INFORMATION CLASSIFICATION POLICY

Code:	8A.8/ISO27001:2013/A8.2.1-3/A8.3.1.3/A9.4.1/A13.2.3
Version:	v 1.5
Date of version:	09/09/2021
Created by:	James Paul
Approved by:	Metin Unal
Confidentiality level:	Confidential

CHANGE HISTORY

Date	Version	Created by	Description of change
04/05/2017	1.0	James Paul	Basic document outline
18/07/2017	1.1	James Paul	Updated/reviewed
18/07/2018	1.2	Fiona Nicholls	Updated/reviewed
03/09/2019	1.3	Di Parker	Updated/reviewed
13/09/2020	1.4	Mark Needham	Updated/reviewed
09/09/2021	1.5	Mark Needham	Updated/reviewed

TABLE OF CONTENTS

1. PURPOSE, SCOPE AND USERS

The purpose of this document is to ensure that information is protected at an appropriate level. This document is applied to the entire Information Security Management System (ISMS) scope, i.e. to all types of information, regardless of the form — paper or electronic documents, applications and databases, people's knowledge, etc.

Users of this document are all employees of OracleCMS.

2. REFERENCE DOCUMENTS

- ISO/IEC 27001 standard, clauses A.8.2.1, A.8.2.2, A.8.2.3, A.8.3.1, A.8.3*3, A.9.4.1, A.13.2.3
- Information Security Policy
- Risk Assessment and Risk Treatment Report
- Statement of Applicability
- Inventory of Assets
- List of Legal, Regulatory and Contractual and Other Obligations
- Incident Management Procedure
- Operating Procedures for Information and Communication Technology/ Disposal and Destruction Policy
- Acceptable Use Policy

3. CLASSIFIED INFORMATION

3.1 Steps and responsibilities

Steps and responsibilities for information management are the following:

Step name	Responsibility
1. Entering the information asset in the Inventory of Assets	CTO
2. Classification of information	Asset owner
3. Information labelling	Asset owner
4. Information handling	Persons with access rights in accordance with this Policy

If classified information is received from outside the OracleCMS, CTO is responsible for its classification in accordance with the rules prescribed in this Policy, and this person becomes the owner of such an information asset.

3.2 Classification of information

3.2.1 Classification criteria

The level of confidentiality is determined based on the following criteria:

- value of information — based on impacts assessed during risk assessment

- sensitivity and criticality of information — based on the highest risk calculated for each information item during risk assessment
- legal and contractual obligations — based on the List of Legal, Regulatory and Contractual and Other Obligations

3.2.2 Confidentiality levels

All information must be classified into confidentiality levels.

Confidentiality level	Labelling	Classification criteria	Access restriction
	Unlabelled	Making the information public cannot harm the organization in any way	Information is available to the public
Internal use	INTERNAL USE	Unauthorized access to information may cause minor damage and/or inconvenience to the OracleCMS	Information is available to all employees and selected third parties
Restricted	RESTRICTED	Unauthorized access to information may considerably damage the business and/or the OracleCMS reputation	Information is available only to a specific group of employees and authorized third parties
Confidential	CONFIDENTIAL	Unauthorized access to information may cause catastrophic or irreparable damage to business and/or to the OracleCMS reputation	Information is available only to individuals in the organization

The basic rule is to use the lowest confidentiality level ensuring an appropriate level of protection, in order to avoid unnecessary protection costs.

3.2.3 List of authorized persons

Information classified as "Restricted" and "Confidential" must be accompanied by a List of Authorized Persons in which the information owner specifies the names or job functions of persons who have the right to access that information.

The same rule applies to the confidentiality level "Internal use" if people outside the OracleCMS will have access to such a document.

3.2.4 Reclassification

CTO/Asset owners must review the confidentiality level of their information assets every two years and assess whether the confidentiality level can be changed. If possible, the confidentiality level should be lowered.

