INFORMATION SECURITY POLICY – MIRI AFRICA LIMITED

INTRODUCTION

In addition to the Miri Africa's ("Miri") comprehensive data protection and data handling policy, this document establishes the framework of Miri's Information Security Policy ("Policy") which illustrates its commitment to protect the Confidentiality, Integrity, and Availability of the data and information of Miri stakeholders in the course of business.

PURPOSE

The purpose of Miri's Information Security Policy is to describe the actions and behaviors required to ensure that due care is taken to avoid inappropriate risks to Miri, its employees, its business partners, and stakeholders.

SCOPE

Miri's Information Security Policy applies equally to any individual, entity, or process that interacts with Miri's Information Resource.

DEFINITIONS

This Information Security Policy reflects the definitions below:

Confidentiality	means ensuring that information is accessible only to those persons that are authorized to have access
Integrity	means protecting the accuracy and completeness of information and the methods that are used to process and manage it
Availability	includes ensuring that information assets such as information, systems, facilities, networks, and computers are accessible and usable when needed by an authorized person
Data Protection Officer	includes any staff of Miri appointed by the management to supervise the administration and enforcement of this policy

POLICY

1. The Information Security Program:

Miri maintains and communicates an Information Security Program consisting of topic-specific policies, standards, procedures and guidelines that:

- serve to protect the Confidentiality, Integrity, and Availability of the Information Resources maintained within the organization using administrative, physical and technical controls;
- provide value to the way Miri conducts business and support institutional objectives;
- comply with all regulatory and legal requirements, including the Cyber Crime Act, Nigeria Data Protection Act, Nigeria Data Protection Regulation and the Freedom of Information Act.

The Information security program is reviewed not less than annually or upon significant changes to the information security environment.

2. Functional Information Responsibilities

2.1 The Executive Management shall be responsible for:

a. evaluating and accessing information risk on behalf of Miri;

b. identifying information security responsibilities and goals and integrating them into relevant processes;

c. supporting the consistent implementation of information security policies and standards;

d. supporting security through clear direction and demonstrated commitment of appropriate resources;

e. promoting awareness of information security best practices through the regular dissemination of materials provided by the Data Protection Officer or his representative;

f. implementing the process for determining information classification and categorization, based on industry-recommended practices, organization directives, and legal and regulatory requirements, to determine the appropriate levels of protection for that information;

g. implementing the process for information asset identification, handling, use, transmission, and disposal based on information classification and categorization;

h. determining who will be assigned and serve as information owners while maintaining ultimate responsibility for the confidentiality, integrity, and availability of the data;
i. participating in the response to security incidents;
j. complying with notification requirements in the event of a breach of private information;
k. adhering to specific legal and regulatory requirements related to information security; and
l. communicating requirements of this policy and the associated standards, including the consequences of non-compliance, to the workforce and third parties, and addressing adherence in third party agreements.

2.2 The Data Protection Officer shall be responsible for:

a. maintaining familiarity with business functions and requirements;
b. assessing compliance with information security policies and legal and regulatory information security requirements;
c. evaluating and understanding information security risks and how to appropriately manage those risks;
d. representing and assuring security architecture considerations are addressed;
e. advising on security issues related to procurement of products and services;
f. escalating security concerns that are not being adequately addressed according to the applicable reporting and escalation procedures;
g. disseminating threat information to appropriate parties;
h. participating in the response to potential security incidents; and
i. participating in the development of enterprise policies and standards that considers Miri's needs; and promoting information security awareness.

3. Information Classification and Handling

a. All information, which is created, acquired or used in support of business activities, must only be used for its intended business purpose;
b. all information assets must have an information owner established within the lines of business;
c. information must be properly managed from its creation, through

authorized use, to proper disposal;

d. all information must be classified on an ongoing basis based on its confidentiality, integrity and availability characteristics;
e. if Miri is unable to determine the confidentiality classification of information, the information must have a high confidentiality classification and, therefore, is subject to high confidentiality controls.
f. merging of information which creates a new information asset or situations that create the potential for merging (e.g., backup tape with multiple files) must be evaluated to determine if a new classification of the merged data is warranted;
g. all reproductions of information in its entirety must carry the same confidentiality classification as the original;
h. a written or electronic inventory of all information assets must be maintained;
i. content made available to the general public must be reviewed by the Data Protection Officer to ensure adherence to the company's disclosure policies and standards;
j. non-public information disclosed to any third party must be confirmed by the Data Protection Officer as appropriate, in accordance with processing principles, is on a need-to-know basis, necessary and on the same degree of data protection measures provided by Miri.

ENFORCEMENT

This policy shall take effect upon publication which may be amended at any time. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, and related civil or criminal penalties.

Signed by:

_____

Name:

Designation: