INFORMATION SECURITY POLICY

Code:	04/ISO 27001:2013/5.2/5.3
Version:	v 1.8
Date of version:	10/09/2024
Created by:	James Paul
Approved by:	Metin Unal
Confidentiality level:	Confidential

CHANGE HISTORY

Date	Version	Created by	Description of change
13/12/2016	1.0	Casey Eldib	Basic document outline
18/07/2017	1.1	James Paul	Reviewed/updated
09/08/2018	1.2	Fiona Nicholls	Reviewed/updated
29/08/2019	1.3	Di Parker	Reviewed/updated
13/09/2020	1.4	Mark Needham	Reviewed
09/09/2021	1.5	Mark Needham	Reviewed/updated
05/09/2022	1.6	Mark Needham	Reviewed/updated
04/09/2023	1.7	Samed Unal	Reviewed/updated
10/09/2024	1.8	Phoebe Gernale	Reviewed/updated

TABLE OF CONTENTS

1. PURPOSE, SCOPE AND USERS

The aim of this top-level Policy is to define the purpose, direction, principles and basic rules for information security management.

This Policy is applied to the entire Information Security Management System (ISMS), as defined in the ISMS Scope Document.

Users of this document are all employees of OracleCMS, as well as relevant external parties.

2. REFERENCE DOCUMENTS

- ISO/IEC 27001 standard, clauses 5.2 and 5.3
- ISMS Scope Document
- Risk Assessment and Risk Treatment Methodology
- Statement of Applicability
- List of Legal, Regulatory and Contractual Obligations
- Business Continuity Plan
- Incident Management Procedure

3. BASIC INFORMATION SECURITY TERMINOLOGY

Confidentiality — characteristic of the information by which it is available only to authorized persons or systems.

Integrity — characteristic of the information by which it is changed only by authorized persons or systems in an allowed way.

Availability— characteristic of the information by which it can be accessed by authorized persons when it is needed.

Information security — preservation of confidentiality, integrity and availability of information. Information Security Management System — part of overall management processes that takes care of planning, implementing, maintaining, reviewing, and improving the information security.

4. MANAGING THE INFORMATION SECURITY

4.1 Objectives and measurement

The objective of information security is to ensure the business continuity of Oracle CMS and to minimize the risk of damage by preventing incidents and reducing their potential impact All the objectives must be reviewed at least once a year by the Chief Technology Officer (CTO).

Oracle CMS will measure the fulfilment of all the objectives. Managing Director is responsible for setting the method for measuring the achievement of the objectives — the measurement will be

performed at least once a year and CTO will analyse and evaluate the measurement results and report them to Senior Management as input materials for the Management review.

4.2 Information security requirements

This Policy and the entire ISMS must be compliant with legal and regulatory requirements relevant to the organisation in the field of information security, as well as with contractual obligations.

A detailed list of all contractual and legal requirements is provided in the List of Legal, Regulatory and Contractual Obligations.

4.3 Information security controls

The process of selecting the controls (safeguards) is defined in the Risk Assessment and Risk Treatment Methodology.

The selected controls and their implementation status are listed in the Statement of Applicability.

4.4 Business continuity

Business continuity management is prescribed in the Business Continuity Management Policy

4.5 Responsibilities

Responsibilities for the ISMS are the following:

- Managing Director is responsible for ensuring that the ISMS is implemented and maintained according to this Policy, and for ensuring all necessary resources are available
- Chief Technology Officer is responsible for operational coordination of the ISMS as well as for reporting about the performance of the ISMS
- Managing Director/ Senior management must review the ISMS at least once a year or each time a significant change occurs, and prepare minutes from that meeting. The purpose of the management review is to establish the suitability, adequacy and effectiveness of the ISMS.
- Customer Experience Manager/ Training Manager will implement information security training and awareness programs for employees
- the protection of integrity, availability, and confidentiality of assets is the responsibility of the owner of each asset
- all security incidents or weaknesses must be reported to Chief Technology Officer
- Chief Technology Officer will define which information related to information security will be communicated to which interested party (both internal and external), by whom and when
- Chief Technology Officer is responsible for adopting and implementing the Training and Awareness Plan, which applies to all persons who have a role in information security management

4.6 Policy communication

Managing Director has to ensure that all employees of OracleCMS, as well as appropriate external parties are familiar with this Policy.

5. SUPPORT FOR ISMS IMPLEMENTATION

Hereby the Managing Director declares that ISMS implementation and continual improvement will be supported with adequate resources in order to achieve all objectives set in this Policy, as well as satisfy all identified requirements.

6. VALIDITY AND DOCUMENT MANAGEMENT

This document is valid as of 4th September 2023.

The owner of this document is Managing Director 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 employees and external parties who have a role in the ISMS, but are not familiar with this document
- non-compliance of the ISMS with the laws and regulations, contractual obligations, and other internal documents of the organisation
- ineffectiveness of ISMS implementation and maintenance
- unclear responsibilities for ISMS implementation

Managing Director

Metin Unal