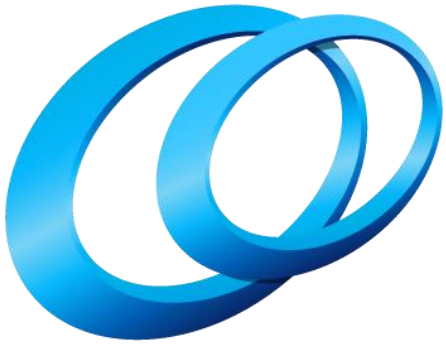

oraclecms
customer management solutions

DATA CLASSIFICATION POLICY

Version:	v 1.9
Date of version:	12/09/2024
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
12/09/2023	1.8	Mark Needham	Reviewed/updated
12/09/2023	1.9	Mark Needham	Reviewed/updated

TABLE OF CONTENTS

1. Introduction

The Data Classification Policy outlines the guidelines and procedures for classifying, handling, and protecting data assets within OracleCMS, an Australian contact centre that also provides bespoke software development services. This policy is designed to ensure the confidentiality, integrity, and availability of company data and to comply with regulatory requirements, including those outlined in the SOC 2 framework.

2. Scope

This policy applies to all employees, contractors, and third-party vendors who have access to company data assets, including but not limited to customer information, proprietary software code, financial records, and operational data.

3. Data Classification Levels

3.1 Public Data (Level 1):

- Public data is information that is intended for unrestricted public access.
    - Examples: Marketing materials, public website content, press releases.
    - Handling: No special handling or protection measures required.

3.2 Confidential/Sensitive Data (Level 2):

- Confidential Sensitive Data, can be considered personally identifiable information (PII) and is sensitive in nature. Therefore, it requires protection from unauthorised access, disclosure, or alteration.
    - Examples: Individuals First Name, Surname, Contact number, Address, Email.
    - Handling: Access to this caller data should be restricted to authorised personnel who have a legitimate need-to-know for performing their duties related to after-hours calls or emergency services. Data should be stored and transmitted using secure methods. Strong access controls, such as role-based access control (RBAC) or least privilege, should be implemented to limit access to authorised users only.

3.3 Internal Use Only Data (Level 3):

- Internal use only data is information that is intended for internal company use and should not be disclosed to external parties.
    - Examples: Internal communications, non-sensitive business documents.
    - Handling: Access restricted to authorised employees and contractors. Data should be stored and transmitted using secure methods. Strong access controls, such as role-based access control (RBAC) or least privilege, should be implemented to limit access to authorised users only. Logs of access to caller data should be maintained and regularly reviewed for unauthorised access or suspicious activities.

3.4 Highly Confidential Data (Level 4):

- Highly confidential data is the most sensitive information that requires the highest level of protection.
    - Examples: Payment card information (PCI), health records (PHI), trade secrets.
    - Handling: Access restricted to a limited number of authorised individuals on a need-to-know basis. Data should be encrypted with strong encryption algorithms. Additional security controls such as multi-factor authentication (MFA) and data loss prevention (DLP) may be required. Logs of access to caller data should be maintained and regularly reviewed for unauthorised access or suspicious activities.

4. DATA CLASSIFICATION PROCESS

4.1 Classification Responsibility

- Data owners are responsible for classifying data assets based on their sensitivity and criticality to the organisation.
- Data owners should regularly review and update data classifications as needed to reflect changes in business requirements or regulatory standards.

4.2 Handling and Protection Methods

- Employees and contractors are responsible for adhering to the handling and protection measures outlined for each data classification level.
- Any data transfer, storage, or processing activities should be conducted in accordance with the classification level of the data.

5. COMPLIANCE AND ENFORCEMENT

5.1 Compliance

This policy complies with relevant regulatory requirements, including those outlined in the SOC 2 framework, as well as industry best practices for data protection and privacy.

5.2 Enforcement

Non-compliance with this policy, including mishandling or unauthorised disclosure of data, may result in disciplinary action, up to and including termination of employment or contract, depending on the severity of the violation and the organisation's disciplinary procedures.

6. POLICY REVIEW

This policy will be reviewed annually or as necessary to ensure that it remains current and aligned with business requirements, regulatory standards, and industry best practices.

7. DOCUMENT RETENTION

Documentation related to data classification, including classification guidelines, data inventories, and classification decisions, will be retained in accordance with the organisation's document retention policies.

8. Validity and Document Management

This document is valid as of 12th September 2023.

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

Chief Technical Officer