MRS OIL NIGERIA PLC
The Cyber Security Incident Response Policy

This Policy is issued pursuant to the Nigerian Data Protection Regulation, 2019 and International Best Practices on Data Protection.

Version 1.0
Date: 30/3/2021

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

Plan Maintenance and Change Management Record

This section contains records of plan updates. Record the version, author name and date, approver 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. For reviews that did not result in any updates, record ‘No Updates’ in the ‘Summary of Changes’ column.

[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
1.0			Plan Creation	Created the Incident Response Plan

Table of contents

1. INTRODUCTION: Purpose of the Policy

MRS Oil Nigeria Plc. is committed to protect its information resources. The Cyber Security and Incidents Response Policy (“the Policy”) provides an overall plan for responding to cyber security or information security incidents. The Policy defines the roles and responsibilities of Management and designated employees (i.e. Incident Response Team) to identify, isolate cyber and data security incidents. The Policy also outlines the characteristics of incidents, determines their scope and risks and the relationships between the Policy and other Data Protection Policies, including reporting requirements.

The Policy determines the appropriate response to incidents and communicates the result and risks to all stakeholders. It proactively reduces the likelihood of any reoccurrence and recommends appropriate training for employees on physical security and environmental controls such as firewalls, malware detection, etc.

The Incident Response Team (IRT) are trained annually to recognize and report identified anomalies in the computer systems immediately to the Incident Response Manager (IRM), who would specify the response protocol. The IRM nominates members of the IRT who shall be trained by Cyber Security experts on the latest cyber security threats and modern techniques of incident remediation. In the event of a cyber-security incident, the Incident Response team who have been trained will expeditiously deal with the matter.

2. DEFINITIONS

Cyber Security Incident - A Cyber Security Incident is any event that threatens the confidentiality, integrity or availability of internal information resources of the Company. This include situations where sensitive information if stolen or lost may be harmful to the Company and stakeholders.

Incident Response Team (IRT) - The IRT is made up of experts in different professions in the Company who are involved in the resolution of cyber-security Incidents. The IRT include the Incident Response Manager, representatives of the legal and I.T department. Representatives of the I.T department include employees who handle technical hardware, networking and front-end software tasks.

Incident Response Manager (IRM) - The IRM oversees all aspects of the Cyber Security Incident. He act as a liaison between IRT and the Management team and reviews all cyber security incidents for the Incident Summary Report and a Process Improvement Plan.

Cyber Security Incident Log - The Cyber Security Incident Log will capture critical information about a Cyber Security Incident and the Company’s response to that incident.

Incident Summary Report (ISR) - The ISR is a document prepared by the IRM at the conclusion of a Cyber Security Incident, with a detailed summary of the incident, including how and why the incident occurred, estimated data loss, affected parties, and impacted services. Finally, it will examine the procedures of the Cyber Security Incident Response Policy, including the procedures followed by the IRT and whether updates are required. The template for the ISR may be seen in Appendix A.

Process Improvement Plan (PIP) - The PIP is a document prepared by the IRM at the conclusion of a Cyber Security Incident. It provides recommendations to avoid or minimize the impact of future Cyber Security Incidents based upon the “lessons learned” from the recently-completed incident. This plan should be kept confidential for security purposes. The template for the PIP may be viewed in Appendix B.

3. INCIDENT RESPONSE TEAM

INCIDENT RESPONSE MANAGER

Name	**Email**
Work Phone	**Mobile Phone**

TECHNICAL CONTACTS

Name	**Email**
Work Phone	**Mobile Phone**

Name	**Email**
Work Phone	**Mobile Phone**

Name	**Email**
Work Phone	**Mobile Phone**

LEGAL COUNSEL

Name	**Email**
Work Phone	**Mobile Phone**

ADDITIONAL MEMBERS

In addition to the members listed above, additional employees may be included to the IRT, based on the nature and scope of the incident, such as, a software support personnel. The IRM may appoint additional members to the IRT as the need arises.

