Retention & Disposal of Customer Data Policy

Version number: 2.2

12 November 2024

NSW GOVERNMENT

Service NSW

Contents

1 Policy Statement

The protection of customer data is a paramount consideration for Service NSW ensuring the delivery of our core values of *Accountability*, *Integrity* and *Trust*.

This Policy outlines the principles and responsibilities of Service NSW in the retention and disposal of data that represents individuals and businesses – i.e. our customer data. The document is best understood within the framework of Service NSW's Data Governance Strategy and our vision to *manage data as an asset to best serve our customers*.

It aims to safeguard personal and sensitive data while recognising the value of customer data to enhance services by establishing policy, business rules and procedures to describe how the retention and disposal of customer data is managed. It also supports 'by design' considerations to enable the organisation to account for the disposal of customer data in accordance with legal obligations and accountability requirements.

By establishing policy, business rules and procedures, we can support all stakeholders in:

- Understanding the flow of information — from creation to disposal — and enabling a holistic approach to the retention and disposal of customer data
- Recognising the multidimensional nature of data retention and disposal, and supporting interdependencies and collaboration among key stakeholders to meet all legal, regulatory and business requirements
- Making day-to-day management of information more efficient and compliant with transparent and clearly defined governance policies and processes

1.1 Principles

This policy sets overarching principles that outline intent and expectations for consistent decision-making around the appropriate retention and disposal of customer data:

Customer is at the centre of everything we do

Customer data is retained only for the **purpose** for which it may be lawfully used

As custodians, we **manage** customer data across the data lifecycle

1.2 Objectives

The key objectives of the policy are:

- **Set overarching principles** to guide design and service decision making
- **Understand the requirements** of policy and legislation applicable to the organisation
- **Provide instructions** for the retention and disposal of customer-based records
- **Outline considerations** for product teams to ensure that solutions enable the proper appraisal of records for preservation or disposal

1.3 Scope

This policy applies to customer data and associated transactions owned and managed by Service NSW regardless of the environment or digital system used.

1.3.1 Audience

All staff, including outsourced service providers and contractors, who manage the data of individuals and businesses (customers) created or stored by Service NSW.

1.3.2 Out of Scope

- Any data where the ownership, collection or retention responsibilities have been defined to be outside of Service NSW. This can be a DCS agency, or any external data ownership as specified in Partnerships Agreements.
- Internal Service NSW records and data which are addressed by an alternate document – Service NSW's Retention and Disposal Standard.

1.4 Ethical Conduct

All activities must be conducted in an ethical and transparent manner and comply with the values, principles and articles in the Code of Conduct.

As a public sector employee, we have a special obligation to act in the public interest when carrying out our duties. Our code is a public statement that provides specific guidance on values and standards of conduct expected across our organisation.

It is essential for us to behave ethically while serving the people of NSW. The Code of Ethics and Conduct is our department's guiding principle to operate ethically.

When collecting, using or storing customer information, we must apply the values and principles of the Ethical Framework of *Integrity, Trust, Accountability* and *Service.*

2 Policy Components

2.1 Responsibilities

Each of the following parties has specific assigned responsibilities under this policy:

- Platform Owners or Product Managers (Data Custodians)
- Portfolio or Business Unit Directors (Data Owners)
- Privacy Team
- Information & Data Governance Team
- Digital Services Senior Leadership Team (SLT)
- Data Governance Committee
- Executive

2.1.1 Platform Owners or Product Managers (Data Custodians)

- Ensure service and product designs comply with this policy
- Ensure provisions for data management including disposal are included in system design and ongoing maintenance of products and applications
- Apply data observability and monitoring on data lineage to determine relationships between data assets
- Consult Privacy and Information Governance
- Engage with Data Owners for authorisation on disposal activities

2.1.2 Portfolio Directors (Data Owners)

- Accountable for the implementation of this Policy for data assets within their portfolio
- Work across Partnership agreements to delivery to ensure retention commitments met
- Ensure that the programs are regularly reviewed for retention or destruction, aligning with the privacy principle to only retain records for as long as they are required
- Advise data custodians when records are being appraised for disposal or retention
- Work with Information Governance & Privacy to authorise Disposal of records
- Provide advice on any records that need to be retained beyond the retention to meet continued investigative, fraud or other business requirements

