DATA PROTECTION POLICY

1. Objective

The objective of this policy is to protect the personal information processed by or disclosed to staff AfriCert or other authorized persons (all hereinafter referred to as Data Owners and Data Users) ensuring its confidentiality, integrity and availability by processing it in accordance with current legislation.

2. Responsibilities of staff and authorized third parties

2.1 C.E.O

On behalf of the Board of Directors, the C.E.O is responsible for approving the Data Protection policy and for ensuring that it is discharged to Staff.

2.2 Data Owner

A Data Owner is responsible for:

1. ensuring that the data is kept up-to-date and that amendments are made promptly following notification of changes.
2. ensuring that the security measures are appropriate for the types of personal data being processed;

2.3 Data Use

All staff and authorized third parties when processing personal data about others, whether held manually or electronically, are responsible for working in compliance with the Data Protection principles.

2.4 Data Subject

As Data Subjects, all staff, operators and authorized third parties are responsible for:

1. ensuring that any personal information that they provide to AfriCert in connection with their employment or other contractual agreement is accurate;
2. informing AfriCert of any changes to any personal information which they have provided, e.g., changes of address;
3. responding to requests to check the accuracy of the personal information held on them and processed by AfriCert, details of which will be sent out from time to time, and informing AfriCert of any errors or changes to be made.

2.4 Data Processor

A Data Processor, or Computer Bureau, will have the contractual responsibility to ensure that any processing of personal data carried out on behalf of AfriCert is done in compliance with AfriCert's Data Protection policy

3. Data Security

It is the responsibility of all staff and any third parties authorized to access AfriCert's personal data sets to ensure that those data, whether held electronically or manually, are kept securely and not disclosed unlawfully, in accordance with AfriCerts's Data Protection Policy.

Unauthorized disclosure will usually be treated as a disciplinary matter, and could be considered as constituting gross misconduct in some cases.

4. Subject Consent to Processing

It will be assumed that consent has been given by the Data Subject for his/her personal data to be used for the purposes advised at the point of collection of that data.

5. Rights of Access to Personal Information

AfriCert respects the right of individuals to access and check the accuracy of any personal data that is being kept about them, either on computer or in a relevant filing system.

6. Publication of AfriCert's Information

It is AfriCert's policy to make as much information public as possible and, in particular, the following type of information may be available to the public through the AfriCert's publications or otherwise by inspection:

- Names of members of the Board of Directors
- List of staff, their internal telephone numbers and corporate e-mail addresses
- Photographs of staff
- Publications dataset
- Job title and grade of staff
- Business achievements e.g. New Accreditations

Any individual who has good reason for wishing details in these lists or categories or other personal data to remain confidential should contact the relevant Data owner.

7. Retention of Data

Personal data processed for any purpose shall not be kept for longer than is necessary for those purposes or as required to comply with other legislation. Some forms of information will be kept for

longer than others and a guide to retention time will be found in the respective certification protocols and the law.

8. Policy Awareness

A copy of the Policy Statement will be given to all new members of staff and to newly-authorized third parties. All staff and authorized third parties will be advised of the existence of this policy which will be posted on AfriCert's website, as will any subsequent revision of the policy. All staff and authorized third parties are to be familiar with and comply with the policy at all times.

9. Policy Implementation and Review

This policy is issued by the authority of the C.E.O, who has delegated the implementation of it to Data owners. The C.E.O will facilitate an annual review of the policy.

10. Redress

Any Data Subject, who considers that the policy has not been followed in respect of personal data about themselves, should raise the matter with the relevant custodian, as appropriate. In the case of staff, if the matter is not resolved it should be raised as a formal grievance. In the case of Third Parties, they should refer the matter to the designated Data Controller.

11. Status of the Policy

This policy does not form part of the formal contract of employment, but it is a condition of employment that employees will abide by the rules and policies made by AfriCert from time to time.

