DATA RETENTION POLICY

Code:	08A.8/ISO 27001:2013/A6.2.1/A8.1.2,3,4.A9.3.1/A11.2.5,6,8,9 A12.2.1/A12.5.1/A12.6.2/A13.2.3/A18.1.2
Version:	v 1.9
Date of version:	08/07/2024
Created by:	James Paul
Approved by:	Metin Unal
Confidentiality level:	Confidential

CHANGE HISTORY

Date	Version	Created by	Description of change
23/04/2017	1.0	Casey Eldib	Basic document outline
24/04/2017	1.1	James Paul	Reviewed/modified
18/07/2017	1.2	James Paul	Updated
09/08/2018	1.3	Fiona Nicholls	Updated/reviewed
03/09/2019	1.4	Di Parker	Reviewed/updated
13/09/2020	1.5	Mark Needham	Reviewed
09/09/2021	1.6	Mark Needham	Reviewed/updated
09/09/2022	1.7	Mark Needham	Reviewed/updated
11/09/2023	1.8	Mark Needham	Reviewed/updated
08/07/2024	1.9	Mark Needham/Metin Unal	Review and modified

TABLE OF CONTENTS

1. PURPOSE

The purpose of this Data Retention Policy is to outline the guidelines and procedures for the retention and disposal of data collected and managed by the contact centre responsible for government customer service lines and portal systems in Australia.

2. Scope

This policy applies to all employees, contractors, and third-party vendors involved in the operation and management of the contact centre's systems and services.

3. Data Types and Retention Periods

3.1 Customer Interaction Data

Call logs, call recordings, chat transcripts, and email correspondence: Retained for a 30 days after interaction unless otherwise requested by the specific client, and will be managed under its own data retention policy.

3.2 Personal Information

Personal details provided by customers (e.g., name, address, contact information): Retained for 30 days after interaction unless otherwise requested by the specific client, and will be managed under its own data retention policy.

3.3 Transaction Record

Records of transactions conducted through the portal systems: Retained for 30 days after transaction unless otherwise requested by the specific client, and will be managed under its own data retention policy.

3.4 Call Recordings

Call Recordings of transactions conducted for each client incoming call: Retained for 30 days after interaction unless otherwise requested by the specific client, and will be managed under its own data retention policy.

3.5 Extracted Data

Any data extracted from any internal systems for the purpose of reviewing and/or providing directly to the client owner, and temporarily stored on a secure local device. This data, once extracted and utilised is required to be deleted immediately from the local device not exceeding 7 days from extraction.

3.6 Data Sets

Data sent by the client directly to any member of OracleCMS for the purpose of review or use relating to the provision of the clients service: This data is to be encrypted whilst stationary, and deleted immediately after use, not exceeding 7 days from original receipt.

3.7 Endpoint Plain Text Data

Data gathered by staff during an interaction with client or customer and entered into any program available on the endpoint (i.e Notepad, Word, Excel, etc) as plain text. This data is to be removed immediately upon use, with staff confirming deletion of said data no later than end of shift.

Note: No staff should be storing this type of data on any endpoint device unless strictly approved by a member of management.

3.8 System Log and System Data

Logs of system access, security incidents, and audit trails: Retained for a minimum of 1 year for security and auditing purposes.

4. Data Storage and Security Methods

a. All data collected and retained by the contact centre is stored securely within an encrypted Azure Server or local server in compliance with the Australian Government Information Security Manual (ISM) and relevant data protection standards, including each state information security standards.

b. Access to sensitive and personal data shall be restricted to authorised personnel only, and encryption shall be used for data transmission and storage.

c. All data extracted from primary systems or sent by the client should be stripped of all personal identifiable and sensitive information whilst being stored on local devices (i.e. endpoints, and local computers).

d. Data that is extracted for the purpose of providing to client/Other departments, shall be deleted immediately after use, not exceeding 7 business days.

e. Regular security assessments and audits shall be conducted to ensure compliance with security standards and identify and address any vulnerabilities.

5. Data Disposal

a. At the end of the retention period, data shall be securely disposed of in accordance with the Australian Privacy Principles (APP) and other relevant regulations, including relevant regulations for each state.

b. Disposal methods may include permanent deletion from electronic systems or secure destruction of physical records.

6. Compliance and Monitoring

a. OracleCMS shall appoint a designated Data Protection Officer (DPO) responsible for overseeing compliance with this policy and relevant data protection laws.

b. Regular audits and reviews of data retention practices shall be conducted to ensure ongoing compliance and identify areas for improvement.

7. Training and Awareness

a. All employees and contractors shall receive training on their responsibilities regarding data retention and protection.

b. Regular awareness campaigns shall be conducted to ensure that all personnel are informed of any updates or changes to data retention policies and procedures.

8. Policy Review

This Data Retention Policy shall be reviewed annually or more frequently as necessary to ensure its effectiveness and compliance with regulatory requirements.

9. Validity and Document Management

This document is valid as of 8th July 2024.

The owner of this document is CTO, who must check and, if necessary, update the document at least once a year.

When evaluating the effectiveness and adequacy of this document, the following criteria need to be considered:

- Number of incidents related to unacceptable or unauthorised use of information assets
- Number of incidents related to inappropriate employee training or awareness programs regarding acceptable use of information assets

Chief Technical Officer