2.1.3 Manager, Privacy

- Provide leadership and advice as per the Privacy Management Framework
- Consult on appraisal processes

2.1.4 Manager, Information and Data Governance

- Administer and update this policy

- Communicate the legislative compliance requirements of the *State Records Act 1998*
- Interpret and implement records retention and disposal authorities
- Consult on appraisal processes
- Escalates issues to Data Governance Committee

2.1.5 Data Governance Committee

- Endorse this policy to Executive
- Approve batch deletion processes of customer data
- Provide strategic support to the implementation of this policy including funding and business unit prioritisation
- Assesses risks with retaining data beyond its minimum requirement against business priorities

2.1.6 Digital Services Senior Leadership Team (SLT)

- Oversee implementation of this Policy within Digital Product Teams
- Provide strategic support in prioritising Policy's implementation within Digital Product Teams
- Ensure policy's requirements are captured in Divisional Plans and standards and defaults

2.1.7 Executive

- Authorise the requirements of this policy
- Ensure compliance and conformance to this policy

2.2 Authorities

2.2.1 Responsibilities under the *Privacy and Personal Information Protection Act 1988 (PPIPA)*

The Service NSW Privacy team provide advice on the appropriateness of the collection of customer data and how the organisation demonstrates the application of the Information Protection Principles.

These responsibilities and activities are addressed through Service NSW's Privacy Management Framework with further community information available through the Service NSW Privacy Management Plan..

These responsibilities align with the principle:

*Customer data is retained only for the **purpose** for which it may be lawfully used*

2.2.2 Responsibilities under the *Health Records and Information Protection Act (HRIPA)*

The purpose of this Act is to promote fair and responsible handling of health information by protecting the privacy of an individual's health information.

As with our obligations under PPIPA, our responsibilities are addressed through Service NSW's Privacy Management Framework..

This aligns with the principle:

*Customer data is retained only for the **purpose** for which it may be lawfully used*

2.2.3 Responsibilities under the *State Records Act 1998*

The *State Records Act 1998* creates a statutory framework for public offices to:

- Make and keep records that fully and accurately document their operations
- Ensure that records and information are stored in conditions appropriate to their format and preservation requirements
- Ensure that records and information are kept for as long as they are needed for business, legal and accountability requirements
- Ensure that records and information are systematically and accountably destroyed when legally appropriate to do so.

Our responsibilities are detailed in the DCS Records Management Policy which aligns with the principle:

*As custodians, we **manage** customer data across the data lifecycle*

2.3 Implementing Data Lifecycle Management

For effective management of records and information, it is important to consider how information will be protected during the stages of its lifecycle. This is especially true of customer data.

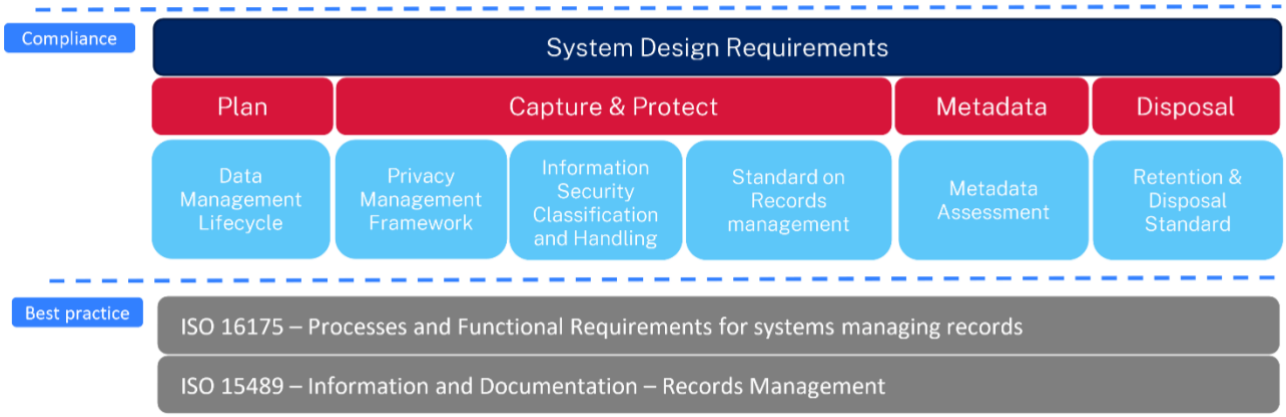
There can exist a tension between the Privacy requirement of retention – *which is to keep personal information for no longer than is necessary* - and the Records requirement - *which is to keep full and accurate records of the activities of the office*.

