1. Purpose

The purpose of Salaam African Bank's Third-Party Information Security Policy is to define Information Security Requirements for contractors, suppliers, consultants, partners and any other third parties accessing its Information Assets and/or responsible for rendering Information Assets related service related to Salaam African Bank.

2. Scope

It applies to:

a. All Salaam African Bank partners, suppliers, consultants, and contractors with access to Salaam African Bank's Information Assets and/rendering any Information Assets related services to Salaam African Bank.
b. Employees, representatives, and agents from other organizations who directly or indirectly support Salaam African Bank's information systems, including auditors and other external consultants.
c. All Salaam African Bank departments, the office building, and data center, including all information assets and information processing facilities without exception.

3. Policy

Prior to entering into any agreement or contract, Salaam African Bank staff shall follow due diligence in selecting third party vendors. Third parties must comply with all applicable procurement, Salaam African Bank policies, practice standards, and agreements as well as any binding legislation at the industry and national levels. This policy supports law in certain areas but shall not replace any potential changes in current or future compliance components levied against third party vendors through statute, law, or contract.

4. General Vendor Responsibilities

The following general responsibilities shall be provided by vendors entering contracts with Salaam African Bank:

- Third party vendors shall provide Salaam African Bank with a point of contact for contract terms and service offering implementation. A Salaam African Bank point of contact will work with the third-party vendors to ensure the vendor complies with all industry and national laws as well as this policy.

- The Head of the Administration Department shall maintain a list of all subcontracted providers and the services performed by each.

4.1 Third Party Contract Terms and Provisions

All contract terms and agreements with third party service providers shall specify the following terms and conditions:

- Data and personnel confidentiality terms shall protect all Salaam Bank Confidential Information and Personally Identifiable Information (PII).

- Role-based controlled user access to Salaam Bank resources and access shall be limited to only those systems to which the vendor provides services.

- Vendor data privacy and information security procedures and protocols shall be made available and meet Salaam Bank requirements for the return, destruction, or disposal of information in the service provider's possession at the end of the agreement.

- The service provider shall only use Salaam Bank information and systems for the purpose of the direct business agreement. No other uses are allowed unless expressly granted in writing by Salaam Bank.

- Any information acquired by the service provider through the course of operational contract execution shall not be used for the service provider's own purposes or divulged to others without the express written consent of Salaam Bank.

- Service providers shall provide Salaam Bank with a list of all staff working on the contracted services. The list shall be updated and provided to Salaam Bank within the stipulated time of staff changes.

- On-site service provider staff members must adhere to all internal facility security protocols and procedures. Upon completion of contracted work, service providers shall return all security access cards and identification.

- Service provider staff members with access to Salaam Bank confidential or client Personally Identifiable Information must be cleared to handle that information. Third party access to Personally Identifiable Information and confidential data shall be activated only when needed and enabled only to the level and degree indicated by the contract statement of work.

- System access shall be deactivated/disabled after services have been completed. IDs used by vendors to access, support, or maintain system components via remote access shall only be enabled during the time needed and disabled when not in use.

- Third party service provider access to systems and software shall be monitored during use as necessitated by the sensitivity and confidentiality of the information.

- Service providers with remote access to Salaam Bank systems shall use all prescribed tools and procedures to access systems remotely.

- Service provider personnel shall report all security incidents directly to the project supervisor and the Information Security Team. Security incident management responsibilities and details must be specified in the contract agreement and specific to data incident/breach notification, procedures, notifications, and remedies.

- Service providers shall follow all applicable Salaam Bank change control processes and procedures when working on Salaam Bank systems.

- Regular work hours and duties shall be defined in the agreement. Work outside of defined parameters must be approved in writing by appropriate Salaam Bank management.

- Service provider access shall be uniquely identifiable and password/access management must comply with all Salaam Bank requirements.

- Upon termination of service provider or at the request of Salaam Bank, the service provider will return or destroy all information and provide written certification of that return or destruction within 48 hours.

- Upon termination of contract or at the request of Salaam Bank, the service provider must surrender all identification badges, access cards, equipment, and supplies immediately. Equipment and/or supplies to be retained by the service provider must be documented by management.

- Service providers are required to comply with all Salaam Bank auditing requirements, including the auditing of the service provider's work.

- Service providers shall include explicit coverage of all relevant security requirements. This includes controls over the processing, accessing, communicating, hosting, or managing the organization's data or adding or terminating services or products to existing information.

- Service providers should include explanations of security mechanisms (e.g., encryption, access controls, and security leakage prevention) and integrity controls for data exchanged to prevent improper disclosure, alteration, or destruction.

- Service provider contracts shall require the provider to acknowledge responsibility for securing Salaam Bank sensitive information the provider possesses or otherwise stores, processes, or transmits on behalf of Salaam Bank.

- Agreements with third party service providers shall specify that the third-party service provider will notify Salaam Bank within one (1) day of discovery of a service provider security incident/breach. Upon such notification, Salaam Bank shall have the right to terminate the agreement with the service provider. Provisions within the contract shall ensure the service provider pays for all costs incurred to remedy the breach including, if appropriate, notifying customers, and any related expenses or damages levied due to the incident and related disclosure.

4.2 Other Stipulations

When dealing with Personally Identifiable Information, service providers shall provide an on-line and print description of security and privacy directives, guidelines, policies, and security safeguards that protect customer information.

No contracts shall be entered into by Salaam Bank where the standard vendor contract template is not used, and all applicable terms applied. Any negotiations between vendor and Salaam African Bank must be completed through the Administration department.