6. INCIDENT MANAGEMENT PRINCIPLES

6.1 CONFIDENTIALITY

Investigation

During a Cyber Security Incident investigation, the IRM or members of the IRT will gather information from multiple computer systems and/or conduct interviews with key personnel based on the scope of the incident in question. All information gathered or discovered during a Cyber Security Incident are strictly confidential throughout the investigative process. All members of the Cyber Security Incident Response Team are trained in information security and data privacy best practices. At the conclusion of the investigative process, the IRM will present a summary of the details of the incident and investigation to the Management Team in line with the content of briefing in the Response Phase on page 9. During this phase, no confidential information will be shared unless it is strictly relevant to the investigation and/or the incident itself.

In the event that an incident involves unauthorized access or disclosure of any confidential information of the Company or an employee, the IRM will communicate to the Management the information relevant to the incident and any additional information requested, which the Company or the affected employee (s) have a right to (e.g. specific company or employee records, etc.). The Company reserves the right to withhold certain information at its discretion, where it is of the opinion that such information may jeopardize current or future investigations, or pose a security risk to the Company and its stakeholders.

Where the incident involves the information of a vendor or customer, the IRM will inform the Management and take appropriate steps in line with the provisions of this Policy to notify the affected persons. Where the incident did not affect sensitive or confidential information, the Managing Director has the discretion to determine whether or not the IRM can share information related to the incident with external stakeholders.

Report Management

All reports generated during an investigation along with the evidence gathered will be securely stored and managed by the IRM. Any physical record will be stored in a locked file with the IRM who has sole access to the file. All digital records will be stored on the Company's network, accessible only by the I.T. Team, which will be backed up and stored in accordance with the Company's regular backup procedures. In the event past records of incidents need to be reviewed, a written request must be made to the IRM with the requestor contact details, the information requested and the reason for the request. The IRM will review the request and has the discretion to approve or deny the request. The Incident Response Team will make all Incident report(s) available to the Managing Director through the IRM.

6.2 COMMUNICATION GUIDELINES

Communication with employees, will be disseminated by the IRM. Initial communication to persons must be made immediately upon the identification of the incident. In some cases, this may include an initial communication (letter, email, phone call) that simply states that the Company's attention has been drawn to the incident and the Incident Response Team is addressing it, with the promise of a follow up. Scenarios for the release of Personally Identifiable Information (PII) are as follows:

- Should there be an unauthorized release of personal data of employees, customers, vendors or any other stakeholder occur, the Company shall notify the affected persons by an email in the most expedient manner.
- Should the release of Bank Verification Number (BVN), Driver's License, Account Number, or Credit/Debit Card number combined with PII occur, the IRM shall liaise with the Managing Director to determine the most expedient manner of communication within twenty-four (24) hours of report of occurrence.
- Updated communications will come from the Incident Response Manager.

- Heads of Departments (HODs) must notify their subordinates of information that is confidential or not. However, HODs should be aware that any material or information communicated to employees could be leaked to the public, including the news media.
- All communication with news media shall be made in line with the Company's Communication Policy. Incoming news media, calls and requests for information will be directed to the Managing Director.

7. CYBER SECURITY INCIDENT PHASES

7.1 IDENTIFY

i. Overview

All employees of the Company have a responsibility to proactively protect data stored within the systems provided to them for work by the Company. Employees must report any event that threatens the confidentiality, integrity or availability of the internal information resources of the Company to their respective Supervisors or the IRM, if the Supervisor is unavailable. Supervisors should immediately bring the incident to the attention of the IRM.

ii. Incident Types

Types of cyber incidents that may threaten the Company's systems are:

- Unauthorized attempts to gain access to a computer, system or the data stored in the Company's electronic filing systems;
- Service disruption, including Denial of Service (DoS) attack;
- Unauthorized access to critical infrastructure such as servers, routers, firewalls, etc.;
- Virus or worm infection, spyware, or other types of malware;
- Non-compliance with security or privacy protocols;
- Data theft, corruption or unauthorized distribution.

iii. Incident Symptoms

Signs a computer may have been compromised include:

- Abnormal response time or non-responsiveness;
- Unexplained lockouts, content or activity;
- Locally hosted websites would not open or would display inappropriate content or unauthorized changes;
- Unexpected programs running;
- Lack of disk space or memory;
- Increased frequency of system crashes;
- Settings changes;
- Data appears missing or changed; and
- Unusual behavior or activity by the employees.

