FOY GLOBAL
INVESTMENT LIMITED

INTEGRATED MANAGEMENT SYSTEM (IMS) POLICY STATEMENT

1.0 INTRODUCTION

This policy defines how Management Systems will be set up, managed, measured, reported on and developed within FOY GLOBAL.

The Executive Management of FOY Global, located at 19, Okotie Eboh Close, Ikoyi, Lagos, is committed to ensuring Information is secure, and Business continues by pursuing full certification to ISO/IEC 27001, and ISO 22301 that the effective adoption of Information Security and Business Continuity best practices may be validated by an external third party.

The Integrated Management System (IMS) is a comprehensive framework designed to systematically identify, assess, manage, and mitigate risks across our organizational processes and information systems. The IMS serves as a strategic tool that ensures our resilience, protects our information assets, and maintains the highest standards of cyber security and business continuity.

In driving these strategic efforts, FOY has set the following objectives of the IMS:

- Train employees on secure handling of sensitive data and business continuity practices.
- Improve response times to security and business continuity incidents
- Monitor and Review the performance and effectiveness of the BCMS and ISMS

(See IMS Objectives and Plan V1 Document)

2.0 POLICY OVERVIEW

FOY GLOBAL's current Integrated Management System (IMS) provides a structured approach for:

- Identifying and assessing organizational risks
- Evaluating potential impacts
- Implementing robust control mechanisms
- Ensuring continuous improvement of our information security practices.

3.0 RISK MANAGEMENT STRATEGY

Our risk assessment and risk treatment plan assess how identified risks are mitigated, aligned with the internationally recognized ISO 27001 for information security. Specific risks we address include:

- Phishing and social engineering attacks
- Potential data breaches
- Unauthorized system access
- Information integrity challenges
- Service failures, among others

4.0 RESPONSIBILITIES AND COMPLIANCE

FOY Commits to satisfy all applicable requirements related to information security;

Employee Responsibilities

All employees of FOY GLOBAL are expected to:

- Read, understand and comply with this IMS policy
- Participate in mandatory training programs and exercises
- Immediately report any security incidents or potential vulnerabilities

5.0 INCIDENT REPORTING PROCESS

Use the dedicated security incident reporting email: info@foyglobalinvestments.com

- Report incidents within 4 hours of discovery
- Provide comprehensive details using the standard incident report template

6.0 EXTERNAL PARTY ENGAGEMENT

For all external parties, including contractors, vendors, and strategic partners, they must:

- Undergo mandatory security awareness training
- Adhere to FOY GLOBAL's information security protocols
- Sign compliance agreements before accessing any company systems or doing business with us

7.0 CYBER RESILIENCE AND INFORMATION PROTECTION

FOY GLOBAL is committed to maintaining robust cyber resilience through;

- End-to-end data encryption
- Multi-factor authentication
- Regular security vulnerability assessments
- Continuous employee cyber security training

Continuous Improvement and Review

8.0 REVIEW PROCESS

- We have an internal audit and compliance manager who conducts quarterly reviews
- External cyber security consultants perform annual in-depth assessments and audits
- Key Performance Indicators (KPIs) monitored include:

* Mean time to detect security incidents
* Number of successful vs. blocked/mitigated cyber threats
* Employee security awareness training and results

The IMSCC owns this document and ensures annual review and Executive Management approval, with interim updates as required by significant organizational or technological changes.

9.0 DOCUMENT ACCESSIBILITY AND CONTROL

- A current version is available on the shared drive (IMS Project)
- Employees are notified of updates via company-wide email and internal communication platform
- This policy is version-controlled and signed by the MD

10.0 POLICY VIOLATION

While maintaining a supportive and educational approach, FOY GLOBAL has established a clear procedure for addressing policy violations:

1. Initial/First time violations trigger mandatory additional training
2. Repeated or severe infractions may result in disciplinary action
3. Significant breaches could lead to termination, according to the Cybercrime Prohibition Act 2015 Compliance is designed to protect both the individual and the organization, emphasizing correction and learning over punitive measures.

11.0 GLOSSARY OF TERMS

IMS: Integrated Management System

Cyber Resilience: An organization's ability to prepare for, respond to, and recover from cyber incidents

Information Asset: Any data, system, or resource critical to business operations

IMSCC: Integrated Management System Committee Chairman

12.0 DOCUMENT CONTROL

Effective Date: [09/12/2024]
Next Review Date: [One Year from Effective Date] Version:
1.0
Approved By:

AFOLAYAN VICTOR FOLUSHO