

Beta Glass Plc

Information Technology Governance Policy

Policy Number:

Review Number:

Responsible Person:

Approved by the Board on: 24th day of March, 2022

1. Introduction

Information is a valuable asset that is critical to the operation of the Company. The value of the Company's information as a company resource and asset is increased by its integrity and appropriate use; conversely, its value is diminished by insufficient capture, retention and destruction practices, compromised protections, or unnecessary restrictions on its access.

Information Technology governance will assist in reducing the legal risks associated with unmanaged or inconsistently managed information; providing reliable information for decision-making; and planning and allocating IT resources effectively.

The Company must employ appropriate safeguards to protect and manage information that is subject to various legal, regulatory, or contractual terms.

2. Purpose

The purpose of this Policy is to institute a framework that will ensure that the Company's information Systems are designed, deployed and implemented to ensure the integrity and confidentiality of data and information, avoid or prevent any breach of confidentiality of information, safeguard data and information, and ensure that information services are available as required and as needed by the Company.

AKK

3. Purpose and Context

The Company's prime objective is to promote good corporate governance and best business practices. It is the role of the Board to ensure that procedures and practices are in place to protect the company's assets and reputation. Information technology has a profound effect on processes within the Company and it is, therefore, essential for the Company to have a sound IT Governance Policy in place in line with legal requirements and the Code of Corporate Governance.

The intent of this Policy is to provide an enterprise framework that is based on the principles of information technology governance to guide the valuation, creation, storage, use, archiving, and deletion of information.

4. System Security

In addition to requirements of law, the use of the Company's information infrastructure is regulated through defined standards, policies and by Internal Control practices. The control systems shall be evaluated regularly to ensure they remain effective and result-oriented.

5. Systems Failure

There is a robust information technology structure that ensures there is consistency and that failure of the system network is prevented at all times. Any employee who engages in acts that are capable of leading to system failure will be sanctioned.

6. Data Backup & Recovery

All Company data is backed up in safe and secured environments in line with policies and rules set by the Company. The system is designed to ensure there is data protection and ease of recovery in the event of failure.

7. Virus Outbreaks & Protection

Effective tools shall be in place at all times to protect IT infrastructure against infections and virus outbreaks.

8. Application of this Policy

This Policy applies to the Company, including all units and departments of the Company.

JAR

9. Definitions

- a. **Information Technology (IT)** – the use of devices, such as computers, laptops, servers, cell phones, and other mobile devices and telecommunications equipment to receive, manipulate, transmit, store, retrieve, dispose and destroy data and information.
- b. **Responsible Officer** – the employee or officer of the Company who is charged with carrying out the responsibilities of an office including the implementation and oversight of policy administration.

10. Strategy

The Company strategy is to create and maintain a highly reliable and secured Information Technology environment to uphold the reputation, integrity and sustainability of the Company.

11.1 Responsibilities

I. The Risk and Board Audit Committee

- a. Report to the board on IT framework and effectiveness of control on IT related risk;
- b. Reviews the legal risks and ensures compliance with applicable laws, codes and best practice pertaining to IT;
- c. Reviews IT risk identification and management;
- d. Ensures that IT risks are adequately addressed. In understanding and measuring IT risks, the members of the committee should understand the Company's overall exposure to IT risks from a strategic and business perspective, including the areas of the business that are most dependent on IT for effective and continual operation;
- e. Obtains appropriate assurance that controls are in place and effective in addressing IT risks;
- f. Considers IT as it relates to financial reporting and the going concern of the Company;
- g. Ensures that the Business Continuity System is current and effective.

File

ii. Executive Management

Management is responsible for:

- a. Implementing the IT Governance Framework;
- b. Providing accurate and timely reports;
- c. Acting within the bounds provided by the policies and delegated authorities;
- d. Managing compliance;
- e. Monitoring IT service delivery and the achievement of agreed service levels;
- f. Continually improving the Company's management of information;
- g. Continually improving the Company's IT security infrastructure.

12. Commitment to this Policy

All Employees are expected to:

- ✓ Be aware of and understand this Policy, and seek guidance as required;
- ✓ Comply with this Policy and understand that compliance is required;
- ✓ Identify and immediately report any suspected or known violation of this Policy.

13. Compliance

The Company's data and information are secure and the Company has put systems in place to ensure there is compliance with applicable laws and international standards. There is also a system of risk management which is part of the Company's overall risk management system.

The company has instituted processes and procedures in compliance with Nigerian Data Protection and Regulation (NDPR) 2019.

14. Failure to Comply

It is every Employee's responsibility to understand this Policy and to comply with it and other the Company's Policies. Failure to comply may result in disciplinary action including impacts to performance ratings, impacts to an Employee's compensation, and termination of employment (with cause).



15. Applicable Laws

The laws, regulations and guidelines that govern the Company shall complement and apply to this Policy and all parties to this Policy are expected to know and comply with these laws and regulations at all times.

16. Attestation

All Employees are required to sign an attestation annually that they have read this Policy and understood their obligations to comply with the principles, policies and laws outlined in this Policy.

17. Review & Amendment

The Board will review this Policy as the need arises and the Policy shall not be amended, altered or varied unless such amendment, alteration or variation shall have been approved by a resolution of the Board.

18. Questions

For any questions about this Policy, the Chief Financial Officer may be contacted.

19. Approval of this Policy

The Board of Directors of Beta Glass PLC approved this Policy this 24th day of March, 2022



Chairman



Secretary