7.2 **ASSESS**

i. Overview

Once anomalous activity has been reported, it is incumbent upon the IRM to determine the level of intervention required. Other members of the IRT may be required to provide input during this phase to help determine if an actual security threat exists. If it is determined that there is an active security threat or evidence of an earlier intrusion, the IRM will immediately notify the entire IRT to deal with the situation in an expeditious manner.

ii. Considerations

- What are the symptoms?
- What may be the cause?
- What systems have been/are being/will be impacted?
- How wide spread is it?
- Which stakeholders are affected?

iii. Documentation

The IRM must accurately document all events in a Cyber Security Incident Log, whether or not the event amounts to a security threat. All Cyber Security Incident Logs will be stored in a single location for review of incident information in the future. The Log should contain the following information:

- Who reported the incident;
- Characteristics of the activity;
- Date and time the potential incident was detected;
- Nature of the incident (Unauthorized access, DoS, Malicious Code, No Incident Occurred, etc.);
- Potential scope of impact;
- Whether the IRT is required to perform incident remediation.

7.3 RESPONSE

i. Briefing of the Incident Response Team (IRT)

Where a significant incident or breach has occurred, the IRM must within two (2) hours of the incident inform the entire IRT of the nature of the incident or breach. As additional information are obtained throughout the investigation, the IRM should inform the IRT so that appropriate decisions, such as the allocation of additional employees, discussions with Management and/or the involvement of law enforcement can be made. Additionally, based on the incident, it will be incumbent on the IRM to consult the Managing Director to determine the appropriate stakeholders to notify of the incident and the appropriate medium to do so.

The IRM must take into consideration the nature of the information or systems involved, the scope of the parties affected, timeliness, potential law enforcement interests, applicable laws and the communication requirements of all Parties involved.

ii. Initial Response

This first steps in any cyber incident response should be to determine the origin of the incident and isolate the issue. This may involve measures such as an immediate disconnection of workstations, servers or network devices from the network to prevent additional loss. To further define the entire scope of the incident, the IRM must ensure that the firewall and system logs are examined and perform vulnerability scans, to ensure that the incident has not spread to other areas. Throughout this process, it will be critical to document evidence and all measures taken in detail. A thorough review and reporting on the incident will be required once the threat has been removed, the vulnerabilities have been removed and the systems has been restored.

iii. Remediation and Recovery

Once the cause has been determined and appropriately isolated, the IRT will remove the vulnerabilities leading to the incident. This may involve some or all of the following:

- Install patches and updates on systems, routers, and firewalls;
- Infected areas cleaned and removed;
- Re-image or re-install operating systems of infected machines;
- Change appropriate passwords;
- Conduct a vulnerability scan of any compromised machines before reconnecting them to the network;
- Restore system backups where possible;
- Document all recovery procedures performed and submit them to the IRM; and
- Closely monitor the systems once reconnected to the network.

7.4 REPORT

i. Overview

Once the threat has been mitigated and normal operation is restored, the IRM will compile all available information to produce an accurate and in-depth summary of the incident in an Incident Summary Report (ISR). A copy of the ISR is located in Appendix A. Throughout the incident, the IRT should keep the Incident Log, which contains detailed records of the incident, as the basis of the report. Interviews will also be conducted with appropriate members of the IRT to obtain additional information that may be available to augment the logs and records kept throughout the process.

ii. Report Contents

The Incident Summary Report (ISR) will include all pertinent information to the incident, such as:

- Dates and times of milestones throughout the process (e.g. incident detection, verification, notifications, remediation steps, completion, etc.);
- List of symptoms or events leading to discovery of the incident;
- Scope of impact;
- Mitigation and preventative measures;
- Restoration logs;
- Stakeholder communication (including copies of memos, emails, etc. where possible).

iii. Timeframe

The ISR should be prepared not later than one (1) week following the incident and future preventative measures may be taken as quickly as possible. Information to prepare the ISR and interviews with the IRT should be conducted immediately to ensure the greatest possible accuracy of information.