12. Data protection risk analysis.

Risk Levels

1. High
2. Medium
3. Low
4. No risks.

Type of Information / Data	Identified risk	Level of risk	Measures taken to eliminate or minimize the risk
1. Client's information in form of emails, Photos, printed copies or recorded media.	• Intentional sharing with unintended recipients by AfriCert staff. • Unintentional transfer of client's information to unintended	3 3	• AfriCert staff bound by confidentiality agreement not to share client's data in an unauthorized manner. • AfriCert Staff trained on matters of confidentiality. • Electronic forms of client information required to be handled and stored as per

	recipients. • Hacking	3	AfriCert's data protection policy. • Photos and scanned/ electronic document copies should not be held for long in personal gadgets but transferred to safe platforms provided by AfriCert as soon as possible. • Sensitive information for clients such as certificates and reports are maintained in their own folders in the server. These folders are only accessible to specific authorized staff in the CB. • Printed copies should always be filed in the relevant files and stored in locked cabinets for safety. • Emails to be secured on the server and with passwords. • Threat protection: • Detect known and unknown malware proactively including viruses, worms, Trojans, spyware, adware, suspicious files, suspicious behavior, potentially unwanted applications (PUAs) and more • Get antivirus, firewall, application and device control in a single agent • Keeping security software up to date
2. Certificates, emails, audit reports and other important information/ documents from AfriCert to the clients.	• Certificates sent to the wrong address. • Emails or information sent to the wrong addresses. • Audit Reports sent to persons who have left the audited organizations.	3 2 3	• Create a concise register of client contact information. Avail this register to all necessary staff (Scheme Managers, Certification Officer, Accounts department, Office Administrator, C.E.O.) and always refer to this register for accurate contact information.
3. Electronically stored data in data storage devices (Server, computers etc)	• Breakdown or malicious infection of data storage facilities by malware		• Sensitive / important data to be stored in two backup systems.

4. Data processing devices. (Computers, phones, flash disks / USB etc.	• Possible intentional access and retrieval of data from the storage devices by unauthorized persons. • Accidental access to information on the devices by unauthorized persons.	2 2	• All devices containing AfriCert's work must have pass word protection. • No one should disclose the sensitive passwords protecting information or data. • No sending of sending/sharing of client information via social media platforms. • Computers and other devices holding AfriCert or client's information should not be left open and unattended. • The files devices should be locked when unattended in a way that they can only be opened using a password. • USB used to transfer information should have only intended files in them. • Personal devices should be avoided for storing or transferring CB related information and where necessary be used in a very limited way, for the shortest time possible and with utmost care. The information should then be transferred to the company server and deleted from the personal device as soon as possible.
5. Important / sensitive emails.	• Possible interception of emails or delivery to the wrong address.	3	• The IT desk at AfriCert to establish a way of filtering sensitive emails such that they can only be accessed by the recipients by use of very secure pass words.

Appendix 1 - Definition of the Terms used in this Policy

Data information which -

a) is being processed by means of equipment operating automatically in response to instructions given for that purpose; or,
b) is recorded with the intention that it should be processed by means of such equipment; or,
c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system; or,

Personal Data: data which relate to a living person/ Company who can be identified from those data or from those data together with other information which is in the possession of, or likely to come into the possession of the Data Controller.

Data Controller: a member of AfriCert who, either alone or jointly, determines the purposes for which and the manner in which any personal data are, or are to be processed. Technically, the Data Controller is the AfriCert's Board, which delegates that responsibility to the C.E.O and then by her to one or more designated Data Controllers.

Data Processor: a person, other than staff of AfriCert, who, or an organization which processes personal data on behalf of the Data Controller

Data Subject an individual/ Company who is the subject of personal data

Data Owner an authorized user of AfriCert's information system, whether manual or electronic, who originates, stores, or edits material held in that system and/or publishes material either manually or electronically subject to the security procedures laid down by the Custodian of that system.

Data User a person authorized by a Custodian to process personal data either on a networked system or on a stand-alone system.

Custodian a person appointed by the C.E.O to be responsible for ensuring that the security measures adopted for AfriCert's Information system, meet the requirements of the Information Systems Security

Processing - obtaining, recording or holding personal data or carrying out any operation on the data including organization, adaptation or alteration of that data, retrieval, consultation or use of the data for disclosure by transmission, dissemination or otherwise making the data available, or alignment, combination, blocking, erasure or destruction of the data.

Relevant Filing System: any set of information relating to individuals not processed automatically that is structured in such a way that specific information relating to a particular individual is readily accessible.

Appendix 2 - The Data Protection Principles

When processing personal information, the following seven principles must be complied with and data must:

1. be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met.
2. be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose.
3. be adequate, relevant and not excessive for those purposes.
4. be accurate and kept up to date.
5. not be kept for longer than is necessary for that purpose.
6. be processed in accordance with the Data Subject's rights.
7. be kept safe from unauthorized access, accidental loss or destruction.

Staff or others who process or use any personal information for AfriCert must ensure that they follow these principles at all times.