AFRICA CLEAN ENERGY SOLUTIONS LIMITED

STATEMENT OF MAJOR ACCOUNTABILITIES

This Statement sets out the Main Accountabilities of the Board.

The Board oversees the general business of the group. The entire Board is responsible for such supervision and oversight.

The Board shall act in the best interests of the group and its business, taking into consideration the interests of the group's shareholders and other stakeholders.

The Board is responsible for the performance of the group, for achieving sustainable growth and for quality of its own performance.

The Board assumes the responsibility for compliance with law and regulations. The Directors are aware of their legal duties.

The Board Charter and Board role descriptions, which have been approved by the Board, provide a full definition of the roles and responsibilities of the Chief Executive Officer, Chief Financial Officer, Chief Operating Officer and Chairperson.

Approval by:

Chairperson of the Board

Chief Executive Officer

AFRICA CLEAN ENERGY SOLUTIONS LIMITED

IT SECURITY POLICY

This policy is designed to ensure that within Africa Clean Energy Solutions Limited and its subsidiary and associate companies ("Group") there includes protection of IT assets, fostering a culture of security awareness, identifying, and remedying security incidents and reassuring third parties that there is a robust IT security protocol in place.

This policy applies to all Directors, Employees, Contractors, and anyone else who accesses information, applications, systems, or equipment ("Users").

Users Responsibility

Users are responsible for protecting the Group's information and technology systems and for complying with this policy.

Where an individual user suspects personal data may have been compromised, they must notify the Data Protection Officer (DPO) immediately.

Password Policy

Unless otherwise specified within this IT Security Policy, the following security requirements should be adhered to when creating passwords;

a. Minimum of eight (8) characters in length, containing characters from all of the following categories;
    a. Uppercase
    b. Lowercase
    c. Numbers
    d. Special characters ie !"£$
b. Must not be the same as or include the user id or be visible when entered
c. Must not be easily guessable

Proper Use of Email

Only open email attachments received from known trusted sources. Any email attachments received otherwise should never be clicked on and/or opened and the email should be deleted.

Group email addresses should not be used to send or receive personal emails.

Email signatures must be in the prescribed Group format.

Acceptable Use of the Internet and Social Networking

Personal internet browsing should be contained to non-working hours.

It is encouraged to link Users own LinkedIn Profile to the Group LinkedIn profile, and for Users own LinkedIn Profile to detail their new role within the Group.

Anti-Virus and General Software

Anti-Virus software is installed and updated on all User IT Equipment.

Only approved Group software is to be installed on Group IT Equipment.

All software installed is monitored by external IT providers and is kept up to date.

Physical/Hardware Security

Certain roles within the Group require the issue and use of laptops and mobile phones. Upon Hardware being issued, a physical record of the Equipment will be listed, and User signature will be taken, identifying the User and the Equipment.

All Group physical files and paperwork should not leave the offices.

When away from your desk, it is important to lock your computer screens when not in use.

All Group mobile devices (including, without limitation, laptops, tablets, mobile telephones) should be kept securely by Users using secure cases where appropriate. Users should not leave such mobile devices unattended other than at their homes or Group premises.

Users are not permitted to connect any of their personal hardware to the IT Systems without express approval of the Board in writing.

Where Users are required to work remotely or from home, it is the User's responsibility to ensure that Group IT systems are secure. When travelling with Group IT systems, the Equipment should be secured in the boot of the Users vehicle.

It is the responsibility of the User to ensure that computer equipment used for home working are themselves properly secured.

Users are responsible for the safeguarding of IT Systems against unauthorised access, misuse, theft, damage or loss when in their home or in transit.

Users must comply with the security requirements of this document, at all times, and where personal data is being processed, they must also comply with the Protection of Personal Information Act (POPIA).

Users must not access internal or confidential/sensitive information over unsecured broadband or public wireless networks as these present a security risk. Users should also be aware of the physical environment when working remotely ensuring no one is looking over their shoulder at information on screen.

