



## DATA TASK FORCE MEETING

December 16, 2024, 3:00 p.m.

1151 Punchbowl St., Conference Room 410, Honolulu, Hawaii 96813

This meeting will be conducted remotely. The public may participate via interactive conference technology (ICT) or in person at the physical meeting location indicated above.

[Click here to join the meeting](#) Meeting ID: 220 414 301 575; Passcode: yy6j47

**Or call in (audio only)**

[+1 808-829-4853](tel:+18088294853), [615153385#](tel:+1615153385) Phone conference ID: 615 153 385#

### AGENDA

- I. Call to Order, Roll Call
- II. Public Testimony  
Individuals may provide oral testimony at the meeting or submit written testimony in advance on any agenda item. Written testimony may be sent via email to [ets@hawaii.gov](mailto:ets@hawaii.gov), Subject: *Data Task Force Testimony*; or delivered to Data Task Force, 1151 Punchbowl Street, B-10, Honolulu, Hawaii 96813. Oral testimony will be limited to three (3) minutes per person or organization.
- III. Review and Approval of the September 16, 2024, Meeting Minutes
- IV. Approve Data/AI Policies
  - Data Privacy Guidelines
  - Data Catalog Guidelines
  - Data Classification Guidelines
  - Data Retention Guidelines
  - Open Data Guidelines
  - GenAI Assistant Technologies Usage Guidelines
- V. 2024 Deliverables Summary
  - Overview with accomplishments summary
  - Discussion point 1: How to ensure future regular updates?
- VI. SR69 Update
  - Summary of the current plan for updates by departments
  - Discussion point 2: How to ensure future regular updates?
- VII. Geospatial Data Governance Framework
- VIII. Discussion point 3: Suggested Topics for Next Meeting on March 17<sup>th</sup>, 2025

IX. Announcements  
Next Meeting: March 17, 2025

X. Adjournment

If you need an auxiliary aid/service or other accommodation due to disability, call Joanna Lee at (808) 587-9735 or email [joanna.y.lee@hawaii.gov](mailto:joanna.y.lee@hawaii.gov) Requests made as early as possible have a greater likelihood of being fulfilled. Upon request, this notice is available in alternate/accessible formats.



**DATA TASK FORCE MEETING - DRAFT**  
September 16, 2024

Meeting was held via Microsoft Teams (videoconference interactive conferencing technology).  
Physical location: 1151 Punchbowl Street, Conference Room 410, Honolulu, Hawai'i

Members Present

Rebecca Cai, Office of Enterprise Technology Services (ETS)  
Mai Nguyen Van, Judiciary  
Timothy Hosoda, Department of Education  
Phan Sirivattha, Department of Human Services  
Steve Sakamoto, Department of Health  
Sandra Furuto, University of Hawai'i  
Thomas Lee, Hawai'i Data Collective  
Kaimana Walsh, Hawai'i Green Growth  
Representative Amy Perruso, State House  
Torrie Inouye, Bank of Hawai'i

Members Excused

Dr. Eugene Tian, Department of Business, Economic Development and Tourism

Other Attendees

ETS: Shelby Albertson, Javzandulam Azuma, Susan Bannister, Juha Kauhanen, Joanna Lee, Kyle Makanui  
Dulce Belen  
Jeff Hickman  
Clayton Lewis  
Derek Vale  
Brian

- I. Call to Order  
Roll call was taken. With quorum established, the meeting was called to order at 3:00 p.m. Chair Cai welcomed new member, Phan Sirivattha, who will represent the Department of Human Services.
- II. Public Testimony  
None.
- III. Review and Approval of the March 18, 2024 and June 17, 2024, Meeting Minutes  
Member Van made a motion to approve the minutes as presented, which was seconded by Member Rep. Perruso. A vote was taken and passed unanimously.

IV. Data Task Force Charter Review and Approval

Member Van made a motion to approve the Charter as presented, which was seconded by Member Rep. Perruso. A vote was taken and passed unanimously.

V. Progress Update

- Data Quality Standards - Review & Approval. Member Lee made a motion to approve the standards as presented, which was seconded by Member Rep. Perruso. Member Sirivattha commented that as a new member he would like time to review. Chair Cai recommended moving this item to the next meeting.
- Data Privacy Standards - Review & Approval. Deferred to the next Data Task Force meeting.
- Data and AI Glossary published on [State Data Office | Data and AI Glossary \(hawaii.gov\)](#) . Chair Cai reported that the Data and AI glossaries were added to the State Data Office website.
- Data Literacy Training published on [State Data Office | Data Literacy \(hawaii.gov\)](#) Training contents have been added to the State Data Office website. Assessment tests have been created for data literacy.

VI. Update from 21<sup>st</sup> Century Data Governance Task Force – Ethnicity Disaggregation

Derek Vale, Chief Data Officer with the Department of Health, gave a brief update on the task force.

- Ensure the committee identify what the potential issues and blockers are toward social determinants of health data standardization. What social determinants or values does the community have and how can the task force best reflect the reality of its population and sub populations.
- Current data is missing in many areas or data is incomplete.
- Need comprehensive consistent standards to ensure all populations are represented. How can the task force help agencies with the standardization.
- Need consistent standards for race, ethnicity, language, sexual orientation, gender identity, housing. Start with race and ethnicity and look at what those barriers are and work toward consistency across agencies with gathering and reporting of the information.
- Develop specific standards for the State and make recommendations to this task force.
- Will prepare a report with recommendations to the Legislature in December. The 21<sup>st</sup> Century Data Governance Task Force sunsets in 2025.

Chair Cai reported on a new federal law enacted in March 2024. Have five years to comply. She suggested sending a memo to departments informing them of this new requirement and requesting that they start collecting such data. Member Sirivattha added that there should be a mechanism for which departments can communicate with this Task Force. Chair Cai will draft a memo for members' review and comments.

VII. Senate Resolution (SR) 69 Action Plan Update

SR 69 wants to improve the State's open data portal by increasing and expanding the data sets available on the open data portal, centralize all open data sets of all state departments onto the open data portal, and continually update the data sets for accuracy and recency of publicly accessible data. Opendata.hawaii.gov would provide citizens all government open data.

Chair Cai has met with most departmental data leads. This group will form a data governance working group to share statewide best practices and use cases to ensure data consistency and quality across the departments. They have agreed on the approach but asked for guidelines regarding data to be replicated on [opendata.hawaii.gov](https://opendata.hawaii.gov). Topics include data sets generated by the department, other data sets obtained by the department, data visualizations and reports, online searches. Chair Cai asked if recommendations should be made.

Member Rep. Perruso cautioned using strong language or making strong recommendations at the onset. Suggested ETS meet with the executive branch and Governor's Office. If data transparency is a priority, their support will increase the likelihood of legislation being introduced and provide funding for more transparency with open data. Chair Cai will follow up with his office.

Member Sirivattha commented on the complexity of defining data and Information sharing. Chair Cai recommended focus on specific use cases that can add value to the citizens. Discuss which departments are involved, what datasets are involved, any definitions that might vary across departments. Hope to come together and have a road map of the different use cases at each department and different data sets involved.

Mr. Vale added that as each use case is developed the team can move on to another. It will take a while to have a standardization. Member Inouye suggested picking a narrower use case where parties are motivated to collaborate.

VIII. Data Team Participation in the Hawaii Code Challenge

The ETS Data Team will be participating in the Annual Hawaii Code Challenge that kicks off on October 12, 2024.

IX. Announcements

Next meeting is on December 16, 2024.

- X. **Adjournment**  
The meeting adjourned at 3:50 p.m.



# Hawaii's Journey to a Data-Driven Future

---

Data Task Force Meeting  
December 16<sup>th</sup>, 2024



# Agenda











1. Approve meeting minutes for the September DTF meeting;
2. Approve data/AI policies:
  1. Data Privacy Guidelines
  2. Data Catalog Guidelines
  3. Data Classification Guidelines
  4. Data Retention Guidelines
  5. Open Data Guidelines
  6. GenAI Assistant Technologies Usage Guidelines
3. 2024 deliverables summary:
  1. Overview with accomplishments summary
  2. Discussion point 1: what is needed to ensure compliance?
4. SR69 update:
  1. Summary of the current plan for updates by departments.
  2. Discussion point 2: how to ensure future regular updates?
5. Geospatial data governance framework
6. Discussion point 3: suggested topics for next meeting on March 17<sup>th</sup>, 2025?




# In 2024, we have created 8 data/AI guideline documents with 7 approved by the State Data Task Force and published on [data.Hawaii.gov](https://data.hawaii.gov)



 <b>Data Quality Guidelines</b>	Guidance to proactively monitor, manage, and improve data quality which includes accuracy, completeness, consistency, timeliness, uniqueness, and validity.	 <b>Data Retention Guidelines</b>	Guidance to define how long a data set shall be stored to ensure compliance and to prevent data loss by ensuring regular backups.
 <b>Data Privacy Guidelines</b>	Guidance to ensure Personally Identifiable Information (PII) data is identified and protected during data collection, processing, storage, usage, and sharing processes.	 <b>Open Data Guidelines</b>	Guidance to ensure that publicly accessible data is consistently shared and updated, outlining how to identify open data (public data) according to the OIP policies.
 <b>Data Catalog Guidelines</b>	Guidance to identify and inventory all existing data assets with a summary of what each data set is, who owns each data set from business, and how it can be used (metadata).	 <b>GenAI Assistant Technologies Usage Guidelines</b>	Guidance to safely and responsibly use GenAI assistant technologies. It includes dos and don'ts, best practices, and key features of specific GenAI tools.
 <b>Data Classification Guidelines</b>	Guidance to classify data based on sensitivity for proper protection including data set level access control. This is the key enabler of secured data sharing.	 <b>Responsible AI Use Guidelines</b>	Guidance to responsibly and ethically use all AI technologies. It includes AI risk management framework and key considerations to ensure responsible use of AI.

 Published

 Drafted, under internal review

 To be approved during the 12/16/2024 Data Task Force meeting

# The State Data Task Force approved the state's Data and AI Strategy on March 16<sup>th</sup>, 2024, with deliverables aligned to the strategic goals



## Hawaii's Data and AI Strategy: drive trust, transparency, citizen satisfaction, and innovation through responsible use of data and AI in public services

### Vision

To drive **trust, transparency, citizen satisfaction, and innovation** by improving security, quality, accessibility, accountability of data and AI.