The best way to overcome this is to design systems that enable the appraisal, sentencing and destruction of data once the minimum retention requirements are met.

While the DCS Standard for requests to delete Personal Information is available to guide one-off deletion requests from the community, the following section defines system requirements that will enable a more holistic and automated retention and disposal process.

2.3.1 Architectural Design

Figure 1 - System Design Resources



For digital services, there are several functional requirements for software used to create and manage digital information. For more information in design approach refer to DCS System Design Requirements, as well as supporting Standards that enable 'by design' considerations.

The following table defines the specific activities and requirements for 'by design' considerations when retaining and disposing customer data:

Table 1: Architectural Design activities

Activity	Requirement	Comments
Determine data needs and requirements across the asset lifecycle	As part of formal project documentation: • Define the system which will represent the 'Source of Truth' • Define the information security classification requirements • Define the storage location of the data • Define the Data Owners of the asset • Define lineage and dependencies of the data • Define accessibility requirements	All requirements cannot not be known or planned for at the outset, but a structured approach from the beginning will assist in further definition as future requirements become known.
Apply recordkeeping system design characteristics to 'Source of Truth' systems	• The solution supports the management of digital records as a core component of the process • Enable the capture of metadata at any time during the record's existence • Be able to apply classifications at individual object/or aggregated level • Be able to allocate an appropriate retention and disposition period in the system for records	To avoid the risk of over retention, it is good practice to retain data in single source of truth system. By retaining multiple copies of data from a transaction, we are duplicating data and inherently increase the risk of unauthorised use, modification, and disclosure. If required to have duplicate, tag as duplicate.
Data is accessible	• Determine functionality that provides customer autonomy in what they would like to do with their information. • Explain to customers through Privacy Collection notices, the requirements in the retention and disposal of customer records • Be able to integrate and interoperate with other systems • Be able to update other systems when a record has been deleted • Apply security and access protocols to protect the content and their metadata from unauthorised access, alteration, or destruction	Digital entry point must be personalised and humanised to build trust with a customer who may never meet the frontline teams. This supports compliance with Information Protection Principles such as Transparent (IPP 6), Accessible (IPP 7), Alteration (IPP 8) and Accurate (IPP 9). Further, establishing interoperable controls will support downstream notifications of transactions or account deletions and allows a centralised process of account deletions.

Activity	Requirement	Comments
The system supports controlled retention, appraisal, and destruction activities	• Be able to sentence data by applying scheduled disposal triggers • Allow a range of disposition triggers, eg. Date of last retrieval, closing date of record • Be able to update retention periods due to changes of legal or business requirements • Configure suitable metadata to capture disposal information • Be able to store the status of the record as being 'Deleted' or 'Transferred' • Provide consistent security controls across the disposal activity as per their Information Security Classification	NSW State Records provide system design guidelines which inform what is expected in a disposal activity. These requirements align to *AS ISO 15489.1: 2017 Information and documentation - Records management* which State Records considers as a Code of Best practice.
Establish business processes on the disposal of records	• Document data lineage so entity relationships are understood • Consult Information Governance & Privacy when appraising records or applying retention • Establish roles that have the permission to delete the records or process disposal	A key step in creating successful data governance is in establishing business processes that support defensible disposal of records and information. To achieve defensible disposal, Digital Services teams must be able to collaborate closely and transparently with Information Governance, Privacy and Business Owners.
Preference automated solution	• Automatically flag records as eligible for disposal • Pause disposition, preventing records from being disposed of (such as legal holds) • Removing legal holds	Automatically applying retention schedules and legal holds to data sources ensures the consistent disposition of unnecessary data whilst validating hold requests and compliance efforts.
Provide evidence of deletion	• The system produces reports relating to deletion of records/data and its associated metadata including: - Unique ID of records and information deleted, - Date and time of deletion - Action done by	The Standard on Records Management highlights that effective management of records and information underpins trustworthy, useful and accountable records and information. As such, organisations must account for the disposal of records, ensure that disposal is in accordance with current authorised authorities and the disposal is documented.
Build Approval Workflow	• Data Custodian collects evidence records have met minimum requirements • Engage Information Governance, Privacy and Data Owners to notify records have met retention periods	For further instructions on the disposal process, please refer to the SNSW Retention & Disposal Standard.

