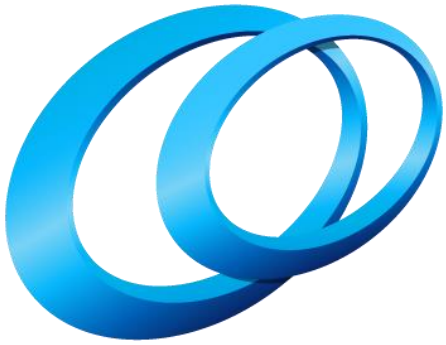

oraclecms
customer management solutions

SYSTEM AND DATA ACCESS REVIEW PROCEDURE

Version:	v 1.8
Date of version:	11/09/2023
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

TABLE OF CONTENTS

1. OBJECTIVE

This procedure outlines the steps to conduct regular access reviews for system and data access within OracleCMS to ensure compliance with security policies, maintain data integrity, and minimise the risk of unauthorised access.

2. INITIATION OF ACCESS REVIEW

2.1. Access reviews should be conducted regularly as per the defined schedule or triggered by significant events such as role changes, terminations, or security incidents.

2.2. The access review process is initiated by the designated access review administrator or security officer.

3. PREPERATION

3.1. Identify the systems, applications, and data repositories to be included in the access review process.

3.2. Compile a list of users with access rights to the selected systems and data repositories.

3.3. Review and update documentation related to user roles, permissions, and access privileges.

4. ACCESS REVIEW EXECUTION

4.1. Generate a list of users and their corresponding access rights for each system and data repository identified for review.

4.2. Notify system owners, data custodians, and relevant stakeholders about the upcoming access review.

4.3. Review user access rights and permissions based on the following criteria:

- Validity of access requests and approvals.
- Appropriateness of access privileges in relation to job responsibilities.
- Compliance with least privilege principles.
- Justification for elevated or sensitive access rights.
- Adherence to segregation of duties.

4.4. Verify user access rights with the approved access control lists, role assignments, and permission matrices.

4.5. Document findings and discrepancies identified during the access review process.

5. REMEDIATION AND APPROVAL

5.1. Address identified discrepancies and violations promptly by taking appropriate remedial actions, such as:

- Revoking unnecessary access rights.
- Updating user roles and permissions.
- Notifying system owners or data custodians about unauthorised access.

5.2. Document remediation actions taken to resolve identified issues.

5.3. Obtain approvals from system owners, data custodians, or designated authorities for remediation actions requiring authorisation.

6. REPORTING AND DOCUMENTATION

6.1. Prepare an access review report summarising the findings, remediation actions, and approval status.

6.2. Share the access review report with relevant stakeholders, including management, IT administrators, and compliance officers.

6.3. Retain documentation related to access reviews, including reports, findings, remediation actions, and approvals, for audit and compliance purposes.

7. FOLLOW UP AND MONITORING

7.1. Conduct follow-up reviews to ensure that remediation actions have been implemented effectively and that access rights remain appropriate and compliant.

7.2. Monitor access requests and approvals regularly to detect and address any unauthorised changes or deviations from established access controls.

8. REVIEW AND CONTINUOUS IMPROVEMENT

8.1. Review the access review process periodically to identify areas for improvement and optimisation.

8.2. Incorporate feedback from stakeholders and lessons learned from previous access reviews to enhance the effectiveness and efficiency of future reviews.

9. COMPLIANCE AND AUDIT

9.1. Ensure that access review procedures comply with relevant regulatory requirements, industry standards, and internal policies.

9.2. Facilitate access reviews as part of internal audits, compliance assessments, or external audits to demonstrate adherence to security controls and data protection measures.

By following this procedure, OracleCMS can effectively manage access to systems and data, mitigate the risk of unauthorised access, and maintain compliance with security policies and regulatory requirements.

This document is valid as of 11th September 2023.

Chief Technical Officer