### Mission

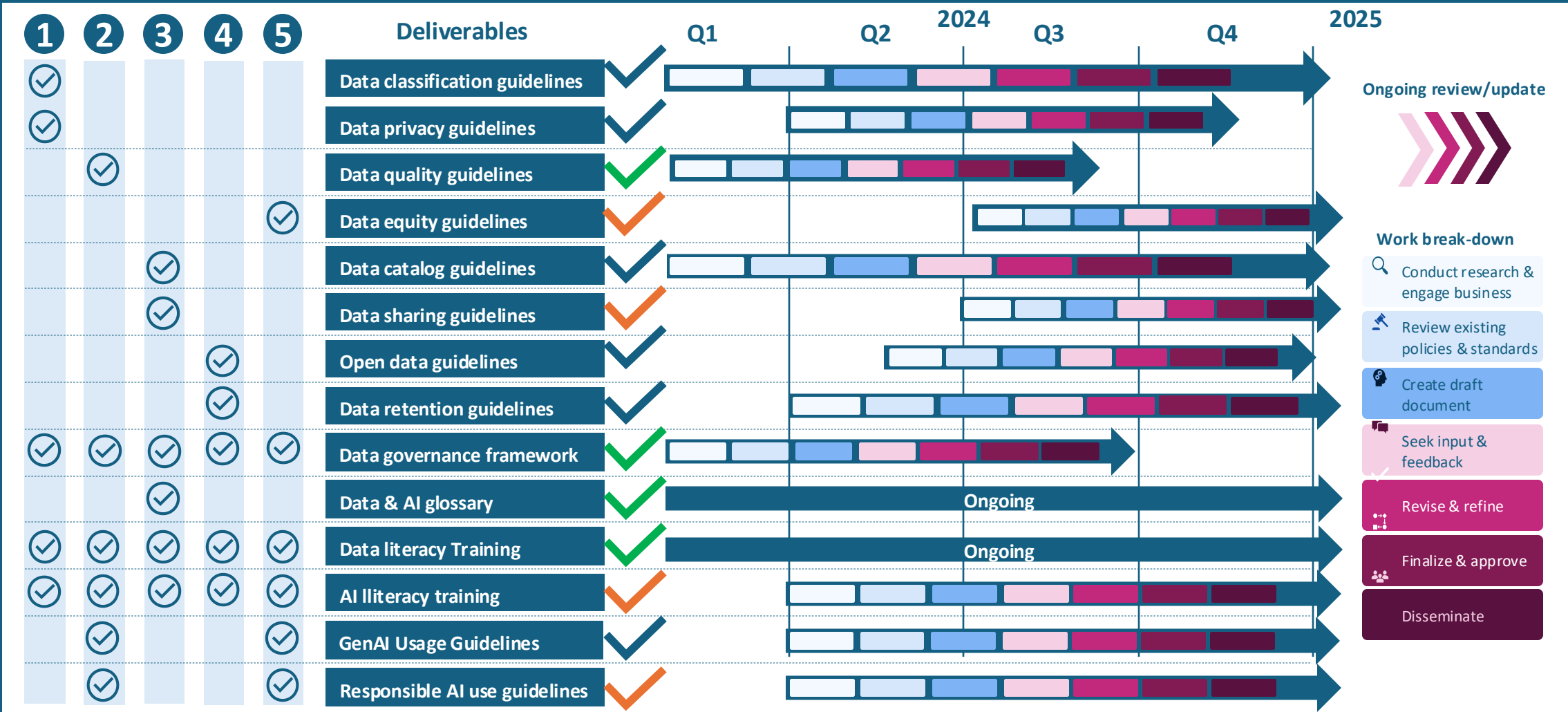
Cultivate a data-driven, impact-focused, and citizen-centric culture to promote data sharing and integration, privacy protection, evidence-based policy making, and responsible use of data and AI.

### Goals

### Objectives

<b>1</b> Protect privacy, ensure security and compliance	<ul style="list-style-type: none"> <li>• Create data classification and masking standards for all data and AI use.</li> <li>• Protect data privacy according to Federal and State laws &amp; regulations.</li> </ul>
<b>2</b> Improve quality, accuracy and reliability	<ul style="list-style-type: none"> <li>• Establish standards, procedures and tools to manage and improve data quality.</li> <li>• Define data and AI governance according to data quality to promote trust.</li> </ul>
<b>3</b> Promote accessibility and inter-operability	<ul style="list-style-type: none"> <li>• Catalog all state data and integrate master data to enable citizen-centric solutions.</li> <li>• Establish data sharing standards and recommend tools to improve inter-operability.</li> </ul>
<b>4</b> Drive accountability and transparency	<ul style="list-style-type: none"> <li>• Identify owners of data set and AI use cases with clearly defined responsibilities.</li> <li>• Update open data standards to ensure governance &amp; transparency in data &amp; AI use.</li> </ul>
<b>5</b> Ensure equity and ethical responsible use of data & AI	<ul style="list-style-type: none"> <li>• Build data and AI governance framework to ensure equity throughout their lifecycle.</li> <li>• Create auditing mechanism to ensure equitable and ethical use in data and AI.</li> </ul>

There are 14 deliverables, with 4 published, 6 to be approved today to publish, and 4 are work in progress



✓ Published   
 ✓ Work in progress   
 ✓ To be approved during the 12/16/2024 Data Task Force meeting

## Discussion point 1: What is needed to ensure compliance to start improving the State's data and AI?



What is needed to ensure compliance to start improving the State's data and AI?

1. Authority?
2. Tools?
3. Resources?
4. Anything else?



# SR69 update (1 of 2): most departments have established plans to update existing open data sets on [opendata.Hawaii.gov](https://opendata.hawaii.gov) according to departmental data leads

Departments	Q4 2024			Q1 2025			Q2 2025			Q3 2025			Q4 2025		
	Oct	Nov	Dec	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
Dept of Health (DOH)	TBD			TBD			TBD			TBD			TBD		
Dept Hawaiian Home Lands (DHHL)	0 data sets			0 data sets			0 data sets			0 data sets			0 data sets		
State Public Charter School Commission (SPCSC)	0 data sets			0 data sets			0 data sets			0 data sets			0 data sets		
Dept of Commerce & Consumer Affairs (DCCA)	0 data sets			0 data sets			0 data sets			0 data sets			0 data sets		
Dept of Attorney General (AG)	0 data sets			2-3 data sets			TBD			TBD			TBD		
Hawai'i Public Housing Authority (HPHA)	0 data sets			0 data sets			0 data sets			0 data sets			0 data sets		
Office of Wellness & Resilience (OWR)	0 data sets			0 data sets			0 data sets			0 data sets			0 data sets		
Office of the Governor	0 data sets			0 data sets			0 data sets			0 data sets			0 data sets		
Dept of Human Resources Development (DHRD)	0 data sets			0 data sets			0 data sets			0 data sets			0 data sets		
Accounting & General Services (DAGS)	19 data sets			19 data sets			19 data sets			19 data sets			20 data sets		
Dept of Taxation	0 data sets			0 data sets			0 data sets			0 data sets			0 data sets		
Hawai'i State Public Library System	4 data sets			2 data sets			1 data set			2 data sets			1 data set		
Executive Office on Early Learning (EOEL)	TBD			TBD			TBD			TBD			TBD		

Note. Updates provided by each data lead with “TBD” indicating departments/offices still working to collect this information or make determinations. According to the March 2024 Open Data Site Audit, there are 547 datasets on [opendata.Hawaii.gov](https://opendata.hawaii.gov), excluding geospatial data. This table includes datasets updated in Q4 2024 and projections for updates in Q1-Q4 of 2025.



# SR69 update (2 of 2): most departments have established plans to update existing open data sets on [opendata.Hawaii.gov](https://opendata.hawaii.gov) according to departmental data leads

Departments	Q4 2024			Q1 2025			Q2 2025			Q3 2025			Q4 2025		
	Oct	Nov	Dec	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
Dept of Business, Economic Development & Tourism (DBEDT)	15 data sets			19 data sets			10 data sets			TBD			TBD		
Dept of Land & Natural Resources (DLNR)	0 data sets			0 data sets			0 data sets			0 data sets			0 data sets		
Dept of Human Services (DHS)	TBD			TBD			TBD			TBD			TBD		
Dept of Education (DOE)	0 data sets			0 data sets			0 data sets			0 data sets			0 data sets		
Dept of Agriculture (DOA)	TBD			TBD			TBD			TBD			TBD		
Hawai'i State Energy Office (HSEO)	0 data sets			0 data sets			0 data sets			0 data sets			0 data sets		
Dept of Budget & Finance (B&F)	0 data sets			TBD			TBD			TBD			TBD		
Dept of Defense (DOD)	0 data sets			TBD			TBD			TBD			TBD		
Dept of Labor & Industrial Relations (DLIR)	0 data sets			TBD			TBD			TBD			TBD		
Dept of Law Enforcement (DLE)	0 data sets			0 data sets			0 data sets			0 data sets			0 data sets		
Dept of Corrections & Rehabilitation (DCR)	0 data sets			0 data sets			0 data sets			0 data sets			0 data sets		
Dept of Transportation (DOT)	TBD			TBD			TBD			TBD			TBD		
Child Support Enforcement Agency	0 data sets			0 data sets			0 data sets			0 data sets			0 data sets		
Judiciary	0 data sets			0 data sets			0 data sets			0 data sets			0 data sets		

Note. Updates provided by each data lead with “TBD” indicating departments/offices still working to collect this information or make determinations. According to the March 2024 Open Data Site Audit, there are 547 datasets on [opendata.Hawaii.gov](https://opendata.hawaii.gov), excluding geospatial data. This table includes datasets updated in Q4 2024 and projections for updates in Q1-Q4 of 2025.

## Discussion point 2: How can we ensure future regular updates to all open data sets on [opendata.Hawaii.gov](https://opendata.hawaii.gov)?



How can we ensure future regular updates to all open data sets on [opendata.Hawaii.gov](https://opendata.hawaii.gov)?