Activity	Requirement	Comments
	• Submit list and Certificate of Destruction to Data Owner and Information Governance Manager for approval to destroy • Update retention periods for records requiring to be maintained • Destroy or transfer all copies of records approved for destruction	
Observability and Monitoring	• Enable key staff to monitor whether records are approaching retention periods or exceeded retention periods • Enable key staff to identify relationships and dependencies which would prevent an account from being deleted. • Data assets are catalogued – with retention periods – in Enterprise Data Catalogue	

2.3.2 Retention Periods

State Records NSW provide the *minimum* retention requirements which helps public offices determine the appropriate balance of not storing records longer than necessary whilst maximising their ability to retrieve records. For more information on Service NSW's approach to Retention & Disposal of records, or the application of retention periods, refer to the Service NSW Retention and Disposal Standard

2.3.2.1 Reference Map for Retention on Transaction Types

This table refers to the most common types of information and data assets that Service NSW manages and maps them against State Records disposal authorities. For assets that aren't included the Information and Data Governance Team can provide technical support to map the appropriate authority.

Function	Function Code	Service NSW Retention Period	Trigger	Retention Authority	Action
Hold	HOLD	-	-	-	Hold for further instruction
Fraud Investigations	FRAUD	10	Last Action Date (On Action Complete)	FA425 1.3.3	Retain minimum of 10 years after action completed, then destroy
Customer accounts ***Includes customer profile information and preferences; authentication and identity assurance records***	DAV	30 days	Deactivation	FA425 1.1.1	Retain a minimum of 30 days after an account is permanently deactivated, or once the associated customer transactions have met their minimum retention periods, whichever is longest, then destroy (see Figure 2 – Account Lifecycle Model)

Proof of Identity Documents	POI		After verification process	GA28 2.6.8	Retain copy until verification and validation process is complete, then destroy
Notifications	NO	2	Last action Date	FA425 1.2.3	Retain minimum of 2 years after administrative or reference use ceases
Notifications – Financial *Communication to the customer.* *Examples, tax invoices, fines*	NO:FIN	7	After End of Financial Year	GA28 7.1.5	Retain minimum of 5 years after end of financial year in which record was created
Grants, Vouchers & Rebates	GVR				
Vouchers *Small value vouchers, eg. Creative Kids*	GVR:VO	3	Created Date	FA425 1.3.2	Retain minimum of 2 years after action completed, then destroy
Rebates & Payments *Large values, manual assessment, evidence or approval required, eg. Fertility Treatment rebate*	GVR:RP	10	Last action date	FA425 1.3.1 - SERVICE DELIVERY - Grant Management	Retain minimum of 10 years after action completed, then destroy
Case Notes	CN				

