common guidelines for data classification based on its sensitivity to ensure consistent practices across State of Hawaii agencies. Adherence to these guidelines enhances data security, ensures data privacy protection, and facilitates compliance with regulatory requirements throughout the state.

Data Classification refers to the assignment of a level of sensitivity to data that results in the specification of controls for each tier of classification. Tiers are assigned according to predefined categories as data are created, amended, enhanced, stored or transmitted.[1]

The Data Classification Guidelines apply to all data sets handled by state agencies. This includes, but is not limited to systems in the cloud, on premises, and on local drives.

## 2.0 Authority

Section 27-44, Hawaii Revised Statutes (HRS),[2] provides the Chief Data Officer with the authority to develop, implement, and manage statewide data policies, procedures, and standards, and establishes a Data Task Force to support the Chief Data Officer in developing, implementing, and managing the State's data policies, procedures, and standards.

## 3.0 Scope

The Data Classification Guidelines apply to all State agencies.

The Data Classification Guidelines provide high level guidelines on data classification. Each agency shall develop additional policies and guidelines as necessary according to relevant federal and state laws and regulations, both at data set level and at the individual field level, to ensure compliance in its operations. Where a conflict exists between the Data Classification Guidelines and an agency's policy, the more restrictive policy will take precedence.

[1] Information Systems Audit and Control Association (ISACA) Glossary. https://www.isaca.org/resources/glossary
[2] HRS §27-44. https://www.capitol.hawaii.gov/hrscurrent/Vol01_Ch0001-0042F/HRS0027/HRS_0027-0044.htm

## 4.0. Information Statement

Data classification is conducted at the field or field value level, as required by relevant laws and regulations. This means that each piece of data is assessed and categorized based on its sensitivity. If a dataset is fully open to the public, detailed classification may not be necessary.

Data classification helps protect sensitive information while promoting transparency. By classifying data properly, agencies safeguard individual privacy and ensure responsible data management. Ultimately, this practice builds public trust and supports the effective use of data in line with the State's open data efforts.

Each agency is responsible for classifying its data into one of the recommended tiers as follows:

- **Public:** Public refers to data intended for unrestricted access and dissemination.
- **Internal:** Internal refers to data used for an agency only. It may be shared between agencies within the State under the terms of a written memorandum of agreement or contract.
- **Protected:** Protected refers to data that, while not as sensitive as classified data, requires protection from unauthorized access or disclosure to prevent potential harm or loss.
- **Classified:** Classified refers to highly confidential data that requires restricted access and strong protection.

When sharing data between different agencies within the State, a data sharing agreement is required unless it is public data. Data must be protected according to the data handling requirements as specified in table 1 below.

Table 1. Data Handling Requirements

| Tiers | Sensitivity | Storage | Transmission | Access |
|---|---|---|---|---|
| Public | Insignificant | Standard storage | Standard transmission methods (e.g., HTTP) | Openly accessible |
| Internal | Low/Moderate | Access-controlled storage | Secure transmission methods (e.g., VPN, SFTP) | Authentication and authorization required |
| Protected | Moderate/High | Encrypted at rest and in transit | Secure methods (e.g., VPN, SFTP, TLS) with additional encryption layers | Role-based access control with granular permissions and multi-factor authentication |

| | | | | |
|---|---|---|---|---|
| Classified | High | High-assurance security storage (e.g., hardware security modules) | Strongest secure methods (e.g., dedicated encrypted channels, zero-knowledge proofs) | Access limited to authorized personnel only |

## 5.0. Compliance

The Data Classification Guidelines shall take effect upon publication. Compliance is strongly recommended.

## 6.0 Contact Information

Submit all inquiries and requests for future enhancements to the Chief Data Office at data@hawaii.gov.

Additional data and AI related standards and guidelines documents can be found at data.hawaii.gov.

## 7.0 Key Terms

All terms shall have the meanings found in the Data and AI Glossary (under Glossaries on https://data.hawaii.gov/).

- **Data Asset**: According to NIST definition, Data Asset refers to any entity that is comprised of data. For example, a database is a data asset that is comprised of data records. A data asset may be a system or application output file, database, document, or web page.[3]
- **Sensitivity**: Sensitivity refers to the potential harm that could result from unauthorized access, disclosure, modification, or destruction of data.[4]
- **Transmission**: Transmission refers to the movement of data across a communication channel.[5]

## 8.0 Revision History

| Date | Description of Change |
|---|---|
| December 16,2024 | Approved by the State Data Task Force |
| February 11, 2025 | Published |

[3] National Institute of Standards and Technology Glossary. https://csrc.nist.gov/glossary/term/data_asset
[4] National Institute of Standards and Technology Glossary. https://csrc.nist.gov/glossary/term/sensitive
[5] National Institute of Standards and Technology Glossary. https://csrc.nist.gov/glossary/term/transmission

## 9. Related Documents

[1] General Services Administration, Protecting PII - Privacy Act, U.S. https://www.gsa.gov/reference/gsa-privacy-program/rules-and-policies-protecting-pii-privacy-act

[2] Office of Information Policy U.S. Department of Justice. Freedom of Information Act (FOIA), 5 U.S.C. § 552. https://www.justice.gov/oip/freedom-information-act-5-usc-552

[3] National Institute of Standards and Technology (NIST) Special Publication 800-30 (Rev. 1): Risk Management Framework for Information Systems and Organizations. https://www.nist.gov/privacy-framework/nist-sp-800-30

[4] Privacy Act of 1974, 5 U.S.C. 552a https://www.govinfo.gov/content/pkg/USCODE-2018-title5/pdf/USCODE-2018-title5-partI-chap5-subchapII-sec552a.pdf

[5] Children's Online Privacy Protection Act (COPPA) — PII of children under 13. https://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title15-section6501&edition=prelim

[6] Payment Card Industry Data Security Standard (PCI DSS) v 3.2. https://www.pcisecuritystandards.org/document_library/?category=pcidss&document=pci_dss

[7] Nacha Operating Rules. ACH payment. https://www.nacha.org/newrules

[8] Internal Revenue Service Tax Information Security Guidelines for Federal, State and Local Agencies. https://www.irs.gov/privacy-disclosure/safeguards-program

[9] Health Insurance Portability and Accountability Act of 1996 (HIPAA). https://aspe.hhs.gov/reports/health-insurance-portability-accountability-act-1996

[10] Privacy of Medicaid Data Records, the Code of Federal Regulations (at 45 CFR 95.621). https://www.hhs.gov/guidance/document/privacy-medicaid-data-records

[11] Medicaid Information Technology Architecture (MITA) 3.0. https://www.medicaid.gov/medicaid/data-systems/medicaid-information-technology-architecture/medicaid-information-technology-architecture-framework/index.html

[12] Criminal Justice Information Services (CJIS) Security Policy. https://le.fbi.gov/cjis-division/cjis-security-policy-resource-center

[13] Family Educational Rights and Privacy Act (FERPA). https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

[14] Hawaii State DOT, Motor Vehicle Driver's License and related offices. https://hidot.hawaii.gov/highways/files/2018/02/Privacy_Policy_Stmnt_mvso-12-12-2017.pdf

[15] Driver's Privacy Protection Act (DPPA) H.R.3365 — 103rd Congress (1993-1994). https://www.law.cornell.edu/uscode/text/18/2721

[16] Critical Infrastructure Information, 6 USC CHAPTER 1, SUBCHAPTER XVIII, Part B https://www.cisa.gov/sites/default/files/publications/CII-Act.pdf

[17] International Organization for Standardization (ISO) 27001: Information security management systems. https://www.iso.org/standard/27001: https://www.iso.org/standard/27001