1. ETS: technology to automate data update
2. ETS: open data coordinator to monitor and analyze open data sets
3. ETS: open data coordinator to work with departments
4. Departments: what is needed?

# We established the State Geospatial Data Governance Framework in collaboration with the State GIS team from DBEDT



## State geospatial data governance working group



ETS GIS Team



State GIS program



Department GIS Data Lead



Departmental GIS Users



- **Statewide data policies and standards:** Develop & review standards and guidelines for geospatial data governance (GIS content management, GIS data catalog, GIS data quality, etc.)
- **Enterprise license management:** Develop process to oversee & track Esri licenses and determine departmental license allocation numbers at the beginning of the EA
- **AGOL User creation and license deployment:** ETS Help Desk create users and deploy licenses in AGOL as identified by Departmental GIS Data Leads



- **Departmental license needs identification:** Identify departmental license needs
- **Departmental AGOL User Type needs identification:** Identify departmental User Type needs and submit request to ETS
- **Oversee Compliance with Esri Agreement:** Oversee departmental compliance with Esri agreement (User Type caps, License Level caps)



- **Identification of datasets to be hosted in Statewide geodatabase:** Identify datasets that are appropriate to share via the Statewide geodatabase and public geoportal
- **Identification of projects involving spatial data and/or analysis:** Identify existing or upcoming projects that have spatial data or analysis components

## Departmental geospatial data governance working group



- **Department Specific GIS Data Rules:** Develop tailored GIS data rules for datasets specific to the department, ensuring compliance within departmental operations, including assignment of publishing roles to appropriate users
- **GIS data quality management:** review and improve own GIS data quality



- **Define Dataset Access Controls:** Establish access control on their content and comply with guidelines for data storage and destruction



## Discussion point 3: Next meeting agenda items suggestions



### Next meeting agenda items suggestions:

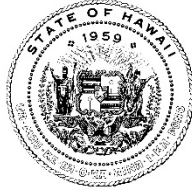
1. **Responsible AI Use Guidelines review**
2. **AI Literacy training update**
3. **Any suggestions?**



**Thank you!**

---





# Data Privacy Guidelines

**Document No: CDO-002**

**Updated: December 8, 2024**

**Issued by: Chief Data Officer**

## 1.0 Purpose

The purpose of the Data Privacy Guidelines is to establish common guidelines for data privacy management across State of Hawaii agencies. Through responsible data privacy practice, State agencies can better serve citizens of the State of Hawaii while protecting privacy, managing risk, and promoting accountability and equity.

## 2.0 Authority

Section 27-44, Hawaii Revised Statutes (HRS),<sup>1</sup> provides the Chief Data Officer with the authority to develop, implement, and manage statewide data policies, procedures, and standards, and 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

### 3.1 State Agencies

The Data Privacy Guidelines are developed with reference to the National Institute of Standards and Technology (NIST) Privacy Framework CORE.<sup>2</sup> It applies to all executive branch departments, including the Department of Education and the University of Hawaii, to ensure that we have common guidelines to protect data privacy across state agencies.

The Data Privacy Guidelines provide high level guidelines on data privacy protecting Personally Identifiable Information (PII) data. Each agency shall develop additional policies and guidelines as necessary according to relevant federal and state laws and regulations, both

---

<sup>1</sup> HRS §27-44. [https://www.capitol.hawaii.gov/hrscurrent/Vol01\\_Ch0001-0042F/HRS0027/HRS\\_0027-0044.htm](https://www.capitol.hawaii.gov/hrscurrent/Vol01_Ch0001-0042F/HRS0027/HRS_0027-0044.htm)

<sup>2</sup> NIST Privacy Framework. <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020.pdf>

at the data set level and at the individual field level, to ensure compliance in its operations. Where a conflict exists between the Data Privacy Guidelines and an agency's policy, the more restrictive policy will take precedence.

### 3.2 Definitions

The Data Privacy Guidelines provide guidelines for using Personal Identifiable Information (PII)<sup>3</sup> in data and Artificial Intelligence (AI)<sup>4</sup> processes.

### 3.3 Covered Use

The Data Privacy Guidelines apply to the handling of PII data in all data sets handled by state agencies, regardless of whether it is used for AI or not. This includes but is not limited to systems in the cloud, on premises, and on local drives.

The Data Privacy Guidelines shall be applied to the entire data life cycle from data creation, data collection, data cleansing and transformation, data storage and modeling, data science and analytics, data visualization, impact tracking, and data retention. It shall also be applied to all data applications, including Machine Learning<sup>5</sup> and AI.

## 4.0 Information Statement

### 4.1 Data Collection

- Data Minimization: Collect and process only the data absolutely needed for specific purposes. No extra PII data shall be collected. This reduces the amount of PII data stored and minimizes the potential for misuse.
- Authorization and Consent: Obtain consent required by law before collecting, using, or disclosing PII data. Provide clear and concise information about data usage, sharing, and options for withdrawing consent. If a data processor requests to repurpose collected PII data, seek consent for that new use. This does not apply to open data and other non-private data. Maintain documented procedures for authorizing data processing activities, including internal approvals and individual consent mechanisms.
- Expressing Data Preferences: State agencies shall provide mechanisms for individuals to express their preferences on how their PII data is collected and used. This may include options to opt out of certain data collection practices or to limit how their PII data is shared with third parties.

---

<sup>3</sup> Refer to 7.0 Definitions of Key Terms

<sup>4</sup> Refer to 7.0 Definitions of Key Terms

<sup>5</sup> Refer to 7.0 Definitions of Key Terms

- Transparency: State agencies must provide clear and transparent notices on what data is being collected, the purpose of its collection, and how it will be used, to ensure compliance with relevant state and federal laws.

## 4.2 Data Processing and Sharing

- Accessing and Managing Data: If possible, allow individuals to have the right to request access to their PII data, review it for accuracy, and request deletion, following applicable legal requirements and data retention policies.
- Data Ownership and Accountability: State agencies shall identify data owners for each data set that contains PII information to promote accountability. Any use of PII data shall be in compliance with all federal, state, and local policies and regulations. No PII data shall be used in any GenAI model.
- Segregation and Access Controls: State agencies shall segregate PII data from public records and establish access controls according to all policies, laws, and regulations.

## 4.3 Data Protection

- Safeguards: State agencies shall implement appropriate safeguards, according to all federal and state laws and regulations, to protect PII data from unauthorized access, disclosure, alteration, or destruction. This includes security best practices, access controls, data encryption, and secure maintenance practices.
- De-identification and Pseudonymization: State agencies shall employ techniques such as de-identification (removing identifiers) and pseudonymization (replacing identifiers with unique codes) to limit the ability to identify individuals. This practice reduces the risk of individuals being singled out from the data set.

## 5.0 Compliance

The Data Privacy Guidelines shall take effect upon publication. The Chief Data Office may amend at any time; compliance with guidelines is strongly recommended to protect state PII data.

## 6.0 Contact Information

Submit all inquiries and requests for future enhancements to the Chief Data Office at [data@hawaii.gov](mailto:data@hawaii.gov)

All Data related policies and guidelines documents can be found at [data.hawaii.gov](http://data.hawaii.gov)

## 7.0 Definitions of Key Terms

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

- **Data Privacy:** Data privacy refers to freedom from intrusion into the private life or affairs of an individual when that intrusion results from undue or illegal gathering and use of data about that individual.<sup>6</sup>
- **Access Control:** Access Control refers to the process of granting or denying specific requests to 1) obtain and use information and related information processing services and 2) enter specific physical facilities (e.g., federal buildings, military establishments, border crossing entrances).<sup>7</sup>
- **Personally Identifiable Information (PII):** Personally identifiable information refers to information that can be used to distinguish or trace an individual’s identity, either alone or when combined with other information that is linked or linkable to a specific individual.<sup>8</sup>
- **De-identification:** De-identification refers to any process of removing the association between a set of identifying data and the data subject.<sup>9</sup>
- **Pseudonymization:** Pseudonymization refers to a de-identification technique that replaces an identifier (or identifiers) for a data principal with a pseudonym in order to hide the identity of that data principal.<sup>10</sup>
- **Artificial Intelligence (AI):** A branch of computer science devoted to developing data processing systems that performs functions normally associated with human intelligence, such as reasoning, learning, and self-improvement.<sup>11</sup>
- **Machine learning (ML):** Machine learning refers to a field within artificial intelligence, focuses on the ability of computers to learn from provided data without being explicitly programmed for a particular task.<sup>12</sup>

## 8.0 Revision History

Date	Description of Change
December 16, 2024	To be reviewed by the DTF

<sup>6</sup> National Institute of Standards and Technology (NIST) SP 800-188.

<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-188.pdf>

<sup>7</sup> National Institute of Standards and Technology (NIST) FIPS PUB 201-3.

<https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.201-3.pdf>

<sup>8</sup> OMB Circular A-130.