Case Management Files	CN:FIL	7	Last action date	FA425 1.2.1	Retain minimum of 7 years after action completed, then destroy
Logs	LOG				
Security Logs *Record capturing an event related to interactions between an information systems and either another information system or an individual's request.*	LOG:SEC	7	Last action date	GA28 16.24.5	Retain minimum of 7 years after action completed, then destroy
Non-Security Log *Record of an event related to an information system's internal function, which is independent of requests made by another information systems or individual parties' interactions.*	LOG:TR	1	Last action date	GA28 20.4.6	Retain in accordance with the organisation's requirements, then destroy
Financial Logs *Logs which contain a record of financial transactions*	LOG:FIN	7	Round (Last action date to end of financial year)	GA28 7.1.1	Retain minimum of 7 years after end of financial year in which transaction was completed, then destroy
Batch Reports	LOG:BAT	0	-		No minimum retention requirements. May be disposed once administrative or facilitative reference ends, under Normal Administrative Practice.
Analytics of Customer Activities *e.g. Digital Products and Services uptake, Service*	ANAL	3	Last action date	GA28 2.20.2	Retain minimum of 3 years after action completed, then destroy

Centre visitation, Website visitation, Sentiment Analysis					
Customer research *Includes notes, plans, and recordings relating to customer consultation and research for the development of programs and services*	RES	0	Last action date	GA28 17.12.2	No minimum retention. Retain until administrative or reference use ceases, then destroy. Records with Personal Information should be de-identified as soon as possible.

Refer to Section 4 Account Lifecycle Conceptual Model for the defined mapping of account statuses against retention periods.

2.3.3 Data that has already met minimum requirements

Despite advances in technology for storage of large amounts of data, we are still required to implement defensible disposal processes. At Service NSW, we have several means to lawfully dispose of records. Mostly this is through the retention and disposal authorities mentioned above.

Another means is in accordance with the Normal Administrative Practice (NAP) provisions of the Act which allow for the disposal of certain types of facilitative and duplicate records. Examples of NAP records include:

- Test data
- Duplicated data
- Batch reports

Disposal actions should be undertaken for any records identified as having met their minimum retention periods. The SNSW Retention & Disposal Standard provides instructions and the Certificate of Destruction template.

2.3.4 Data that cannot be destroyed

It is expected that only in very limited circumstances would it not be possible for an organisation to destroy personal information held in electronic format. Situations where this might occur include:

Where the organisation is aware of possible legal action (including legal discovery, court cases, formal applications for access) where the record may be required as evidence.

- Where the records are required to be transferred to another agency
- Where there are no Retention & Disposal Authorities which cover the function of the record
- Disposal Alerts, where records are required for Inquiries and Royal Commissions
- Where the records are required to be held for investigative or legal purposes
- Where the context (the knowledge necessary to sustain the records meaning) would be greatly impacted

In these cases, it is important to engage Information Governance and Privacy who can advise the best course of action. Considerations and course of action may include:

- Obtain authority from State Records for the disposal of the record
- De-identifying elements of the record to minimise the risk of data breach
- Applying a different retention authority which reflects the updated status of the record

3 Monitoring, implementation and exceptions

3.1 Monitoring and implementation

As a result of the implementation of this Policy, the following activities will be overseen by the Information and Data Governance Team:

1. Advice to business and product teams who manage customer data to explain the policy's requirements and application to their operating context
2. Assurance over deletions through compilation of metrics including assets sentenced and deleted, data storage cost avoidance and data breach cost avoidance
3. Yearly audit over business and product teams' data holdings to assess compliance with Policy's requirements and address over-retention issues

3.2 Exceptions

The retention periods in section 2.3.2.1 primarily specify a minimum period. Records may be retained longer if the Data Owner advises a continuing business need to the Manager, Information and Data Governance who will escalate any concerns to the Data Governance Committee. The Committee will assess the risk of retaining these records against the applied business need.