7.5 REVIEW

i. Post-Incident Review Meeting

After the conclusion of the incident, the IRM and possibly select members from the IRT will meet with Management to discuss the event in detail, review response procedures and construct a Process Improvement Plan (PIP) to prevent a reoccurrence of similar incidents. The compiled Incident Report constructed by the IRM will serve as a guide for this meeting.

In the meeting, a summary of the incident will be presented and findings discussed. The IRM will share the full scope of the breach (as comprehensively as possible), causes of the breach, how it was discovered, potential vulnerabilities that still exists, communication gaps, technical and procedural recommendations, and the overall effectiveness of the response plan.

As a whole, the group will review the information presented, determine any weakness in the process and all appropriate actions moving forward to modify the plan, address any vulnerabilities and what communication is required to various stakeholders.

ii. Process Improvement Plan

The IRM will draft a Process Improvement Plan (PIP) based on the results of the review meeting. The plan should discuss any applicable items necessary to prevent future incidents to the extent practicable, including cost and time frame requirements where possible. The PIP will also include a review strategy to ensure all recommendations made in the PIP are concluded timely. Areas of focus may include, but are not limited to:

- New hardware or software required;
- Patch or upgrade plans;
- Training plans (Technical, end users, etc.);
- Policy or procedural change recommendations;
- Recommendations for changes to the Incident Response Plan;
- Communication recommendations.

Additionally, the PIP must be kept strictly confidential for security purposes. Any communication required to external stakeholders must be drafted separately and include only information required to prevent future incidents.

8. REVIEW OF POLICY

This Policy shall be reviewed every five (5) years or as deemed necessary, in line with the applicable laws.

APPENDIX A: INCIDENT SUMMARY REPORT
INCIDENT SUMMARY

Type of Incident	
Date Incident Originated	
Date Incident Was Detected	
By Whom Was Incident Detected	
How Was Incident Detected	
Scope of Incident (Districts / Systems Affected)	
Date Incident Corrected	
Corrective Action Types (Training, Technical, etc)	

Summary of Incident Symptoms:

Summary of Incident Type and Scope:

Summary of Corrective Actions:

Summary of Mitigation Processes and Internal Communication:

APPENDIX B: PROCESS IMPROVEMENT PLAN

PROCESS IMPROVEMENT PLAN

Areas of Success Summary:

Areas in Need of Improvement Summary:

Recommended Improvements to Avoid Future Incidents:

Recommended Improvements to the Cyber Security Incident Response Plan

Improvement	Timeframe	Cost

APPENDIX C: INCIDENT LOG

INCIDENT LOG

Incident Title:
Incident Opened Date:

Incident Description

Action / Event	Date / Time	Performed / Reported by	Details

APPENDIX D: EMPLOYEE COMPLAINT FORM

Employees may file a complaint about a possible breach or improper disclosure of personal data of employees, vendors, customers, stored by the Company using this form. A privacy complaint may be made with the online form and the complaint sent to the Company's Data Protection Officer with a copy to the Incident Response Manager.

CONTACT INFORMATION

First Name: Last Name:

Phone Number: Email:

Role:

IMPROPER DISCLOSURE OR BREACH OF INFORMATION

Data Violation Occurred:

Description of Data Compromised:

APPENDIX E: EMPLOYEE COMPLAINT LOG

APPENDIX E: EMPLOYEE COMPLAINT LOG

Description of Improper Disclosure or Breach:

Additional Information:

Complainant Name	Date Complaint submitted
Description of the Complaint	
Findings	
Date the Report was Shared with Complainant	

Approved by the Board of Directors

This 8 **day of** April **2021**

Chairman