<https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf>

<sup>9</sup> National Institute of Standards and Technology (NIST) Glossary. [https://csrc.nist.gov/glossary/term/de\\_identification](https://csrc.nist.gov/glossary/term/de_identification)

<sup>10</sup> National Institute of Standards and Technology (NIST) Glossary. <https://csrc.nist.gov/glossary/term/pseudonymization>

<sup>11</sup> U.S. Department of State. <https://www.state.gov/artificial-intelligence/#:~:text=Artificial%20Intelligence%20and%20Society&text=%E2%80%9CThe%20term%20'artificial%20intelligence',influencing%20real%20or%20virtual%20environments.%E2%80%9D>

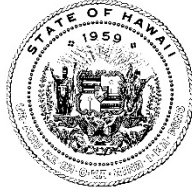
<sup>12</sup> National Institute of Standards and Technology (NIST). <https://www.nccoe.nist.gov/ai/adversarial-machine-learning>

## 9.0 Related Documents and Sources

- [1] Information Quality Act <https://www.govinfo.gov/content/pkg/PLAW-106publ554/html/PLAW-106publ554.htm>
- [2] 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>
- [3] Critical Infrastructure Information, 6 USC CHAPTER 1, SUBCHAPTER XVIII, Part B <https://www.cisa.gov/sites/default/files/publications/CII-Act.pdf>
- [4] Driver's Privacy Protection Act (DPPA) H.R.3365 — 103rd Congress (1993-1994). <https://www.law.cornell.edu/uscode/text/18/2721>
- [5] Family Educational Rights and Privacy Act (FERPA). <https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html>
- [6] Health Insurance Portability and Accountability Act of 1996 (HIPAA). <https://aspe.hhs.gov/reports/health-insurance-portability-accountability-act-1996>
- [7] 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>
- [8] Criminal Justice Information Services (CJIS) Security Policy. <https://le.fbi.gov/cjis-division/cjis-security-policy-resource-center>
- [9] Internal Revenue Service Tax Information Security Guidelines for Federal, State and Local Agencies. <https://www.irs.gov/privacy-disclosure/safeguards-program>
- [10] 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>
- [11] Nacha Operating Rules. ACH payment. <https://www.nacha.org/newrules>
- [12] Payment Card Industry Data Security Standard (PCI DSS) v 3.2. [https://www.pcisecuritystandards.org/document\\_library/?category=pcidss&document=pci\\_dss](https://www.pcisecuritystandards.org/document_library/?category=pcidss&document=pci_dss)
- [15] Hawaii State DOT, Motor Vehicle Drivers License and related offices. [https://hidot.hawaii.gov/highways/files/2018/02/Privacy\\_Policy\\_Stmnt\\_mvso-12-12-2017.pdf](https://hidot.hawaii.gov/highways/files/2018/02/Privacy_Policy_Stmnt_mvso-12-12-2017.pdf)

[16] Fair Information Practice Principles (FIPPs). [Fair Information Practice Principles \(FIPPs\) | FPC.gov](#)





# Data Catalog Guidelines

**Document No: CDO-003**

**Updated: December 8, 2024**

**Issued by: Chief Data Officer**

## 1.0 Purpose

The purpose of the Data Catalog Guidelines is to establish common guidelines for data catalog management across State of Hawaii agencies. Through effective data catalog management, state agencies can promote transparency and data sharing, improve data governance and compliance, and enable evidence-based decision-making across the State of Hawaii agencies.

## 2.0 Authority

Section 27-44, Hawaii Revised Statutes (HRS),<sup>1</sup> provides the Chief Data Officer with the authority to develop, implement, and manage statewide data policies, procedures, and standards and 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

### 3.1 State Agencies

The Data Catalog Guidelines apply to all state agencies.

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

### 3.2 Definitions

---

<sup>1</sup> HRS §27-44. [https://www.capitol.hawaii.gov/hrscurrent/Vol01\\_Ch0001-0042F/HRS0027/HRS\\_0027-0044.htm](https://www.capitol.hawaii.gov/hrscurrent/Vol01_Ch0001-0042F/HRS0027/HRS_0027-0044.htm)

A data catalog is a detailed inventory of all data assets (and information about those data assets) in an organization, designed to help data professionals quickly find and understand data efficiently for any business purposes.

### 3.3 Covered Use

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

## 4.0 Information Statement

Each agency is responsible for creating and maintaining its data catalog and metadata. The following are the recommended minimum requirements:

- **Ownership:**

Each agency shall identify a data steward for each data assets. A data steward is an agency official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination and disposal.<sup>2</sup>

Responsibilities of data steward for each data asset shall include:

1. Define access control to ensure compliance.
2. Maintain quality of the data.
3. Ensure data integrity and security.

- **Completeness:**

The data catalog shall include all relevant data assets for each specific business use case including spatial data, regardless of format, location, or storage method (databases, spreadsheets, files, cloud storage, etc.). This includes databases, spreadsheets, files, cloud storage, and any other potential data sources and storage locations.

- **Metadata:**

The catalog shall include up-to-date metadata information about each data asset. This metadata serves as essential information about the data, fostering interoperability and data sharing.

- **Automation:**

Automated tools and workflows are strongly recommended whenever possible for data catalog creation and updates to improve efficiency and accuracy.

---

<sup>2</sup> National Institute of Standards and Technology (NIST) Glossary.  
[https://csrc.nist.gov/glossary/term/information\\_steward](https://csrc.nist.gov/glossary/term/information_steward)

## 5.0 Compliance

The Data Catalog Guidelines shall take effect upon publication. The Chief Data Office may amend at any time; compliance with guidelines is strongly recommended.

## 6.0 Contact Information

Submit all inquiries and requests for future enhancements to the Chief Data Office at [data@hawaii.gov](mailto:data@hawaii.gov).

Additional data related policies and guidelines documents can be found at [data.hawaii.gov](http://data.hawaii.gov).

## 7.0 Definitions of Key Terms

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

- **Data Catalog:** Data Catalog refers to an organized inventory of data assets in the organization. It uses metadata to help organizations manage their data. It also helps data professionals collect, organize, access, and enrich metadata to support data discovery and governance.<sup>3</sup>
- **Metadata:** Information describing the characteristics of data including, for example, structural metadata describing data structures (e.g., data format, syntax, and semantics) and descriptive metadata describing data contents (e.g., information security labels).<sup>4</sup>
- **Data Asset:** 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.<sup>5</sup>
- **Data Steward:** A data steward is an agency official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.<sup>6</sup>
- **Data Governance:** Data Governance refers to setting direction on data use through prioritization and decision making, and ensuring alignment with agreed-on direction and objectives.<sup>7</sup>
- **Spatial data:** Spatial data, also known as geospatial data, refers to information that

---

<sup>3</sup> Oracle. <https://www.oracle.com/big-data/data-catalog/what-is-a-data-catalog/>

<sup>4</sup> National Institute of Standards and Technology (NIST) Glossary. <https://csrc.nist.gov/glossary/term/metadata>

<sup>5</sup> National Institute of Standards and Technology (NIST) Glossary. [https://csrc.nist.gov/glossary/term/data\\_asset](https://csrc.nist.gov/glossary/term/data_asset)

<sup>6</sup> National Institute of Standards and Technology (NIST) Glossary. [https://csrc.nist.gov/glossary/term/information\\_steward](https://csrc.nist.gov/glossary/term/information_steward)

<sup>7</sup> Information Systems Audit and Control Association (ISACA). <https://www.isaca.org/resources/glossary>

explicitly describes the location, shape, and relationships of geographic features and phenomena. It can exist in various formats and dimensions, including:<sup>8</sup>

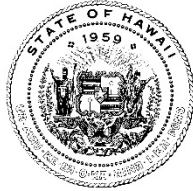
- Points: Representing discrete locations (e.g., addresses, landmarks).
- Lines: Representing linear features (e.g., roads, rivers, boundaries).
- Polygons: Representing areas with defined extents (e.g., buildings, countries).
- Rasters: Representing continuous data on the earth's surface using grid cells (e.g., elevation, temperature, windspeed, precipitation). Higher-resolution data has smaller grid cells and represents data with greater precision.
- Images: Capturing spatial information through pixels (e.g., satellite imagery, aerial photographs).
- Lidar: Refers to a type of remote sensing data that uses lasers, commonly used to create high-resolution elevation models.
- 3D models: Representing objects and features in three dimensions.

## 8.0 Revision History

Date	Description of Change
December 16, 2024	To be reviewed by the DTF

---

<sup>8</sup> Types of Spatial Data. <https://geographicbook.com/types-of-spatial-data/>



## Data Classification Guidelines

**Document No: CDO004**

**Updated: December 8, 2024**

**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.

### 2.0 Authority

Section 27-44, Hawaii Revised Statutes (HRS),<sup>1</sup> provides the Chief Data Officer with the authority to develop, implement, and manage statewide data policies, procedures, and standards and 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

#### 3.1 State Agencies

The Data Classification Guidelines apply to all state agencies.

The Data Classification Guidelines provide high level guideline 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 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.

#### 3.2 Definitions

---

<sup>1</sup> HRS §27-44. [https://www.capitol.hawaii.gov/hrscurrent/Vol01\\_Ch0001-0042F/HRS0027/HRS\\_0027-0044.htm](https://www.capitol.hawaii.gov/hrscurrent/Vol01_Ch0001-0042F/HRS0027/HRS_0027-0044.htm)

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.<sup>2</sup>

### 3.3 Covered Use

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.

## 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.

This approach 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, it 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 the 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
-------	-------------	---------	--------------	--------

---

<sup>2</sup> Information Systems Audit and Control Association (ISACA) Glossary. <https://www.isaca.org/resources/glossary>

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. The Chief Data Office may amend at any time; compliance with guidelines is strongly recommended.

## 6.0 Contact Information

Submit all inquiries and requests for future enhancements to the Chief Data Office at [data@hawaii.gov](mailto:data@hawaii.gov).

## 7.0 Definitions of Key Terms

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

- **Data Asset:** 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.<sup>3</sup>
- **Sensitivity:** Sensitivity refers to the potential harm that could result from unauthorized access, disclosure, modification, or destruction of information.<sup>4</sup>
- **Transmission:** Transmission refers to the movement of information across a communication

<sup>3</sup> National Institute of Standards and Technology Glossary. [https://csrc.nist.gov/glossary/term/data\\_asset](https://csrc.nist.gov/glossary/term/data_asset)

<sup>4</sup> National Institute of Standards and Technology Glossary. <https://csrc.nist.gov/glossary/term/sensitive>

channel.<sup>5</sup>

## 8.0 Revision History

Date	Description of Change
December 16, 2024	To be reviewed by the DTF

## 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](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).

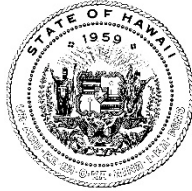
<https://aspe.hhs.gov/reports/health-insurance-portability-accountability-act-1996>

---

<sup>5</sup> National Institute of Standards and Technology Glossary. <https://csrc.nist.gov/glossary/term/transmission>



- [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](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/CI-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>



# Data Retention Guidelines

**Document No: CDO005**

**Updated: December 8, 2024**

**Issued by: Chief Data Officer**

## 1.0 Purpose

The purpose of the Data Retention Guidelines is to establish common guidelines for data retention across State of Hawaii agencies.

## 2.0 Authority

Section 27-44, Hawaii Revised Statutes (HRS),<sup>1</sup> provides the Chief Data Officer with the authority to develop, implement, and manage statewide data policies, procedures, and standards, and 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

### 3.1 State Agencies

The Data Retention Guidelines apply to all state agencies.

