fsduganda
Financial Sector Deepening

BILL & MELINDA GATES foundation

UKaid
from the British people

FINANCIAL SECTOR DEEPENING UGANDA

Promoting inclusive financial markets that foster job creation, reduce poverty, and improve Uganda's competitiveness

Compliance guidance tool to guide FITSPA members on the implementation of NPS Act 2020

June 2021

NPS Regulations - Overview

Overview of National Payment Systems Act, 2020 (1/2)

The National Payment Systems Act was passed by Ugandan parliament in May 2020 and gazetted in September 2020.
The objective of the Act is to regulate payment systems, provide for the safety and efficiency of payment systems; provide for the functions of the central bank in relation to payment systems; prescribe the rules governing the oversight and protection of payment systems; provide for financial collateral arrangements and regulate payment service providers; issuance of electronic money, and oversight of payment instruments.

The Bank of Uganda has released several regulations to guide on the implementation of the Act. These include:

- National Payment System(NPS) regulations
- Agent regulations
- Sandbox regulations

Before the Act's commencement, many FITSPA members were not regulated, while a few had received no-objection letters from the BOU. From 4 March 2021, many of these FinTechs will be expected to comply with the regulations' requirements. Considering that the FinTech industry in Uganda is still in its formative stages and most of the entities have been operating outside the regulatory sphere, there is an urgent need for providing support to the Association and its members to ensure timely compliance.

Overview of National Payment Systems Act, 2020 (2/2)

To this end, we have developed a compliance guidance tool to support FITSPA members to operationalize the NPS implementing regulations.

The compliance guidance tool gives guidance on the general criteria assessed in the licensing process including, but not limited to, the following four areas:

1. Governance (suitability of the members of the management body and suitability of shareholders)
2. Internal organization (risk management, compliance and audit frameworks)
3. Program of operations
4. Capital and liquidity

Eligibility for licensing payment system

1. A payment system is eligible to be licensed by the central bank if that payment system has any of the following objects-

a) clearing of payment instructions between financial and non-bank
b) settling of obligations arising from the clearing of payment instructions
c) transfer of funds from one account to another using an electronic device
d) transfer of electronic money from one electronic device to another
e) provision of technological services to facilitate switching routing, clearing or data management for or on behalf of a payment system provider
f) provision of electronic payment services to the unbanked and under-banked population
g) provision of financial communications networks
h) ordering or transmitting payment instructions
i) storing of information on a device for purposes of effecting payments
j) fulfilling payment obligations at points of sale, merchant outlets or over the internet
k) any other objects as may be prescribed by the central bank by regulations

2. Subject to subsection (1), a payment system shall be eligible to be licensed by the central bank if that payment system is interoperable with other payment systems in the country and internationally.

Categories of licenses

The categories of licenses granted under section 9 of the Act are as follows-

a) payment systems operator license

b) payment service provider license

c) issuer of a payment instrument license

If a FinTech is applying for multiple licenses e.g., a switch and an e-money issuer:

- BOU will combine the licenses into one operating license (a special license)
- FinTech must pay fees for each category of license combined e.g. for above example, FinTech will pay the total application and licensing fees under switch and e-money issuer
- For capital requirement - combined licenses will maintain minimum capital that is the highest among the classes combined

Payment Systems Operator license

A payment systems operator license shall be issued in respect of the following categories -

a) switches in respect of routing of payment transactions, authorization and settlement request from merchants, acquiring and issuing banks

b) technology used in the provision of payments and settlements services

c) aggregators or integrators in respect of aggregation of merchant services, processing services, provision of hardware and software, printing and personalization of electronic magnetic card, inward international remittances services, merchant acquiring, point of sale deployment, payment aggregation

d) any other category that the central bank may prescribe

Payment Service Provider license

A payment service provider license shall be issued in respect of the following categories -

(a) electronic money issuer in respect of issuance of electronic money, recruitment and management of agents, creation and management of wallet, wallet based domestic money transfers including transfers to and from bank accounts, cash in and cash out transactions, investment, savings, credit products only in partnership with banks, insurance and pension products only with authorized insurance and pension companies and cross-border payments or transfers

(b) any other category that the central bank may prescribe.