Office access fobs and keys should be safeguarded against theft or loss, when at home or in transit. When last to leave the office, Users are responsible to ensure the office is securely locked.

Responding to a Breach in Security

As in all cases of security while the Group endeavours to do everything it can to prevent the attacks and outcomes described the preventative measures are not always successful. In the case of a breach the following steps will be taken in each case:

a. Data Loss – Data will be restored to the active system
b. Data Theft – In line with POPIA individuals and organisations affected by the theft of data will be informed as soon as possible.
c. Virus/Malware Detection – Attempts will be made to establish what the virus/malware is, what it is doing and where it came from before being removed.
d. Physical Theft/Damage – Equipment will be replaced as soon as possible to prevent disruption to the operation of the Group.
e. Breach of Security – The root cause will be found and steps put in place to prevent the same kind of breach happening again.

Policy Violation Procedure

Any Users found in violation of this policy will be subject to the company's disciplinary procedures and where in violation of the law will be reported to the relevant authorities. Due to the varying severity of such violations, the action taken by the Group will be judged on a case by case basis.

Authority

This policy may be amended by the Board at its sole discretion without prior notification and will be reviewed annually.

Approval by:

Chairperson of the Board

Chief Executive Officer

AFRICA CLEAN ENERGY SOLUTIONS LIMITED

MONITORING AND REVIEW OF PROCESS DOCUMENTS POLICY

This policy ensures that process documents are adequately maintained and up to date.

The following best practice is implemented:

- Clear, concise process documents are to be retained
- Master documents should be easy to edit and update
- Control of document changes is to be maintained
- Finalised documents to be filed in pdf prior to general distribution
- Process documents should be accessible to all
- Review of charters, policies, and manuals to be undertaken annually

Approval by:

Chairperson of the Board

Chief Executive Officer

AFRICA CLEAN ENERGY SOLUTIONS LIMITED

CONFLICT OF INTERESTS – RELATED PARTY TRANSACTIONS POLICY

This policy is designed to ensure that every Conflict of Interest and Related Party Transaction is conducted in a manner that will protect Africa Clean Energy Solutions Limited and its subsidiary or associate companies ("Group") and is appropriately disclosed.

A Related Party is considered as follows:

a. A person or a close member of that person's family who:
    - Has control, joint control or significant influence over the Company or other member of the Group; or
    - Is a member of the key management personnel of the Company or other member of the Group.
b. An entity where any of the following conditions applies:
    - The entity and the Company are members of the same Group (which means that each parent, subsidiary and fellow subsidiary, associate, joint venture is related to the others);
    - The entity is controlled or jointly controlled by a person identified (a), or has significant influence over the entity or is a member of key management personnel
c. Related parties include, directors, shareholders, senior officer, immediate family members of the same.

Related Party Transaction Review, Approval and Reporting

a. All related party transactions should be conducted at arm's length;
b. Where in doubt whether a transaction is at arm's length, approval must be sought from the Audit and Risk Committee;
c. Related parties involved in the said transaction must be excluded from the approval, execution and monitoring process;
d. A register of related party transactions should be maintained.

Conflict of Interest and Disclosure

Directors and Employees of the Group may be exposed to situations that potentially raise conflict of interests. A conflict of interest is a situation in which a person has, directly or indirectly, a personal, professional or business interest sufficient to appear to influence that objectivity of his/her duties within the Group.

a. Directors and Employees shall not allow such direct or indirect interest to conflict with their duties and take precedence over the Group's interest.
b. Such an interest must be disclosed to the Board.
c. Decisions to enter into transactions in which there are conflicts of interest with Board members or Employees require the approval of the Board.

Authority

This policy may be amended by the Board at its sole discretion without prior notification and will be reviewed annually.

Approval by:

Chairperson of the Board

Chief Executive Officer