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

### 3.2 Definitions

The Data Retention Guidelines refer to the practice of storing data for a specific period.

---

<sup>1</sup> HRS §27-44. [https://www.capitol.hawaii.gov/hrscurrent/Vol01\\_Ch0001-0042F/HRS0027/HRS\\_0027-0044.htm](https://www.capitol.hawaii.gov/hrscurrent/Vol01_Ch0001-0042F/HRS0027/HRS_0027-0044.htm)

The Data Retention Guidelines apply to data retention, not records retention, as record retention policies are published by the Hawaii State Archives. For an explanation on the difference between data and records, please refer to the section 7.0, Definitions of Key Terms.

## 4.0 Information Statement

Each State agency is responsible for retaining its records based on retention and disposal schedules<sup>2</sup> developed by the Hawaii State Archives, Records Management Branch and in compliance with relevant regulatory requirements. The Data Retention Guidelines shall align with the longest approved retention period for the records created from or reliant upon that data. For additional regulatory references, please see Appendix A.

The following section outlines general guidelines. Each agency must also adhere to any additional policies and guidelines set by federal and state laws to ensure compliance. If there is a conflict between requirements, the stricter rules will apply.

### 4.1 Data Retention and Backup

To prevent data loss, particularly for electronic data, regular data backup is recommended. Frequency is based on the type of data and the risk of losing data to be regulated by each agency. Backups should be retained until the next full backup is successfully completed.

### 4.2 Safeguard data during retention

Data protection must be applied to all forms of data, whether actively used or stored as backups and archives. This includes implementing security measures such as encryption, access controls, and regular audits to prevent unauthorized access or data breaches. The specific measures will vary based on the classification of the data, as outlined below:

- **Public data:** Basic security measures are sufficient for public data, including access controls to prevent unauthorized edits or deletions. Maintaining version histories is also important to ensure the accuracy of shared information.
- **Internal Data:** Internal data shall have role-based access controls to restrict access to authorized personnel. While encryption is less critical, role-based access controls adds a layer of protection, particularly for electronic records. Regular reviews are necessary to ensure compliance and to detect any unauthorized access.
- **Protected Data:** Strong encryption is essential for protected data, both at rest and in transit. Multi-factor authentication shall be required for access, and data masking

---

<sup>2</sup> State of Hawaii records retention and disposition schedules can be found at: <https://ags.hawaii.gov/archives/about-us/records-management/records-retention-and-disposition-schedules/>

techniques can be employed when sharing sensitive information for analysis. Organizations shall also have incident response plans in place to quickly address breaches.

- **Classified Data:** The highest security guidelines apply to classified data. This includes using advanced encryption for both stored and transmitted information. Physical records shall be kept in locked cabinets or safes, and electronic data must reside on secure servers. Strict access controls and regular security audits are crucial for identifying vulnerabilities. Additionally, clear protocols for securely destroying classified data must be established once the classified data is no longer needed.

### 4.3 Data Disposal Methods

Data that must be retained according to the State's retention and disposition schedules is prohibited from disposal or deletion until the designated retention period has expired. Once the retention period has lapsed, data owners are responsible for determining the appropriate disposal methods based on the classification of the data, as outlined below:

- **Public Data:** Dispose using standard deletion methods. This may include simply deleting files from storage systems or removing them from public-facing platforms. However, organizations shall still ensure that this deletion is done in a manner that prevents unauthorized recovery, such as clearing data from recycle bins or temporary files.
- **Internal Data:** Use secure deletion methods to ensure data cannot be recovered after deletion. This means employing techniques that render the data irretrievable after deletion, such as overwriting the data multiple times or using specialized software designed for secure erasure. For example, the Mil Spec DoD 5220.22-M standard recommends overwriting the data with multiple passes to ensure it is thoroughly sanitized, making it unrecoverable by data recovery tools.
- **Protected Data:** Implement secure disposal practices. This includes using cryptographic erasure, which ensures that the data is encrypted in such a way that it cannot be reconstructed. Additionally, physical destruction of storage media—such as shredding hard drives or degaussing magnetic media—must be employed to guarantee that the data is permanently destroyed. Organizations shall also document these disposal activities to maintain accountability and compliance.
- **Classified Data:** Follow the highest guidelines for disposal to ensure complete destruction of both media and data. This requires rigorous protocols for handling both digital and physical media. Organizations shall utilize advanced encryption techniques for digital data and implement strict physical destruction methods for hard copies and storage devices. Additionally, it is crucial to validate that the data cannot be recovered after disposal, ensuring compliance with security requirements and protecting sensitive information.

Additional Considerations: Regular training sessions shall be conducted to ensure all personnel are aware of their responsibilities regarding data handling based on sensitivity tiers.

## 5.0 Compliance

The Data Privacy Guidelines shall take effect upon publication. The Chief Data Office may amend at any time; compliance with guidelines is strongly recommended.

## 6.0 Contact Information

Submit all inquiries and requests for future enhancements to the Chief Data Office at [data@hawaii.gov](mailto:data@hawaii.gov).

All Data related policies and guidelines can be found at [data.hawaii.gov](http://data.hawaii.gov)

## 7.0 Definitions of Key Terms

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

- **Data:** Data refers to a representation of information, including digital and non-digital formats.<sup>3</sup>
- **Records:** Records means information with fixed form and content, regardless of physical form or characteristics, created or received in the course of government activity and set aside as evidence of that activity. In databases, "records" mean a collection of related data fields.<sup>4</sup>

## 8.0 Revision History

Date	Description of Change
December 16, 2024	To be reviewed by the DTF

## Appendix A. Data Retention requirements by Organization.

Organization	Retention Period	Notes
--------------	------------------	-------

<sup>3</sup> NIST Privacy Framework Version 1.0. <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020.pdf>

<sup>4</sup> HRS§ 94-1.1. [https://www.capitol.hawaii.gov/hrscurrent/Vol02\\_Ch0046-0115/HRS0094/HRS\\_0094-0001\\_0001.htm](https://www.capitol.hawaii.gov/hrscurrent/Vol02_Ch0046-0115/HRS0094/HRS_0094-0001_0001.htm)

Basel II <sup>5</sup>	3-7 years of data history	
Children's Online Privacy Protection Act (COPPA) <sup>6</sup>	5 years after the child turns 13 or after the account is terminated	
Federal Information Security Management Act (FISMA) <sup>7</sup>	Minimum of 3 years	
Health Insurance Portability and Accountability Act (HIPAA) <sup>8</sup>	6 years from creation or last effective date	Applies to healthcare organizations and their business associates
Internal Revenue Service (IRS) <sup>9</sup>	3 years from the date of filing	Varies based on specific circumstances
National Endowment for the Humanities (NEH) <sup>10</sup>	3 years from the final FFR's submission date	
National Industrial Security Program Operating Manual (NISPOM) <sup>11</sup>	Max 2 years for classified material post-contract completion	
National Institute of Health (NIH) <sup>12</sup>	3 years from the date the annual FFR is submitted	
National Science Foundation (NSF) <sup>13</sup>	3 years after submission of all required reports	
North American Electric Reliability Corporation (NERC) <sup>14</sup>	3-6 years based on the compliance verification period	
Payment Card Industry Data Security Standard (PCI-DSS) <sup>15</sup>	Varies; organizations set their own requirements	
Sarbanes-Oxley Act (SOX) <sup>16</sup>	7 years after audit or review of financial statements	

<sup>5</sup> [https://www2.pacinfo.com/PDF/asigra/Asigra\\_Compliance.pdf](https://www2.pacinfo.com/PDF/asigra/Asigra_Compliance.pdf)

<sup>6</sup> <https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions>

<sup>7</sup> <https://www.congress.gov/bill/107th-congress/house-bill/3844>

<sup>8</sup> <https://aspe.hhs.gov/reports/health-insurance-portability-accountability-act-1996>

<sup>9</sup> <https://www.irs.gov/taxtopics/tc305>

<sup>10</sup> <https://www.neh.gov/sites/default/files/inline-files/Data%20Management%20Plans%2C%202019.pdf>

<sup>11</sup> <https://www.federalregister.gov/documents/2020/12/21/2020-27698/national-industrial-security-program-operating-manual-nispom>

<sup>12</sup> [https://grants.nih.gov/grants/policy/nihgps/html5/section\\_8/8.4.2\\_record\\_retention\\_and\\_access.htm](https://grants.nih.gov/grants/policy/nihgps/html5/section_8/8.4.2_record_retention_and_access.htm)

<sup>13</sup> <https://www.nsf.gov/policies/records/retention-schedule.jsp>

<sup>14</sup> [https://www.nerc.com/pa/Stand/Resources/Documents/Compliance\\_Bulletin\\_2011-001\\_Data\\_Retention\\_Requirements.pdf](https://www.nerc.com/pa/Stand/Resources/Documents/Compliance_Bulletin_2011-001_Data_Retention_Requirements.pdf)

<sup>15</sup> <https://www.pcisecuritystandards.org/>

<sup>16</sup> <https://sarbanes-oxley-act.com/>



# Open Data Guidelines

**Document No: CDO-006**

**Updated: December 8, 2024**

**Issued by: Chief Data Officer**

## 1.0 Purpose

The purpose of the Open Data Guidelines is to establish a framework for identifying, prioritizing, and managing the publication of data sets<sup>1</sup> across State of Hawaii agencies. Developed in accordance with Hawaii Revised Statutes (HRS) sections [§27-44](#) and [§27-44.3](#),<sup>2</sup> the Open Data Guidelines provide guidelines for data governance, data stewardship, and the procedures for making public data<sup>3</sup> available on the State's Open Data portal at [opendata.hawaii.gov](https://opendata.hawaii.gov) or successor website designated by the Chief Data Officer.

Technical requirements referenced in HRS section §27-44.3, including machine-readable<sup>4</sup> format specifications, metadata, and web publishing protocols, are outlined in a separate document titled the *State of Hawaii Open Data Technical Guidelines*. This separation ensures that the Open Data Guidelines and technical specifications are easily understood and referenced for better implementation.

