POLICY FOR TRACKING EXTERNAL GPS

Version:	v 1.4
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
13/09/2020	1.0	Mark Needham	Reviewed
09/09/2021	1.1	Mark Needham	Reviewed/updated
09/09/2022	1.2	Mark Needham	Reviewed/updated
11/09/2023	1.3	Mark Needham	Reviewed/updated
12/09/2023	1.4	Mark Needham	Reviewed/updated

TABLE OF CONTENTS

1. Purpose

This policy outlines OracleCMS's approach to tracking client user GPS data for geo-fencing when logging into jobs via our developed portals. It ensures compliance with privacy regulations, data security measures, and operational requirements.

2. Scope

This policy applies to all client users accessing OracleCMS-developed portals that require geo-fencing to verify job locations, track work attendance, and enhance security.

3. Policy Statement

OracleCMS implements GPS tracking with geo-fencing capabilities to:

- Verify that users are within designated job site boundaries before logging into jobs.
- Enhance security by preventing unauthorised access from unapproved locations.
- Improve operational efficiency and workforce management.
- Ensure compliance with contractual obligations and safety regulations.

4. Data Collection and Usage

- GPS data is collected only when users log in to a job via the designated portal.
- The system records location data in real time and validates the user's position against predefined geo-fenced areas.
- GPS data is not continuously tracked when users are logged out or outside of work hours.
- The collected data is used exclusively for operational, security, and compliance purposes.

5. User Consent and Notification

- Users are required to provide consent before enabling location tracking within the portal.

- Clear notifications are provided to users about when and why their location data is being collected.
- Users may review location tracking permissions and adjust settings within compliance requirements.

6. Data Security and Privacy

- GPS data is usually provided direct to the client and not held in any storage system by OracleCMS.
- If required by specific client in accordance with contractual requirements, OracleCMS can store GPS data under the following requirements:
    - All GPS data is encrypted and stored securely to prevent unauthorised access.
    - Access to location data is restricted to authorised personnel for operational and security purposes only.
    - OracleCMS adheres to all applicable privacy laws and industry best practices in handling GPS data.

7. Retention and Deletion

- In the event that GPS data is required to be held by OracleCMS for a specific client or service the following requirements must be adhered too:
    - GPS data is retained for a predefined period in accordance with regulatory and contractual requirements.
    - Data no longer required for operational purposes will be securely deleted in compliance with OracleCMS's data retention policies.

8. Compliance and Enforcement

- Users who attempt to bypass or manipulate geo-fencing controls may be subject to account restrictions or further investigation.
- OracleCMS will periodically audit geo-fencing functionality to ensure accuracy and compliance.
- Any concerns or complaints regarding location tracking can be addressed through OracleCMS's data privacy officer.

9. Validity and Document Management

This document is valid as of 12th September 2024.

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 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