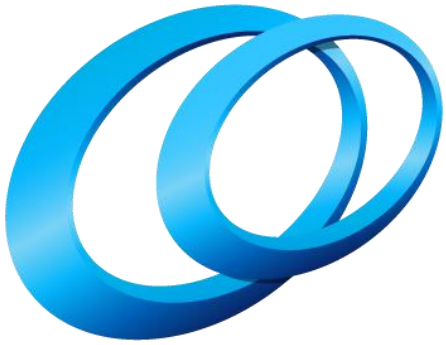

oraclecms
customer management solutions

DATA DISPOSAL POLICY

Code:	
Version:	v 1.10
Date of version:	1/09/2024
Created by:	Casey Eldib, James Paul & Brad Unal
Approved by:	Metin Unal
Confidentiality level:	Confidential

CHANGE HISTORY

Date	Version	Created by	Description of change
24/04/2017	1.0		Basic document outline
28/04/2017	1.2	Brian Grant	Vormetric cryptographic key and control details added
02/05/2017	1.3	James Paul	Reviewed
18/07/2017	1.4	James Paul	Updated
18/07/2018	1.5	Fiona Nicholls	Reviewed/updated
03/09/2019	1.6	Di Parker	Reviewed/updated
13/09/2020	1.7	Mark Needham	Reviewed/updated
09/09/2021	1.8	Mark Needham	Reviewed/updated
07/09/2022	1.9	Mark Needham	Reviewed/updated
11/09/2023	1.10	Mark Needham	Reviewed/updated
01/09/2024	1.11	Mark Needham	Reviewed/Updated

TABLE OF CONTENTS

1. Purpose

The purpose of this policy is to define the procedures and guidelines for the secure and compliant disposal of data at OracleCMS. The goal is to ensure that all data is destroyed in a manner that protects the confidentiality, integrity, and availability of sensitive information and complies with ISO 27001 and SOC 2 standards.

2. Scope

This policy applies to all employees, contractors, and third-party vendors who handle or manage data within OracleCMS. It covers the disposal of all types of data, including electronic data, physical documents, and storage media such as hard drives, USB drives, CDs, and other portable devices.

3. Policy Requirements

3.1 Data Classification

- **Data Sensitivity:** All data must be classified based on its sensitivity level (e.g., public, internal, confidential, highly sensitive). The disposal method will vary depending on the data classification to ensure it is destroyed appropriately.
- **Confidential and Highly Sensitive Data:** Any data classified as confidential or highly sensitive must be subject to the most stringent disposal methods to ensure that it cannot be recovered or accessed post-disposal.

3.2 Data Retention and Disposal

- **Retention Policy:** Data must be retained according to OracleCMS' data retention policy. Once the retention period has expired, data must be securely disposed of in accordance with this policy.
- **Scheduled Disposal:** Data disposal must be carried out on a scheduled basis for data that has reached its retention period or is no longer required for operational or legal purposes.

3.3 Data Disposal Methods

- **Electronic Data:** Electronic data must be disposed of using methods that ensure complete and permanent destruction. Acceptable methods include:
    - **Data wiping:** Using specialised software to overwrite data multiple times to ensure it is unrecoverable.

    - **Physical destruction:** Physically destroying storage devices (e.g., shredding hard drives, breaking CDs) to ensure data cannot be recovered.
- **Physical Documents:** Confidential and sensitive physical documents must be shredded or incinerated. Paper recycling bins or unsecured disposal methods are not permitted for sensitive information.
- **Portable Media:** Devices such as USB drives, CDs, and other portable storage must be wiped or physically destroyed to prevent unauthorized recovery of data.
- **Cloud Storage:** For data stored in cloud environments, ensure that the deletion process is permanent and complies with the provider's data destruction standards. This includes verifying that backup copies are also destroyed.

3.4 Third Party Disposal Services

- **Approved Vendors:** If third-party vendors are used for data destruction, they must be pre-approved by the IT or Security Department. Vendors must provide certification that the data has been securely destroyed in compliance with industry standards and legal requirements.
- **Audit and Verification:** Disposal processes carried out by third-party vendors must be auditable. OracleCMS reserves the right to request proof of destruction and audit the vendor's practices to ensure compliance with security and regulatory standards.

4. Roles and Responsibilities

- **Employees:** Ensure that data is disposed of in accordance with this policy, report any concerns or violations, and handle data disposal securely.
- **IT Department:** Responsible for managing the secure deletion of digital data and ensuring that proper tools are used for data destruction.
- **Compliance Officer:** Ensures that data disposal procedures align with regulatory and legal requirements and conducts audits to verify compliance.
- **Third-Party Vendors:** Must comply with the organisation's data disposal policy and provide evidence of secure disposal when handling data on behalf of the organisation.

.

5. Auditing and Monitoring

Regular audits of data disposal practices will be conducted to ensure compliance with this policy. Employees and third-party vendors may be required to provide proof of proper data disposal.

6. Violations

Failure to comply with this policy may result in disciplinary action, up to and including termination of employment or contract. Legal consequences may also arise if data is improperly disposed of.

6. Review and Updates

This policy will be reviewed annually or when there are significant changes in regulatory requirements or operational practices. Updates will be communicated to all employees and relevant stakeholders.

7. Validity and document management

This document is valid as of 1/09/2024

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

Managing Director

Metin Unal