Definitions:

- Electronic money business - means the issuance, transfer, payment and redemption of electronic money and any other activity permitted under the NPS Regulation 2020
- Non-bank electronic money issuer - means an entity incorporated under the laws of Uganda as a limited company licensed under the NPS Act
- Special account - means an account opened by a financial institution or microfinance deposit-taking institution to deposit funds received from consumers in exchange of electronic money issued at par value by the bank
- Trust - means a body corporate (referred to under section 49 (5) of the NPS Act)
- Trustee - means a person appointed by the electronic money issuer with the approval of the central bank to manage the trust account
- Trust account - means an account opened by a non-bank electronic money issuer to deposit funds received from consumers in exchange of electronic money issued at par value by the non-bank electronic money issuer

Issuer of a Payment Instrument license

An issuer of payment instrument license shall be issued in respect of the following categories -

a) stored value card a license in respect of storing electronic money value

b) any other category that the central bank may prescribe

Key to note:

I. An issuer of payment instrument shall not issue stored value or prepaid cards unless it is a deposit-taking financial institutions licensed by the central bank with clearing capacity.

II. Notwithstanding sub regulation (1) an issuer of payment instrument which is not deposit-taking financial institutions may enter into partnership with deposit-taking financial institution with clearing capacity to issue stored value or prepaid cards.

What will BoU do with your application?

I. Vet the Substantial Shareholders, Directors & Senior Managers. Foreign based applicants may attract due diligence costs to be met by the applicant.

II. Review the application documents

III. Make a decision within 60 days of receipt of a complete application. Where a license is to be issued, the licensee shall pay the license fee

Grant of license:

I. If satisfied that the applicant meets the requirements, BoU will grant a license to the applicant
II. BoU may grant a license subject to such conditions as the central bank may consider necessary and may, from time to time, add, vary or substitute the conditions as it deems appropriate
III. BoU may, by regulations, prescribe different classes of a license in respect of each category of a license under the NPS Act
IV. A licensee shall not conduct activities that are not specified in its license
V. BoU shall publish in a newspaper of wide circulation in Uganda, a list of all licenses under the Act at least once every year
VI. Where BoU declines to grant a license to an applicant, the central bank shall, within thirty days, notify the applicant of its decision and specify the reasons for the refusal in writing

NPS Regulations – Licensing under the NPS Act

Procedure to apply for the license

FinTech companies need to demonstrate not only that they comply with the relevant regulatory requirements but also that they have considered and taken into account the various risks posed by their business more generally.

To go to the section you are interested in, please click on any tab below:

Part A - License fees and capital requirements

Part B - Documents required to apply for licenses

Part C - Business plan

Part D - Operational policies and procedures

Part E - Risk, IT, and audit management

Part F - Governance and internal controls

Part G - Safeguarding of customer funds

Part H - Access to sensitive payment data

Part A - License: application, license and annual fees (1/2)

The NPS Act has different license categories and capital requirements with fees applicable to each category. The following is a summary of the fees for the various license categories:

License category	License class	Application fees (UGX)	License fees (UGX)	Annual fees (UGX)
Payment systems operator	a) Funds transfer systems i. Large funds transfer systems whose transaction value exceeds UGX.100bn per month.	3,000,000	25,000,000	25,000,000
	ii. Medium funds transfer a system whose transaction value exceeds UGX.1bn per month and does not exceed UGX.100bn per month.	3,000,000	20,000,000	20,000,000
	iii. Small funds transfer systems whose transaction value does not exceed UGX.1bn per month.	3,000,000	15,000,000	15,000,000
	b) Clearing system/switches	3,000,000	25,000,000	25,000,000
	c) Settlement systems	3,000,000	25,000,000	25,000,000
	d) Third party systems	3,000,000	10,000,000	10,000,000

License: fees and capital requirements (2/2)

License category	License class	Application fees (UGX)	License fees (UGX)	Annual fees (UGX)
Payment service provider	a) Electronic money issuer i. Large electronic money issuer whose total trust account value exceeds UGX.200bn.	3,000,000	25,000,000	25,000,000
	ii. Medium electronic money issuer whose total trust account value exceeds UGX.500M but does not exceed UGX.200bn.	3,000,000	20,000,000	20,000,000
	iii. Small electronic money issuer whose total trust account value does not exceed UGX.500M.	3,000,000	15,000,000	15,000,000
	b) Any other payment service provider license	3,000,000	5,000,000	5,000,000
Issuer of a payment instrument		Nil	Nil	Nil

License: capital requirements (1/2)

The following is a summary of the capital requirements for the different license categories:

License category	License class	Minimum Capital requirement (UGX)
Payment systems operator	a) Funds transfer systems- I. Large funds transfer systems whose transaction value exceeds UGX.100bn per month.	1,000,000,000
	II. Medium funds transfer systems whose transaction value exceeds UGX.1bn per month and does not exceed UGX.100bn per month.	500,000,000
	III. Small funds transfer systems whose transaction value does not exceeds UGX. 1bn per month.	100,000,000
	b) Clearing systems or switches	500,000,000
	c) Settlement systems	250,000,000
	d) Third party systems	100,000,000

