

ICT SECURITY POLICY

1. It is the policy of Agrobank that while IT resources and information should be provided to enable employees of the Bank and relevant external parties to satisfactorily complete their duties, these resources should be subject to adequate control :-
 - 1.1. To ensure the protection of programs, information and facilities of the computerized information processing systems from unauthorized access and use.
 - 1.2. Minimize the risks of unauthorized disclosure of information
 - 1.3. The protection of information stored on the information processing facilities from loss or destruction.
 - 1.4. The reliability of the computerized information processing and the continued availability of the computerized information processing facilities.
2. The control implemented will be suitable of the asset value and its risk exposures. This policy will form the basis from which IT security standards and procedure are developed.
3. IT security objectives are defined as follows:-

3.1. Integrity of information

Information produce by IT resources of Agrobank source must be free from unauthorized modification and corrupted information. The attributes of integrity of information shall be as follows.

- 3.1.1. Transactions are authentic and unique (valid).
- 3.1.2. Transactions are recorded as intended (accurate)
- 3.1.3. Transactions are not missing (completeness)
- 3.1.4. Transactions are up to date (pertinence).
- 3.1.5. Transactions are not recorded in a misleading manner (presentation)

3.2. Confidentiality of information

The access to the information of Agrobank and its clients is to be allowed on a need to know basis. Here are some examples on how Agrobank protects its clients online:

- 3.2.1 Agrobank use Anti-virus protection to help detect and prevent viruses.

3.2.2 Agrobank's firewalls help block unauthorized access by individuals or networks.

3.2.3 Agrobank online website's Secure Socket Layer (SSL) encryption creates a secure connection with its client's browser when login, or fill out an application, or register in online services. This protects information from being intercepted.

3.2.4 Agrobank does not and will not share the client's usernames and passwords with anyone—and strongly recommend that the client don't share theirs either.

3.2.5 AgroBank online website automatically log client out of their secure session after a period of inactivity to help protect against others seeing or trying to use the online accounts.

3.3. Source and information continuity during interference

Each source and information of necessity for Agrobank's business process is at levels that could be accepted by Management and availability in during interruption duration that could be accepted by Management.

3.4. Compliance with statutory and regulatory requirements

The information processing system of the Bank must at all times be in compliance with all statutory and regulatory requirements.