Data Retention Guidelines

Document No: CDO005
Updated: December 8, 2024
Issued by: Chief Data Officer

1.0 Purpose

The purpose of the Data Retention Guidelinesis to establish common guidelinesfor data retention across State of Hawaii agencies.

2.0 Authority

Hawaii Revised Statutes (HRS)[1] Section §27-44, established within the Office of Enterprise Technology Services, in the Department of Accounting and General Services, and under the authority of the Chief Information Officer, the Chief Data Officer to develop, implement, and manage statewide data policies, procedures, standards, and guidelines. HRS §27-44 also established a Data Task Force to assist the Chief Data Officer in developing the State's data policies, procedures, and standards.

3.0Scope

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.

[1] HRS §27-44. 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[2] 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 data. 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

[2] 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 Officer in the Office of Enterprise Technology Services, Department of Accounting and General Services, at data@hawaii.gov.

All Data related policies and guidelines can be found at 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.[3]
- **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.[4]

8.0 Revision History

Date	Description of Change
December 16, 2024	Approved by the State Data Task Force

Appendix A. Data Retention requirements by Organization.

Organization	Retention Period	Notes

[3] NIST Privacy Framework Version 1.0. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020.pdf
[4] HRS§ 94-1.1. https://www.capitol.hawaii.gov/hrscurrent/Vol02_Ch0046-0115/HRS0094/HRS_0094-0001_0001.htm

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

[5] https://www2.pacinfo.com/PDF/asigra/Asigra_Compliance.pdf
[6] https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions
[7] https://www.congress.gov/bill/107th-congress/house-bill/3844
[8] https://aspe.hhs.gov/reports/health-insurance-portability-accountability-act-1996
[9] https://www.irs.gov/taxtopics/tc305
[10] https://www.neh.gov/sites/default/files/inline-files/Data%20Management%20Plans%2C%202019.pdf
[11] https://www.federalregister.gov/documents/2020/12/21/2020-27698/national-industrial-security-program-operating-manual-nispom
[12] https://grants.nih.gov/grants/policy/nihgps/html5/section_8/8.4.2_record_retention_and_access.htm
[13] https://www.nsf.gov/policies/records/retention-schedule.jsp
[14] https://www.nerc.com/pa/Stand/Resources/Documents/Compliance_Bulletin_2011-001_Data_Retention_Requirements.pdf
[15] https://www.pcisecuritystandards.org/
[16] https://sarbanes-oxley-act.com/