## 2.0 Authority

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

## 3.0 Scope

### 3.1 State Agencies

The Open Data Guidelines apply to all State agencies as outlined in Section [§27-44](#), HRS:

---

<sup>1</sup> Refer to 7.0 Definitions of Key Terms

<sup>2</sup> HRS [§27.44 capitol.hawaii.gov](#) and [§27-44.3 capitol.hawaii.gov](#)

<sup>3</sup> Refer to 7.0 Definitions of Key Terms

<sup>4</sup> Refer to 7.0 Definitions of Key Terms

*“(c) Each department shall update its electronic data sets in the manner prescribed by the chief data officer and as often as is necessary to preserve the integrity and usefulness of the data sets to the extent that the department regularly maintains or updates the data sets.”*

### 3.2 Covered Use

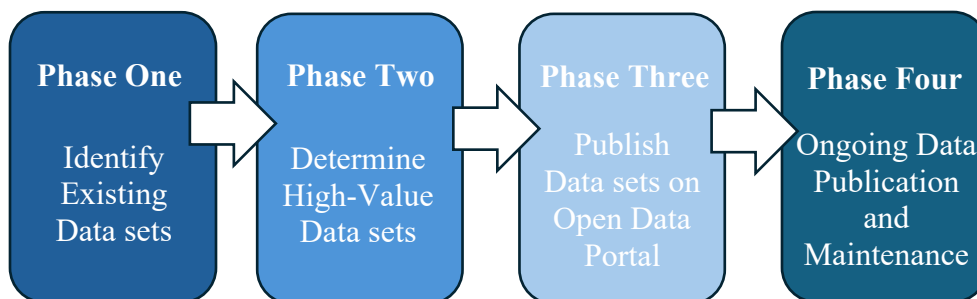
The Open Data Guidelines apply to all data assets handled by State agencies categorized as Open Data<sup>5</sup> as outlined in section 27-44 (a) and (b), HRS. Open Data Guidelines apply to all data sets published to the State’s Open Data portal at [opendata.hawaii.gov](https://opendata.hawaii.gov).

## 4.0 Information Statement

### 4.1 Requirements of the Open Data Guidelines

To enhance transparency, accessibility, and usability of statewide data, State agencies are encouraged to publish high-value<sup>6</sup> data sets on the State’s Open Data platform, [opendata.hawaii.gov](https://opendata.hawaii.gov).

To publish open data sets on the [opendata.hawaii.gov](https://opendata.hawaii.gov) site, it is recommended to follow the phases outlined below.



#### 4.1.1: Identify Existing Data sets

Conduct an assessment to identify data sets published on State agency websites unavailable on the State’s Open Data platform, [opendata.hawaii.gov](https://opendata.hawaii.gov).

#### 4.1.2: Determine Value of Data sets

Assess identified data sets to determine their value. To determine whether a dataset is considered high value, evaluate it against the following criteria/questions:

---

<sup>5</sup> Refer to 7.0 Definitions of Key Terms

<sup>6</sup> Refer to 7.0 Definitions of Key Terms



- Public Impact - Does the dataset contribute to transparency or improve public trust? How often is it accessed or downloaded by the public?
- Economic Value - Does the dataset provide insights that can drive economic development, innovation, business creation. Are businesses or researchers leveraging this data for new products/services?
- Social Impact - Does the dataset support decision-making in critical areas such as healthcare, education, housing? Can it inform policy to address societal challenges (i.e. homelessness, climate change.)
- Operational Impact for Government - Does the dataset improve internal operations, decision-making, or service delivery? Is it frequently used across multiple government agencies or sectors?

#### **4.1.3: Publish High-Value Data sets on Open Data Portal**

Publish high-value data sets from state agency websites to the State’s Open Data platform.

Apply formatting guidelines as outlined in *State of Hawaii Open Data Technical Guidelines*.

#### **4.1.4: Update Regularly**

State agencies establish a regular update schedule for data sets published on [opendata.hawaii.gov](http://opendata.hawaii.gov) to ensure data remains accurate and up to date.

## **4.2 Ownership and Responsibility**

### **4.2.1 Ownership**

State agencies retain ownership over the Open Data set(s) published to [opendata.hawaii.gov](http://opendata.hawaii.gov). Public users acquire no ownership rights to this data and all data sets published on [opendata.hawaii.gov](http://opendata.hawaii.gov) become a public resource available to anyone with access to the Internet.

The public use of the Open Data set(s) may include development of applications. In this case, the developers retain all intellectual property ownership in their applications, excluding the State data itself, whose ownership continues to reside with the state agency.

### **4.2.2 Responsibility**

State agencies that own the Open Data set(s) are responsible for all aspects of quality, integrity, and security of the dataset contents. State agencies do not relinquish control of their data to the Chief Data Office when the dataset is submitted for publication to [opendata.hawaii.gov](http://opendata.hawaii.gov).

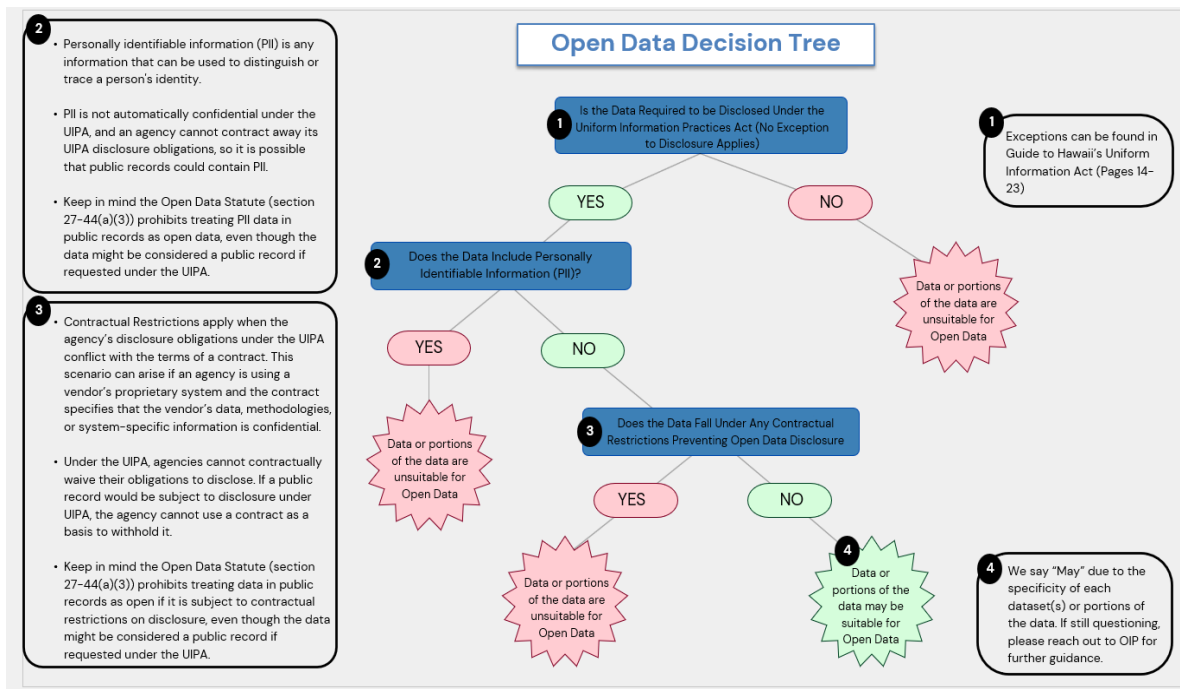
State agencies are responsible for ensuring that their submitted data meets the criteria of Open Data as outlined in the next section and has been appropriately reviewed by Office of Information Practices if needed. If a data set is not publishable in its raw format, State agencies are responsible for identifying what processing can occur to make the data publishable. State agencies are responsible for maintaining and regularly updating data sets published on [opendata.hawaii.gov](http://opendata.hawaii.gov) and meeting publication guidelines as outlined in the *State of Hawaii Open Data Technical Guidelines*.

### 4.2.3 Open Data Quality

Open Data sets should adhere to recommended data quality guidelines to ensure accurate and reliable data is accessible to the public.

## 4.3 Identifying Publishable Data

In accordance with section 27-44.3, HRS, these Guidelines include processes to determine data sets that are appropriate for online disclosure. As reviewed by the Office of Information Practices, the following graphic and steps outlined below can be followed to make the appropriate determinations. Final determination should always be made in consult with Office of Information Practices.<sup>7</sup>



<sup>7</sup> Office of Information Practices, <https://oip.hawaii.gov/>

### **4.3.1: Is the Data Required to be Disclosed Under the Uniform Information Practices Act (UIPA)?<sup>8</sup>**

**Yes** → Go to Step 2.

**No** → Data or portions of the data are unsuitable for Open Data.

### **4.3.2: Does the Data Include Personally Identifiable Information (PII)?**

**Yes** → Data or portions of the data are unsuitable for Open Data.

**No** → Go to Step 3.

#### **Considerations:**

- Personally identifiable information (PII) is any information that can be used to distinguish or trace a person's identity.
- The Open Data Statute (section 27-44(a)(3), HRS)<sup>9</sup> **prohibits** treating PII data in public records as Open Data, even though the record might be considered a public record if requested under the UIPA.

### **4.3.3. Does the Agency Have Contractual Restrictions that prevent Open Data disclosure?**

**Yes** → Data or portions of the data are unsuitable for Open Data.

**No** → Data or portions of the data “may” be suitable for Open Data

#### **Considerations:**

- Contractual restrictions apply when the agency’s disclosure obligations under the UIPA conflict with the terms of a contract. This scenario can arise if an agency is using a vendor’s proprietary system and the contract specifies that the vendor’s data, methodologies, or system-specific information is confidential.
- Under the UIPA, agencies cannot contractually waive their obligations to disclose. If a public record would be subject to disclosure under UIPA, the agency cannot use a contract as a basis to withhold it.

---

<sup>8</sup> Hawaii Uniform Information Practices Act, <https://oip.hawaii.gov/wp-content/uploads/2024/08/August-2024-UIPA-Manual-Final.pdf>

<sup>9</sup> HRS [§27-43 capitol.hawaii.gov](https://www.capitol.hawaii.gov/statutes/title27/chapter27-43.html)

- The Open Data Statute (section 27-44(a)(3),HRS)<sup>10</sup> **prohibits** treating data in public records as Open Data if it is subject to contractual restrictions on disclosure, even though the data might be considered a public record if requested under the UIPA.

