MRS OIL NIGERIA PLC
DATA AND INFORMATION CHANGE MANAGEMENT POLICY
This Policy is issued pursuant to the Nigerian Data Protection Regulation, 2019 and International Best Practices.

Review Frequency This document is reviewed biennially.
Document Ref.: MRS DICMP
Version Number: V. No. 1
Document Author: Mr. Olatunji Sanusi **Designation:** I.T Manager
Document Owner: **Designation:** Data Protection Officer

MRS Oil Nigeria Plc's Record of Change to the Data and Information Change Management Policy

MRS Oil Nigeria Plc. ("the Company") records planned updates under this section. The version number, author's name and date, approver's name and date, change type (i.e., high-level descriptor such as: 'Contact List Updates'), and a brief summary of the changes to the plan should be provided in the appropriate columns. For reviews that did not result in any updates, record 'No Updates' in the 'Summary of Changes' column.

Version	Author (Name, & Date)	Approver (Name, & Date)	Change type	Summary of Changes
1.0			Plan Creation	Created the Incident Response Plan

CONTENTS

1. INTRODUCTION:

The Change Management refers to the process of preparing, equipping and supporting individuals to successfully adopt change in order to drive Organizational success and outcomes.

2. POLICY STATEMENT:

The purpose of this Policy is to manage changes to information systems, resources, assets and personal data of all Company's stakeholders, in a rational and predictable manner, to enable the stakeholders plan. These changes require careful thoughtfulness, monitoring and follow-up evaluation to reduce negative impacts and increase the value of information resources and personal data management of Data Subjects collected, retained and processed by the Company.

All changes to any information system, resource, asset or personal data must be reviewed and approved by the Board Nomination and Corporate Governance Committee, documented and well communicated to relevant stakeholders.

3. DEFINITIONS:

a. **Change** means any implementation of new functionality, interruption of service, repairs of existing functionality, change in networking functionality, and removal of existing functionality.
b. **Change Management** means the process of requesting, developing, approving and implementing a planned or unplanned change within the Information Technology Systems (ITS), to ensure that information resources are protected against improper modification before, during and after system implementation.
c. **Change Item/Change Request** means a documented request to modify the ITS infrastructure.
d. **Data Protection Officer** means the Manager responsible for the collection of personal data and establishing controls that provide security of ITS.
e. **Data Custodian** means the holder of a data, the agent charged with the responsibility of processing and storage of information. He is the provider of services.
f. **Emergency Change** means a change in the immediate priority where an ITS personnel is required to execute a change without any review or approval. This is normally in a service outage, system down or an urgent outage prevention situation. The subsequent change is to be reviewed, communicated and closed during the next scheduled change meeting.
g. **ITS Infrastructure** means the network, server, storage, database and solutions technologies managed by the Information Technology Services department.
h. **Non-Emergency Change** means a change of regular priority where the review of the change request is made during the change meeting and the approval is received prior to the change made.
i. **Scheduled Change** means formal notification received, reviewed and approved by the review process in advance of the change to be made.
j. **Urgent Change** means a change of escalated priority, where review and approval of the change is received from an ITS Officer, prior to the change made and it is subsequently reviewed, communicated and closed during the next scheduled change meeting.
k. **Unscheduled Change** means the failure to present notification to the formal process in advance of the changes made. An unscheduled change does not include an event of a system failure or the discovery of a security vulnerability.

4. POLICY PROCEDURES:

a. All Changes to IT services must follow a structured process for appropriate planning and execution.
b. All Changes must follow an approved Change Management process of planning, evaluation, review, approval, and documentation.
c. The significance of the change to be defined as a "change" is set by the Change Management Committee's (CMC) procedures and guidelines for Change Management.
d. All changes affecting computing environment facilities, such as air –conditioning, water, heat, plumbing, electricity and alarms need to be reported to or coordinated with the DPO;
e. The members of the CMC appointed by the Board Nomination and Corporate Governance Committee will meet regularly to review change requests and ensure that change reviews and communications are satisfactorily performed;
f. Information Security Office/Data Protection and Management Office must be included in the Change Management Committee to ensure that the Company's information and digital assets are adequately secured at all times.
g. A formal written request must be submitted for all changes, whether scheduled or unscheduled or emergency ones.
h. All scheduled change request must be submitted in accordance with change management procedures to allow the CMC sufficient time to review the request for approval.
i. A Change request must fulfill Information Security requirements.
j. All change requests must receive formal CMC approval before proceeding with the change.
k. All change requests must be submitted early to allow the CMC adequate time to process the request according to its severity, complexity and urgency.
l. The Chairman of the CMC may reject a scheduled or unscheduled change for reasons including, but not limited to, inadequate planning, inadequate back out plans, the timing of the change will negatively impact a key business process such as a year-end accounting, or if adequate resources cannot be readily available. Adequate resources may be a problem on weekends, holidays, or during special events.
m. Customer notification must be completed for each scheduled or unscheduled change following the steps contained in the Change Management Procedure.
n. A Change Review must be completed for each scheduled or unscheduled change following the steps contained in the Change Management Procedures.
o. A Change Management Log must be maintained for all changes. The log must contain, but is not limited to:

    i. Date of submission and date of change;
    ii. Owner and custodian contact information;
    iii. Nature of the change;
    iv. Indication of success or failure.

p. Proper testing should be performed for any change;
q. An adequate back-up/fall back plan for aborting and recovering from unsuccessful changes and unforeseen events must be in place with clear stakeholders' responsibilities and accountabilities.
r. Proper communication to relevant stakeholders and date owners should be performed at all times when needed.
s. Any change consequence like possible problems arising from the change or a worst case scenario, must be communicated and approved by the relevant data owners.
t. A proper inventory to all change management processes, logs and approvals should be in place.
u. Change Management Policy domain is for data and information systems and digital assets that have been processed and must have passed the release management processes.

v. Where a new data and information systems will integrate with other running components, it must be governed by this Policy.

5. BREACH OF THIS POLICY

Any user who violates a part of this Policy may be subjected to disciplinary action, up to termination of employment or dismissal from employment.

6. POLICY REVIEW

This Policy shall be reviewed every two (2) years or as deemed necessary, in line with the applicable laws.

Approved by the Board of Directors
On May 27, 2020