3.3 Information labelling

Confidentiality levels are labelled in the following way:

- paper documents — the confidentiality level is indicated in the top right corner of each document page; it is also indicated on the front of the cover or envelope carrying such a document as well as on the fifing folder in which the document is stored
- electronic documents — the confidentiality level is indicated in the top right corner of each document page

- information systems — the confidentiality level in applications and databases must be indicated on the system access screen, as well as in the top right corner of each consecutive screen displaying confidential information
- electronic mail —the confidentiality level is indicated in the first line of the e-mail body
- electronic storage media disks, memory cards, etc, — the confidentiality level must be indicated on the top surface of such a medium
- information transmitted orally — the confidentiality level of confidential information to be transmitted in face-to-face communication, by telephone or some other means of communication, must be communicated prior to the information itself

3.4 Handling classified information

All persons accessing classified information must follow the rules listed in the following table. [job title] must initiate disciplinary action each time the rules are breached or if the information is communicated to unauthorized persons. Each incident related to handling classified information must be reported in accordance with the Incident Management Procedure.

Information assets may be taken off-premises only after obtaining authorization in accordance with the Acceptable Use Policy.

The method for secure erasure and destruction of media is prescribed in the document Operating Procedures for information and Communication Technology / Disposal and Destruction Policy.

	Internal use	Restricted*	Confidential*
Paper documents	Only authorized persons may have access If sent outside the organization, the document must be sent as registered mail Documents may only be kept in rooms without public access Documents must be frequently removed from printers or fax machines	The document must be stored in a locked cabinet Documents may be transferred within and outside the organization only in a closed envelope if sent outside the organization, the document must be mailed with a return receipt service documents must immediately be removed from printers or fax machines only the document owner may copy the document only the document owner may destroy the document	The document must be stored in a safe The document may be transferred within and outside the organization only by a trustworthy person in a closed and sealed envelope Faxing the document is not allowed The document may be printed out only if the authorised person is standing next to the printer
Electronic documents	Only authorized persons may have access when files are exchanged via services such as FTP, instant messaging, etc., they must be password protected access to the	Only persons with authorization for this document may access the part of the information system where this document is stored when files are exchanged via services such as FTP,	The document must be stored in encrypted form The document may be stored only on servers which are controlled by the organization

	information system where the document is stored must be protected by a strong password The screen on which the document is displayed must be automatically locked after 3 minutes of inactivity	instant messaging, etc., they must be encrypted only the document owner may erase the document	The document must not be exchanged via services such as FTP, instant messaging, etc.
Information systems	Only authorized persons may have access to the information system must be protected by a strong password the screen must be automatically locked after [number] minutes of inactivity The information system may only be located in rooms with controlled physical access	Users must log out of the information system if they have temporarily or permanently left the workplace data must be erased only with an algorithm which ensures secure deletion	Access to the information system must be controlled through an authentication process using smart cards or biometric readers The information system may only be installed on servers controlled by the organization the information system may only be located in rooms with controlled physical access and identity control of people accessing the room
Electronic mail	Only authorized persons may have access to the sender must carefully check the recipient all rules stated under "Information systems'	E-mail must be encrypted if sent outside the organization	All e-mails must be encrypted
Electronic storage media	Only authorized persons may have access media or files must be password protected if sent outside the organization, the medium must be sent as registered The medium may only be kept in rooms with controlled physical access	Media and files must be encrypted media must be stored in a locked cabinet If sent outside the organization, the medium must be mailed with a return receipt service only the medium owner may erase or destroy the medium	Media must be stored in a safe Media may be transferred within and outside the organization only by a trustworthy person in a closed and sealed envelope
Information transmitted	Only authorized persons may have access to information unauthorized persons must not be present	The room must be soundproof The conversation must not be recorded	Conversation conducted through a means of communication must be encrypted no

	in the room when the information is communicated		transcript of the conversation may be

*Controls are implemented cumulatively, meaning that controls for any confidentiality level imply the implementation of controls defined for lower confidentiality levels — if stricter controls are prescribed for a higher confidentiality level, then only such controls are implemented.

4. MANAGING RECORDS KEPT ON THE BASIS OF THIS DOCUMENT

Record name	Storage location	Person responsible for storage	Controls for record protection	Retention time
Managing Director COO CTO CFO	Together with the information where the confidentiality indicated	CTO/information asset owner	The same as for the protection of information	The List must exist as long as the information itself exists

5. VALIDITY AND DOCUMENT MANAGEMENT

This document is valid as of 13th September 2020

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 unauthorized access to information
- number of information assets classified with an inappropriate confidentiality level

Chief Technology Officer