



DATA CAPTURE AND VALIDATION PROCEDURE

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

Change History2

1. Purpose3

2. SCOPE3

3. REVIEW FREQUENCY AND TIMING.....3

4. REVIEW PROCESS4

5. KEY ROLES AND RESPONSIBILITIES.....5

6. RECORD KEEPING AND DOCUMENTATION.....6

7. Policy Review6

8. Validity and Document Management6

1. PURPOSE

The purpose of this Data Capture and Validation Procedure is to ensure that data collected by OracleCMS is accurate, complete, secure, and processed in compliance with applicable data protection regulations. This procedure outlines the steps involved in capturing data, validating its accuracy, and ensuring the data meets predefined quality standards before being used for processing or storage.

2. SCOPE AND OBJECTIVES

This procedure applies to all data capture and validation processes within OracleCMS, including:

- Data collected via customer interactions (phone, email, web forms, etc.)
- Data captured through third-party sources or integrated systems
- Sensitive or personal data that requires special handling in compliance with data protection regulations

The objectives of this procedure are to:

- Ensure the accuracy and quality of captured data.
- Maintain compliance with data protection laws, including the **Digital Personal Data Protection Act** (DPDPA), **GDPR**, and other relevant regulations.
- Safeguard the integrity and security of data throughout its lifecycle.
- Ensure that data is validated before use in processing, reporting, or decision-making.

3. DATA CAPTURE PROCESS

Data Sources Data will be captured from the following sources:

- **Customer Interactions:** Data collected from phone calls, emails, online forms, and other communication channels.
- **Third-Party Systems:** Data imported from integrated systems or received from third-party service providers.
- **Automated Systems:** Data generated automatically by OracleCMS systems (e.g., logs, sensor data).
- **Manual Entry:** Data manually entered by agents or employees.

Data Types The types of data that will be captured include:

- **Personal Data:** Names, contact details, customer identifiers.
- **Sensitive Data:** Financial details, health information, or any other information requiring additional protection.

- **Non-Personal Data:** System logs, operational data, and performance metrics.

Data Capture Methods

- **Automated Data Capture:** OracleCMS will use automated systems to capture data whenever possible to reduce human error and ensure consistency.
- **Manual Data Capture:** In cases where data must be manually entered, standard templates or forms will be used to ensure consistency and minimize errors.

Data Collection Policies

- All data capture methods will adhere to **data minimization principles**, ensuring that only necessary data is collected.
- Data will be captured only after obtaining the necessary **consent** (if required), ensuring lawful processing under applicable data protection laws.
- Captured data will be stored securely and only accessible to authorized personnel.

4. DATA VALIDATION PROCESS

4.1 Data Integrity Checks

- **Format Validation:** Ensuring that data entered is in the correct format (e.g., phone numbers, email addresses, dates).
- **Range Checks:** Verifying that numerical data falls within acceptable ranges (e.g., age, transaction amounts).
- **Required Fields:** Ensuring that all mandatory fields are populated before submitting data for processing.
- **Uniqueness Checks:** Checking for duplicate data entries, such as multiple records for the same individual or business.

4.2 Accuracy Validation

- **Cross-Verification:** Data captured from multiple sources (e.g., customer forms, databases) will be cross-verified to ensure consistency and accuracy.
- **Third-Party Validation:** Data received from third-party sources will be validated against authoritative or trusted databases where possible.
- **Consistency Checks:** Ensuring that the data makes sense when cross-referenced with other related data. For example, ensuring that a customer's address matches their geographic region.

4.3 Completeness Checks

- **Field Completion:** Ensuring that all required fields are filled before processing.

- **Contextual Validation:** Ensuring that the collected data makes sense within the given context (e.g., a valid product code for an order, correct customer account number).

4.4 Real-Time Validation

- Where feasible, data will be validated in **real time** as it is captured to reduce the chances of incorrect data entering the system. This includes checks for valid input, formatting errors, and required fields.

4.5 Manual Validation

- Data that cannot be validated automatically will be flagged for **manual review** by the appropriate personnel. This includes checking for data inconsistencies or errors that cannot be resolved automatically.

5. DATA VALIDATION TOOLS AND TECHNOLOGIES

OracleCMS will use the following tools and technologies to support data capture and validation:

- **Validation Scripts:** Automated scripts and algorithms for validating data formats, ranges, and required fields.
- **Data Validation Software:** Use of third-party software (where appropriate) to verify data accuracy and consistency, especially for sensitive or complex datasets.
- **Business Rules Engine:** A set of pre-defined business rules that help in checking if the captured data aligns with expected patterns or conditions (e.g., ensuring customer addresses match the region).
- **Audit Logs:** Keeping detailed audit logs of data capture and validation activities to track any discrepancies, errors, or issues.

6. ROLES AND RESPONSIBILITIES

Data Capture Teams:

- Ensure data is captured accurately and securely following the established procedures.
- Communicate with customers or third-party services to clarify missing or incomplete data.

Data Validation Teams:

- Review and validate data manually when automatic validation fails or discrepancies are found.
- Ensure that data is correct, complete, and ready for processing or use.

IT and Security Teams:

- Implement and maintain systems to automate data capture and validation processes.
- Ensure that all captured data is securely stored and protected from unauthorized access or loss.

Compliance and Legal Teams:

- Review data capture and validation practices for compliance with data protection laws.
- Ensure data consent practices are in place and that sensitive data is handled securely.

7. DATA CORRECTION AND ERROR HANDLING

Error Notification: When data errors or discrepancies are identified during validation, the appropriate stakeholders will be notified immediately for correction.

Error Logging: A log of all validation errors will be maintained for future reference and process improvement.

Data Correction: A documented process for correcting erroneous data will be followed, ensuring that corrections are done in a way that maintains data integrity and security

8. MONITORING AND REPORTING

Ongoing Monitoring: Continuous monitoring will be conducted to ensure that data capture and validation processes are working as intended. Key performance indicators (KPIs) will be established to track data quality metrics.

Periodic Audits: Periodic audits will be carried out to assess the effectiveness of the data capture and validation procedures. The results of these audits will be used to improve processes.

Reporting: Regular reports on data validation performance, including error rates and correction actions, will be provided to senior management and relevant stakeholders.

9. DATA RETENTION AND DISPOSAL

- **Retention Periods:** Data will be retained in accordance with OracleCMS's data retention policies. Captured data will not be retained longer than necessary.
- **Data Disposal:** When data is no longer needed, it will be securely deleted or anonymized to prevent unauthorized access.

10. VALIDITY AND DOCUMENT MANAGEMENT

This document is valid as of 8th July 2024.

The owner of this document is CIO, 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

