

## ICT SECURITY POLICY

1. Resources and information on ICT shall be accessible to the relevant staff and external party to enable them to perform their duties. The resources shall be subjected to sufficient control, namely:-
  - 1.1 To ensure protection on the programming, no access and application of information and system facilities on computerized information processing shall be allowed without authorization;
  - 1.2 To minimize the risk of unauthorized disclosure;
  - 1.3 To ensure every information are accurate and correct;
  - 1.4 To protect the information kept in the information processing system facilities from damage or lost.
  - 1.5 Integrity of computerized information processing and availability of information processing and continuity of the facility computerized information processing .
  - 1.6 To ensure access only to authorized users or receiving information from authorized sources.
  
2. The control which are implemented should be suitable with the asset value and risk exposures. The control measures shall be based on relevant assessment with current changes on natural weakness of ICT assets, any threat due to such weakness, any possible occurring risks, and any suitable preventive measures that need be taken in dealing with such risk.
  
3. Security features on the information are as follows:-
  - 3.1 Information integrity  
Information produced by Bank's ICT source must be free from unauthorized modification and not corrupted.
    - 3.1.1 Transaction are genuine and unique.
    - 3.1.2 Transaction are be accurate
    - 3.1.3 Transaction are complete
    - 3.1.4 Transaction are updated.
  
  - 3.2 Secrecy of information  
Information should not be disclosed easily without authorization and consent and access on the Bank and Customer information should be allowed based on the need to know basis.
  
  - 3.3 Cannot be disputed  
All data and information shall be from an authorized source and are not disputable data.
  
  - 3.4 Correctness of Information  
All data and information shall be guaranteed on its correctness.
  
  - 3.5 Continuity of source and ICT information during disruption  
Every source and information required for the Bank's business process is at the level acceptable to the Management and available even during disruption which can be accepted by Management
  
  - 3.6 Compliance with the statutory and regulatory requirements  
Bank information processing's system shall at any time in compliance with statutory and regulatory requirements