4 Account Lifecycle Conceptual Model

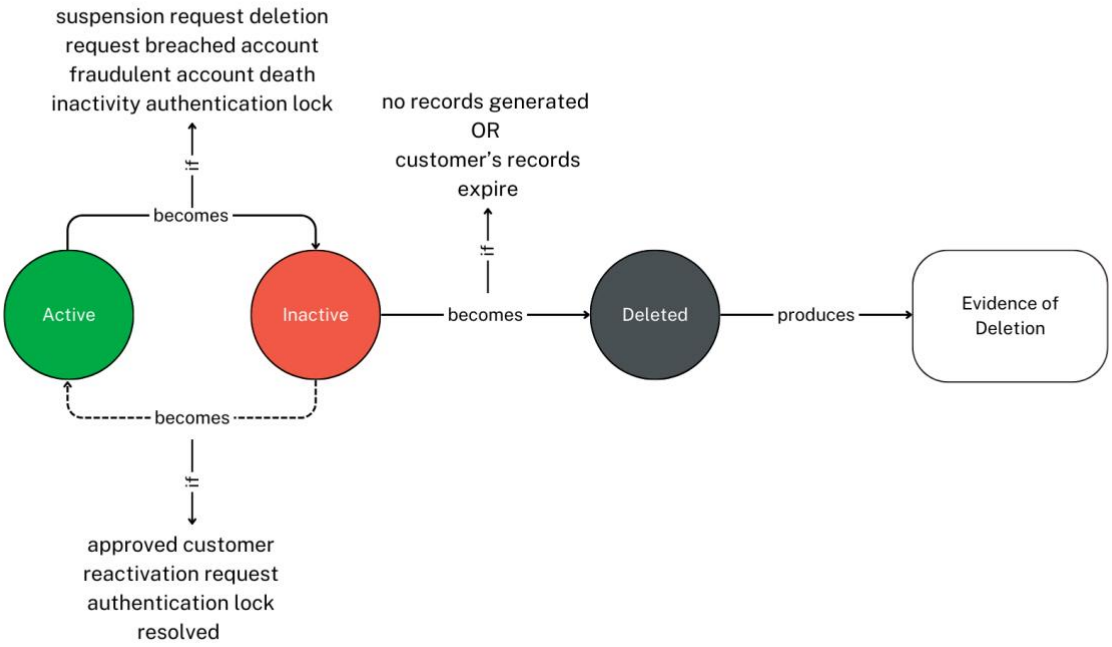


Figure 2. Account Lifecycle Conceptual Model

5 Glossary

Term	Definition	Source
Administrative Use	Ephemeral or transitory data that is of a trivial nature or short-term value that they do not contribute to ongoing business functions.	
Attribute Attribute(s)	An item of information or data associated with a subject. Examples of attributes include information such as name, address, date of birth, email address, mobile number, etc.	01 Glossary of Abbreviations and Terms, Digital Identity, Australian Government Trusted Digital Identity Framework Release 4.8 – Feb 2023
Audit Log	A chronological record of system activities including records of system access and operations performed.	01 Glossary of Abbreviations and Terms, Digital Identity, Australian Government Trusted Digital Identity Framework Release 4.8 – Feb 2023
Customer Account	A customer account is a record of an individual’s or business’s interactions and transactions with Service NSW including authentication and identity assurance. It includes identifiable information such as name, address, contact details, and preferences.	
Customer Data	A data entity with one or more attributes that represent an individual or business.	
De-identify	Deidentified information is information from which the identifiers about the person have been permanently removed, or where the identifiers have never been included.	

Destroy *Destruction* *Destruct* See also Purge	Process of eliminating or deleting a record, beyond any possible reconstruction. The process includes destroying all copies of the record.	Adapted from AS ISO 15489.1 2017, Part 1 Clause 3.7 Glossary of recordkeeping Terms State Records NSW (Accessed 2023)
Disposal	The destruction of records or their transfer to another organisation, for example, State Archives and Records Authority of NSW archives. Includes a range of processes associated with implementing records retention, destruction or transfer decisions which are documented in disposition authorities or other instruments.	Records Management Policy (DCS) Glossary of Recordkeeping Terms | State Records NSW AS ISO 15489.1 2017 Part 1, Clause 3.8
Digital Identity	A distinct electronic representation of an Individual which enables that Individual to be sufficiently distinguished when interacting online with services. A Digital Identity may include Attributes and Assertions which are bound to a Credential. A Digital Identity can be used by Individuals to access online services.	Digital ID Bill; Accreditation Rules; Digital ID Rules (digitalidentity.gov.au)
Purge *purging*	Purging is the process of completely removing data from the storage media such that it cannot be recovered.	DAMA International. (2017) DAMA-DMBOK Data Management Body of Knowledge 2nd Edition, Technics Publications, New Jersey
Personal Information	Information or an opinion (including information or an opinion forming part of a database, whether or not recorded in a material form) about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion	NSW Privacy and Personal Information Act (PPIPA)
Product	A resource produced for customers to use or exchange for value.	Service NSW Business Glossary
Service	An offering through which a customer can find information or complete a transaction.	Service NSW Business Glossary
Transaction Record	A record, either system or manually generated, including the specific details of when and how a transaction took place.	Managing scanned customer documentation

