INFORMATION SECURITY POLICY STATEMENT

The management of Greenwich Registrars and Data Solution Limited ("GRDS") recognizes that her activities and operations require a level of security to be determined and enforced. We are committed to continually improving an Information Security Management System (ISMS) to ensure that data and information systems are adequately protected against the loss of confidentiality, integrity, and availability.

We are committed to ensuring that in business operations and the delivery of our services clients, shareholders, staff members, and other stakeholder requirements are determined and met with the aim of enhancing satisfaction.

Information Security Management System
In support of our commitments, the Information Security Management System ("ISMS") has been developed and is appropriate to the nature, scale, and impacts of our activities, products, and services.

The Information Security Management System and its associated organizational arrangements, systems, and procedures will be reviewed at least annually and revised as necessary to ensure its continuing suitability.

The Objectives of implementing and maintaining an Information Security Management System ("ISMS") for the benefit of all stakeholders include:

- ✓ To ensure 99% protection of GRDS information assets and systems from unauthorised access.
- ✓ To ensure 100% compliance with legal and regulatory requirements addressing information security.
- ✓ To ensure 99% of information security risks and cyber threats are reduced and are effectively managed.

To achieve the Information Security objectives, GRDS has established Information Security Policies:

- **Project Management Policy:** A policy regulating how projects are planned, executed, and delivered based on proven project management methodologies, to ensure projects are completed on time and on budget.
- **Mobile Device Policy:** A policy which establishes rules for how mobile devices are used and secured within an organization.
- **Remote Working Policy:** A policy that regulates employees that work from a non-office location.
- **Acceptable Use Policy:** A policy stipulating constraints and practices that a user must agree to for access to a corporate network, the internet, or other resources.
- **Information Labelling and Classification Policy:** A comprehensive policy used to categorize an organization's stored information based on its sensitivity level, ensuring proper handling and lowering organizational risk.
- **Access Control Policy:** A policy that specifies how access is managed and who may access information under what circumstances.
- **Password Policy:** The policy establishes standards for the creation of strong passwords, the protection of those passwords, and the management process for all organization information systems and services.
- **Cryptographic Policy:** This policy establishes requirements for the use and protection of cryptographic keys throughout their entire lifecycle.

- **Clear Desk and Clear Screen Policy:** A policy which ensures that all sensitive/confidential materials are removed from an end user workspace and locked away when the items are not in use, or a user leaves his/her workstation.
- **Change Management Policy:** The guiding standard that describes the procedures for and specifies the rules and levels of authorization required to approve, different types of Changes.
- **Malware Protection Policy:** A policy designed to protect systems from cyberattacks and malware attacks.
- **Backup Policy:** *A* set of rules and procedures that describe the organisation's strategy when making backup copies of data for safekeeping.
- **Software Policy:** This policy sets out how software will be acquired, registered, installed, and developed within GRDS. This policy also sets rules to manage versions of the software and related documentation used in GRDS.
- **Capacity Management Policy:** A policy which ensures optimal utilization of capacity in terms of IT infrastructure, resources and capabilities to meet the agreed current and future business requirements.
- **Network Security Policy:** A formal document that outlines the principles, procedures and guidelines to enforce, manage, monitor and maintain security on a computer network.
- **Solution Delivery Life Cycle Policy:** A policy which ensures a clear definition of goals and stages of building or purchasing a software solution.
- **Managing Third-party Vendor Policy:** A policy which establishes guidelines and practices for how organizations assess, monitor, remediate and report on the risk posed by vendors, suppliers, and business partners.
- **Incident and Problem Management Policy:** This policy’s purpose is to restore agreed IT services as soon as possible and to minimize disruptions by proactive identification and analysis of the cause of incidents and by managing problems to closure.
- **IP, Copyright, and Software Licensing Policy:** This policy aims to protect GRDS’ Intellectual Property and minimize the possibility of infringement of the Intellectual Property rights of the organization and the third parties.
- **Records Management and Data Retention Policy:** GRDS has adopted this Policy as its approach to managing Personal Data as well as all company data or records from the point of collection or creation, through to use, storage/retention and disposal/destruction.
- **Records Management and Document Retention Policy:** The policy was established to aid in dealing with all issues identified with paper records storage and to eliminate unnecessary retention of paper records.
- **Data Protection Policy:** This Policy sets out how GRDS collects, processes, and stores the personal data of its employees, customers, clients, contractors, vendors, and other third parties. It sets rules and guidelines that inform how ongoing compliance with data protection laws should be ensured in GRDS.
- **Patch Management Policy:** A set of guidelines to ensure controlled, efficient, and secure patching of GRDS systems.
- **Bring Your Own Device (BYOD) Policy:** A policy that allows employees in an organization to use their personally owned devices for work-related activities.

The Information Security Policies will be provided and made available to all relevant stakeholders.

The Information Security Policies will be reviewed periodically to take account of applicable local, statutory, regulatory, and customer requirements and any changes in business activity.

The Information Security Policies are applicable to all GRDS' employees, its contractors, its consultants, and other individuals affiliated with Third Parties who have access to GRDS' information or business interest.

Our Commitments:

Compliance
To comply with all relevant legislation, regulations, and other requirements specifically related to our business activities.

Communications
To ensure our policy is brought to the attention of all our people and seek their co-operation in supporting the management in its efforts to establish and maintain our information security objectives. To ensure our policy is available to potential and existing clients and other interested parties through conventional marketing methods and on our website.

Continual Improvement
To the continual improvement of our management systems and our performance to reach our ISMS objectives. This is achieved by consultation with members of staff, clients, and other interested parties and by Management Review.

Resources
To determine and ensure the provision of the necessary resources to allow us to achieve our objectives for information security.

Competence
To determine the necessary competence of our people and to ensure through training and experience they are competent to undertake their duties. To provide guidance and assistance to enable all our people to understand and carry out their responsibilities about the requirements of the ISMS.

Awareness
To promote a workplace culture of increased information security in our people.

Suppliers and Contractors
To satisfy ourselves that any organization which is contracted to carry out any work of a critical nature to us can demonstrate that it pays due regard to our information security requirements in relation to the product and services they supply to us.

For further enquiries on the Information Security Management System, or to report suspected information security incidents or weaknesses, kindly contact the Risk and Control unit: riskandcontrol@gtlregistrars.com

The responsibility to achieve Information Security objectives and enjoy the benefits of the ISMS strongly depends on every stakeholder in Greenwich Registrars and Data Solutions Limited. All stakeholders are encouraged to ensure they play their part in delivering GRDS' Information Security objectives.

Thank you.

Kayode Falowo
Board Chairman