## 5.0 Compliance

The Open Data Guidelines shall take effect upon publication. The Chief Data Officer may amend at any time; compliance with Guidelines is strongly recommended.

## 6.0 Contact Information

Submit all inquiries and requests for future enhancements to the Chief Data Office at [data@hawaii.gov](mailto:data@hawaii.gov)

Additional data related Guidelines can be found at [data.hawaii.gov](http://data.hawaii.gov).

## 7.0 Definitions of Key Terms

Definitions have been taken from State’s Open Data portal, [opendata.hawaii.gov](http://opendata.hawaii.gov), or defined by other Open Data documents as listed in the related documents and sources section of the Open Data Guidelines.

- **Data:** Means final versions of statistical or factual information in:
  - In alphanumeric form reflected in a list, table, graph, chart, or other non-narrative form, that can be digitally transmitted or processed; and
  - Regularly created or maintained by or on behalf of and owned by a department that records a measurement, transaction, or determination related to the mission of that department.<sup>11</sup>
- **Data set:** Means a named collection of related records on an electronic storage device, with the collection containing individual data units organized or formatted in a specific and prescribed way, often in tabular form, and accessed by a specific access method that is based on the data set organization; provided that a data set shall not include any data that is protected from disclosure under applicable federal or state law, or contract, or data that is proprietary.<sup>12</sup>
- **High-value data:** Data qualifies as high-value if it can be used to increase agency accountability and responsiveness; improve public knowledge of the agency and its operations; further the core mission of the agency; create economic opportunity; or respond to need and demand as identified through public consultation.<sup>13</sup>

---

<sup>10</sup> HRS [§27-43 \(capitol.hawaii.gov\)](http://capitol.hawaii.gov)

<sup>11</sup> Act 263 SLH 2013 [https://www.capitol.hawaii.gov/sessions/session2013/bills/HB632\\_CD1\\_.pdf](https://www.capitol.hawaii.gov/sessions/session2013/bills/HB632_CD1_.pdf)

<sup>12</sup> Act 263 SLH 2013 [https://www.capitol.hawaii.gov/sessions/session2013/bills/HB632\\_CD1\\_.pdf](https://www.capitol.hawaii.gov/sessions/session2013/bills/HB632_CD1_.pdf)

<sup>13</sup> The U.S. National Archives and Records Administration [archives.gov](http://archives.gov)

- **Machine-readable:** Refers to information or data that is in a format that can be easily processed by a computer without human intervention while ensuring no semantic meaning is lost.<sup>14</sup>
- **Open data:** Refers to publicly available data structured in a way that enables the data to be fully discoverable and usable by end users.<sup>15</sup>

### 8.0 Revision History

Date	Description of Change
December 16,2024	To be reviewed by the DTF

### 9.0 Related Documents and Sources

The State of Hawaii Open Data Guidelines utilizes input from several city, state and federal Open Data resources.

[1]. Act 167 SLH 2022  
[https://www.capitol.hawaii.gov/session/archives/measure\\_indiv\\_Archives.aspx?billtype=HB&billnumber=1885&year=2022](https://www.capitol.hawaii.gov/session/archives/measure_indiv_Archives.aspx?billtype=HB&billnumber=1885&year=2022)

[2]. Act 263 SLH 2013  
[https://www.capitol.hawaii.gov/session/archives/measure\\_indiv\\_Archives.aspx?billtype=HB&billnumber=632&year=2013](https://www.capitol.hawaii.gov/session/archives/measure_indiv_Archives.aspx?billtype=HB&billnumber=632&year=2013)

[3] Hawaii Senate Resolution 69  
[https://www.capitol.hawaii.gov/sessions/session2024/bills/SR69\\_.pdf](https://www.capitol.hawaii.gov/sessions/session2024/bills/SR69_.pdf)

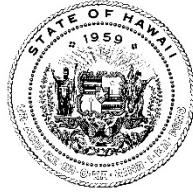
[4] Hawaii Uniform Information Practices Act <https://oip.hawaii.gov/wp-content/uploads/2024/08/August-2024-UIPA-Manual-Final.pdf>

[5]. Open Data Policy and Technical Standards Manual for the City and County of Honolulu  
[https://data.honolulu.gov/dataset/Open-Data-Policy-and-Technical-Standards-Manual-fo-uuax-nfka/about\\_data](https://data.honolulu.gov/dataset/Open-Data-Policy-and-Technical-Standards-Manual-fo-uuax-nfka/about_data)

[6]. Open Government Data.gov <https://data.gov/open-gov/#:~:text=The%20OPEN%20Government%20Data%20Act%20makes%20Data.gov%20a%20requirement,in%20the%20Data.gov%20catalog.>

<sup>14</sup> Federal Enterprise Data Resources [Resources.data.gov](https://resources.data.gov)

<sup>15</sup> Executive Office of the President [https://www.whitehouse.gov/wp-content/uploads/legacy\\_drupal\\_files/omb/memoranda/2013/m-13-13.pdf](https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/memoranda/2013/m-13-13.pdf)



## GenAI<sup>1</sup> Assistant Technologies Usage Guidelines

**Created date: November 18, 2024**

**Last Update date: December 5, 2024**

**Issued by: Chief Data Officer**

### General Guidelines for all GenAI tools

1. **FREE GenAI tools are NOT SECURE!** When utilizing these tools, verify whether you are using a State licensed or free version.
2. **Avoid** uploading/inputting non-public work-related data to any free GenAI tool as it could become publicly available.
3. If non-public data is accidentally entered into a free GenAI tool, notify your departmental IT and security lead immediately.
4. Human oversight must be applied in every GenAI use. GenAI users must review all content generated by GenAI tools before publishing. Human oversight must ensure the accuracy and fairness of the results and ensure the GenAI tools use accurate and updated information.
5. For each State licensed GenAI tool, please refer to the “Tool Specific Guidelines” section to reference detailed information regarding usage of these technologies. If the GenAI tool is not listed, treat it as a free version and follow guidance provided under “General Guidelines for all GenAI tools” (1 through 3) above.

This document will frequently be updated as additional state licensed GenAI tools are made available. It is advised to check this document regularly.

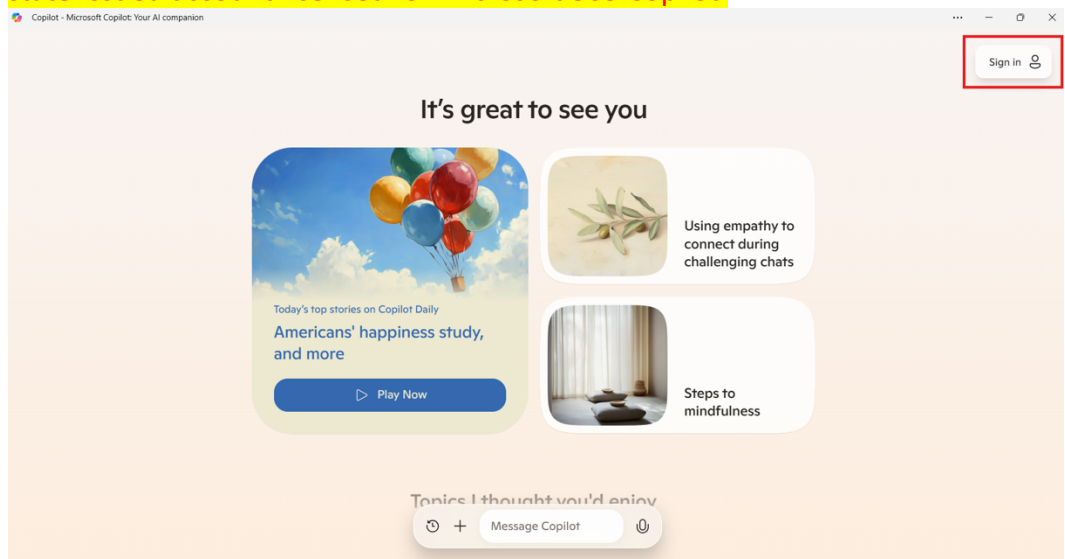
---

<sup>1</sup> GenAI refers to the class of AI models that emulate the structure and characteristics of input data in order to generate derived synthetic content which can include images, videos, audio, text, and other digital content, as defined in Executive Order (E.O.)14110. <https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/>

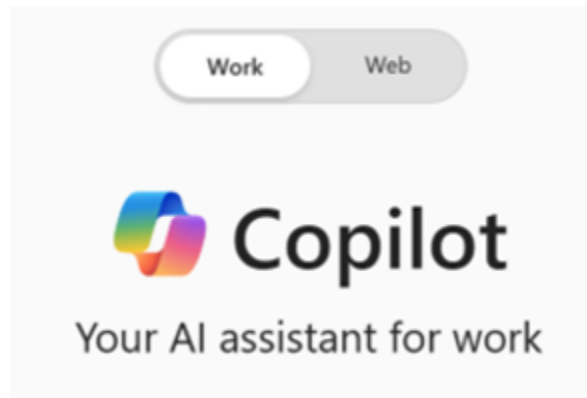
## Tool specific Guidelines

### Microsoft GenAI Copilot Guidelines

1. A free version of Microsoft Copilot on Windows may come pre-installed on state issued PCs with Windows 11. Please note that 4.1 applies to this version.
2. For those using a state licensed version of Microsoft Copilot, please refer to the table below on the “Do’s” and “Don’ts” while using this tool. Violations may result in license revocation.
  - i. To check whether you are using a free or licensed version of a Microsoft GenAI Copilot tool, please see the information below: **You are using a free version of Microsoft Copilot if you are not signed into the product with a state-issued account licensed for Microsoft 365 Copilot.**



- ii. Signing into Microsoft Copilot with a personal account gives you access to the public version of Copilot, which is available through: [copilot.microsoft.com](https://copilot.microsoft.com).
- iii. **You are using a licensed version of Microsoft Copilot if you are signed into the product using a state-issued account with a Microsoft 365 Copilot license. Users will see an option to switch between "Work" and "Web" modes. A toggle that is similar to the one shown below should appear:**



3. Microsoft Copilot's **Work Mode** and **Web Mode** are toggles that determine the context in which the GenAI assistant operates, particularly regarding the type of data it accesses and the environment it functions within. Here's a breakdown of the two modes:
  - i. **Work Mode** is designed to focus on enterprise data and organizational content. It provides access to files, emails, chats, and documents stored within your Microsoft 365 ecosystem, such as SharePoint, Teams, or OneDrive for Business. Operating within your organization's security and compliance boundaries, it adheres to enterprise policies and protections. This mode is ideal for tasks involving sensitive or company-related information, such as drafting business documents, analyzing internal data, or summarizing team conversations.
  - ii. **Web Mode**, on the other hand, focuses on general, publicly available information from the web. It accesses online sources such as websites, public articles, or databases, rather than internal organizational data. Operating outside enterprise security environments, it relies on publicly accessible web-based resources. This mode is best suited for general queries, researching external topics, or creating content based on publicly available information.