6 Related Policies and Documents

Issuer	Type	Document Name
Information Privacy Commission	Legislation	Privacy and Personal Information Protection Act 1998
Information Privacy Commission	Legislation	Health Records and Information Privacy Act 2002
International Standards Organization (ISO)	Standard	ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements
NSW State Records	Legislation	State Records Act 1998
NSW State Records	Regulation	State Records Regulation 2015
NSW State Records	Mandatory Standard	Standard on Records Management
Department of Customer Service	Policy	DCS Records Management Policy
Department of Customer Service	Policy	Information Security Policy
Department of Customer Service	Policy	NSW Cyber Security Policy
Digital.nsw	Guideline	Information Classification, Labelling and Handling Guidelines
Service NSW	Strategy	Data Governance Strategy 2023-2026
Service NSW	Plan	Data Breach Response Plan
Service NSW	Standard	Retention and Disposal Standard
Service NSW	Standard	Information Security Classification & Handling Standard

7 References

- Department of Customer Service, (2023), NSW Cyber Security Policy 2023-2024 Version 6.0, https://www.digital.nsw.gov.au/sites/default/files/2024-02/NSW-Cyber-Security-Policy-2023-2024.pdf

- Lorrie Luellig, L. and Frazier, J., (2013), A COBIT Approach to Regulatory Compliance and Defensible Disposal, A COBIT Approach to Regulatory Compliance and Defensible Disposal (isaca.org)

- National Archives of Australia, (2023), Principle 1: Business Information is Systematically Governed, https://www.naa.gov.au/information-management/standards/information-management-standard-australian-government/principle-1-business-information-systematically-governed

- National Archives of Australia, (2023), Retaining, Managing and Disposing of data and datasets, Retaining, managing and disposing of data and datasets | naa.gov.au

- NSW State Records, (2023), Records Systems, Characteristics and Functions, https://staterecords.nsw.gov.au/recordkeeping/guidance-and-resources/records-systems-characteristics-and-functions

- NSW State Records, (2023), Standard on Records Management, Standard on records management | State Records NSW

8 Document Control

8.1 Document Approval

Name and Position	Date
Trusted and Secure Executive Leadership Team	19 September 2023
Trusted and Secure Executive Leadership Team	18 June 2024

8.2 Document Version Control

Version	Status	Date	Prepared By	Approved By	Comments
0.1	Draft	2 May 2023	Angela Johnson		Initial draft
0.2	Draft	2 June 2023	Angela Johnson		Incorporating Privacy and Information Governance advice
1.0	First version	19 September 2023	Angela Johnson	Executive Leadership Team	First version of policy following 6-month discovery and consultation process
2.0	Second version	18 June 2024	Michael Carney	Executive Leadership Team	Policy review. Added roles for Data Governance Committee and Digital Services Leadership Team; further definition of MyServiceNSW account and included data artefacts; POI documentation retention period added. Revised periods for logs. General semantic and reference changes. More Policy references
2.1	Amended second version	31 July 2024	Michael Carney	Manager, Data Governance	Updated definition of security log; updated disposal authority and retention period associated with customer research
2.2	Amended second version	12 November 2024	Michael Carney	Manager, Data Governance	Accessibility considerations upgraded for publications

8.3 Review Date

This policy will be reviewed in **June 2025**.

It may be reviewed earlier in response to post-implementation feedback from Business Units.

2-24 Rawson Place
Sydney NSW 2000

Office hours:
Monday to Friday
9.00am to 5.00pm

T: 13 77 88
E: info@service.nsw.gov.au
W: www.service.nsw.gov.au