Microsoft Copilot Usage Guidelines	
Do's	Don'ts
Use <b>Work Mode</b> by signing into your Work Account when using Copilot for business. This step is important when using online based copilot products including Copilot Bing, Edge, Windows, and Business Chat Online.	Use Web (Personal) Mode for business tasks, as it may expose sensitive data.
Ensure the <b>Enterprise Protection Shield</b> icon is visible in Copilot Web, Windows, and M365. 	Proceed with tasks if the Enterprise Protection Shield icon is not visible.
Use the <b>Work or School Results</b> page in Bing Web for business-related searches.	Rely on the All Results page in Bing Web for state-related or sensitive searches.
Use the <b>More Balanced</b> or <b>More Precise</b> output modes in Copilot Windows for higher accuracy.	Select the More Creative output mode when accuracy is critical.
Only use <b>PUBLIC DATA</b> for <b>Bing</b> or <b>Edge</b> as such data will become publicly available.	Upload non-public, confidential or sensitive data to Bing or Edge.
Routinely clear conversation history to protect any stored data.	Leave conversation history uncleared, risking exposure of sensitive information.
Review outputs critically for fairness, neutrality, and accuracy.	Assume GenAI outputs are unbiased, accurate, or final without verification.
Routinely review source data to ensure it is up-to-date and accurate.	Use outdated, incomplete, or incorrect resources as input data.
Verify Copilot's suggestions against trusted official sources.	Assume Copilot's responses are always accurate without cross-referencing.
Report outdated or incorrect references to your supervisor and departmental data leads.	Ignore instances where Copilot references outdated or irrelevant data.
Craft neutral and specific prompts free of leading language.	Use prompts with subjective, biased, or leading language which leads to bias.
Keep prompts clear, concise, and specific to the task.	Include excessive or irrelevant details in prompts.
Treat Copilot outputs as drafts and refine as needed.	Use Copilot's output verbatim without review, especially for critical communications.
Focus on essential information needed for the task at hand.	Use overly detailed or complex prompts that may confuse Copilot.

## Appendix A: Key Features for Microsoft 365 Copilot

Copilot in Microsoft 365 is application specific.

365 Application	Feature Description
<b>Word</b>	<ul style="list-style-type: none"> <li>• Generate text with and without formatting in new or existing documents.</li> <li>• Create content, summarize, ask questions about your document, and do light commanding.</li> </ul>
<b>PowerPoint</b>	<ul style="list-style-type: none"> <li>• Create a new presentation from a prompt or Word file using enterprise templates.</li> <li>• Summary and Q&amp;A</li> <li>• Add slides, pictures, or make deck-wide formatting changes.</li> </ul>
<b>Excel</b>	<ul style="list-style-type: none"> <li>• Get suggestions for formulas, chart types, and insights about data in your spreadsheet.</li> </ul>
<b>Loop</b>	<ul style="list-style-type: none"> <li>• Create content that can be collaboratively improved through direct editing.</li> </ul>
<b>Outlook</b>	<ul style="list-style-type: none"> <li>• Get coaching tips and suggestions on clarity, sentiment, &amp; tone, and an overall message assessment and suggestions for improvement.</li> <li>• Summarize an email thread to quickly understand the discussion.</li> <li>• Pull from other emails or content across Microsoft 365 that the user already has access to.</li> </ul>
<b>Teams</b>	<ul style="list-style-type: none"> <li>• Summarizes up to 30 days of chat content, using only the current thread for responses. Ask questions or use prewritten prompts, with clickable citations to the source content. Conversations take place in a side panel and close when the panel does.</li> <li>• Uses the transcript in real-time to answer questions and only uses the transcript and knows the name of the user typing the question. Can type any question or use predetermined prompts. Answers questions only related to the meeting conversation from the transcript. The user can copy/paste an answer and access Copilot after the meeting ends.</li> <li>• Automates important administrative tasks of a call, like capturing key points, task owners, and next steps. It supports voice over Internet Protocol (VoIP) and public switched telephone network (PSTN) calls.</li> <li>• Generate ideas, organize ideas into themes, create designs based on ideas, and summarize whiteboard content.</li> </ul>
<b>OneNote</b>	<ul style="list-style-type: none"> <li>• Use prompts to draft plans, generate ideas, create lists, and organize information to help you find what you need.</li> </ul>
<b>Forms</b>	<ul style="list-style-type: none"> <li>• Use prompts to draft questions and suggestions that help you create surveys, polls, and other forms.</li> </ul>

## Appendix B: Key Features for Microsoft Business Chat Copilot

**CAUTION:** When using Business chat online through Microsoft.com/copilot, this is a **FREE** software version intended for use with **public data only**. Please ensure that no private or sensitive information is input.

To enable full functionality and activate work mode for enterprise-level protections, you must **sign in** with your **work account and have a valid Microsoft Copilot License**.

Users can interact with Business Chat using open-ended prompts. Business Chat can be accessed through Teams (chat), Microsoft 365 apps, or by going to [microsoft.com/copilot](https://microsoft.com/copilot).

Feature	Description	Prompt Example
<b>Work Across Multiple Apps</b>	Connects to Microsoft apps like Teams, Outlook, and Word, allowing you to access information from different tools in one place.	<i>Example:</i> "Find the latest report in Word and summarize it in Teams."
<b>Ask Questions and Provides Answers</b>	Ask open-ended questions and get responses based on the current context of your work.	<i>Example:</i> "What were the key points discussed in today's meeting?"
<b>Helps with Tasks and Documents</b>	Create, manage, and track tasks and documents, pulling information from multiple sources like emails or files.	<i>Example:</i> "Create a task in Teams based on the action items in my Outlook email."
<b>Summarize Data</b>	Helps you understand key points and make decisions by summarizing data and content from different tools.	<i>Example:</i> "Summarize the recent customer feedback from the latest reports."
<b>Supports Teamwork</b>	Makes it easier to share information and collaborate with your team by pulling data from various sources.	<i>Example:</i> "Share the meeting notes from OneNote with the project team in Teams."

## Appendix C: Key Features for Microsoft Edge Copilot

**CAUTION:** This is a **FREE** software version intended for use with **public data only**. Please ensure that no private or sensitive information is input.

To enable full functionality and activate work mode for enterprise-level protections, you must sign in with your **work account and have a valid Microsoft Copilot License**.

A sidebar Copilot tool in Microsoft Edge provides assistance-based on opened tabs.

Feature	Description	Prompt Example
<b>Web Page Summarization</b>	Summarize long web pages into concise summaries.	<i>Example:</i> "Summarize the key points of this article about climate change policies."
<b>Text Generation from Web Content</b>	Generate new text based on the content of a web page.	<i>Example:</i> "Generate a summary for a blog post on digital marketing trends."
<b>Writing Assistance in Forms and Text Boxes</b>	Copilot assists with drafting, editing, and enhancing writing in web-based forms, comment sections, or social media posts.	<i>Example:</i> "Help me write a professional comment on a news article about healthcare reform."
<b>Search Assistance</b>	Refine or expand search queries, helping you find more relevant results based on what you're researching.	<i>Example:</i> "Refine my search for software development tools to include only those suitable for small businesses."
<b>Extract Key Data From Web Pages</b>	Extracts and presents key data or statistics from web pages for easy reference.	<i>Example:</i> "Extract the most important statistics from this report on global economic trends."

## Appendix D: Key Features for Microsoft Bing Copilot

**CAUTION:** This is a **FREE** software version intended for use with **public data only**. Please ensure that no private or sensitive information is input.

To enable full functionality and activate work mode for enterprise-level protections, you must sign in with your **work account and have a valid Microsoft Copilot License**.

Web-based Copilot tool, accessible through Bing for general assistance with public web content. Copilot Bing provides a range of result features.

Feature	Description	Example of Output
<b>ALL results page</b>	If there's a relevant work or school result, it will appear at the top of the search results page, followed by relevant public web results.	<b>Work Result:</b> "Quarterly Sales Report (Internal Document)" followed by <b>Public Web Result:</b> "Best practices for sales growth strategies."
<b>WORK or SCHOOL results page</b>	This page only shows work or school results from your organization and never includes public web results.	<b>Work Result Only:</b> "Annual Budget Summary (Internal Document)" without any public web distractions or irrelevant results.

## Appendix E: Key Features for Windows Copilot

**CAUTION:** This is a **FREE** software version intended for use with **public data only**. Please ensure that no private or sensitive information is input.

To enable full functionality and activate work mode for enterprise-level protections, you must sign in with your **work account and have a valid Microsoft Copilot License**.

Windows Copilot is integrated directly into the Windows operating system, and accessible through the taskbar or windows side bar on laptop/desktop. Copilot Windows provides customized result features based on subject area.

Feature	Description	Example of Output
<b>More Creative</b>	The output will be more imaginative and inventive but might lack in accuracy.	For a project proposal intro: "Imagine a world where data flows seamlessly, empowering every decision with groundbreaking insights!"
<b>More Precise</b>	The output will be highly accurate and detailed but may not be as creative.	For a project proposal intro: "This project aims to integrate data from 15 state agencies, improving efficiency by 25% within one year."
<b>More Balanced</b>	The output will be a blend of both creativity and accuracy, balancing the two aspects.	For a project proposal intro: "Harnessing data from 15 state agencies, this initiative will drive a 25% efficiency boost, unlocking new insights."