License: fees and capital requirements (4)

The following is a summary of the capital requirements for the different license categories:

License category	License class	Minimum Capital requirement (UGX)
Payment service provider	a) Electronic money issuer I. Large electronic money issuer whose total trust account value exceeds UGX.200bn.	10,000,000,000
	II. Medium electronic money issuer whose total trust account value exceeds UGX.500M but does not exceed UGX.200bn.	5,000,000,000
	III. Small electronic money issuer whose total trust account value does not exceed UGX.500M.	250,000,000

Guidance notes to FinTechs on licensing

Note 1

There are different license classes depending on the nature of businesses and value of transactions that FinTechs are engaged in. The different license classes have got different application and license fees which is paid once and annual fees paid every year the FinTech continues to be in business.

Note 2

The Act specifies the minimum capital requirements to be maintained by the FinTechs based on the license categories. The minimum capital requirement is to be maintained unimpaired by losses or other adjustments at all times. For FinTechs with combined licenses, they need to maintain the minimum capital that is the highest among the classes combined.

For example, if a FinTech has a combined license of a payment system operator license (whose value exceeds 100 billion) and has a minimum capital requirement of UGX 1 billion and a switch license with a capital requirement of UGX 500 million, then the FinTech will be required to maintain the capital requirement of UGX 1 billion.

Note 3

The FinTechs will be required to restore the minimum capital in a period of not more than 90 days in case of impairment of their capital positions

Part B - Documents required to operate a payment system or offer payment service (1/4)

An application to operate a payment system or offer payment services shall be made in **Form A** as set out in Schedule II to the Regulations. The application shall be accompanied with:

01

Proof that the applicant's objects are per section 8 (1) of the Act in the case of the payment system.

02

A detailed description of the product or services of FinTech and its operations.

03

List of the shareholders, including the beneficial owners.

04

The business plan with financial projections for the first three years.

05

The applicant's organizational, governance and management structure.

06

Risk management framework with a disaster recovery plan, cybersecurity plan, and business continuity arrangements.

Documents required to operate a payment system or offer payment service (2/4)

07

Policies and procedures for transacting with customers include disclosure requirements, complaints, prices, and redress mechanisms.

08

Certified copy of incorporation documents and certified copy of the certificate of incorporation.

09

At least two recommendation letters from persons of good repute within the financial sector attesting to the directors', managers', and shareholders' credibility.

10

Duly filled **fit and proper person form** for shareholders, directors, and managers.

11

Certificate of good conduct for shareholders, including beneficial owners, directors, and managers.

12

Source of funds with supporting documents.

Documents required to operate a payment system or offer payment service (2/4)

13

In the case of a foreign company, a copy of the certificate of incorporation of the foreign company is certified by a public notary.

14

A certified copy of a systems license from NITA Uganda or Uganda Communication Commission.

15

A tax identification number and a copy of the tax clearance certificate.

16

Audited financial statements for the previous two years

17

Proof of payment of the application fees.

18

Documented procedures and policies for monitoring, detecting, and reporting money laundering incidences in line with AML and CFT laws.

Documents required to operate a payment system or offer payment service (2/4)

19

Documented plan for agents' and merchants' intended use, including issuing, acquiring, and redemption mechanisms and drafts of merchant and agent agreements.

20

Documented outsourcing arrangements.

21

Information on planned or existing participation in a domestic or foreign payment system and list of countries where applicant is licensed to engage in business

22

Evidence of holding the minimum paid-up capital, including the projected level and quality of capital, balance sheet composition, and growth plans.

23

Agreement between the applicant and supervised financial institution to show where all charges, fees, and penalties shall be recovered.

24

In the case of an electronic money issuer, a copy of the customer service agreement

Guidance notes to FinTechs on application process

Note 1

Application for a license is made directly to the Bank of Uganda which has the right to accept or reject applications based on their assessment. Feedback will be given on specific areas by Bank of Uganda.

Note 2

FinTechs need to have the requisite fees ready when making application to the Bank of Uganda. The application for license needs to be accompanied by the application fees for the licenses that the FinTechs are applying for. In the case of combined licenses, the FinTech need to make application fee payment for both licenses.

Note 3

Application for license is to be made through form A and FinTechs need to attach the supporting documents required by Bank of Uganda.

Note 4

In order to ensure a smooth and seamless application process, FinTechs should ensure that they have all the requisite documents, policies and licenses before starting the application process. Applications such as system licenses from NITA or Uganda Communications Commission should be obtained before starting the application process for the NPS license

Illustration 1: licensing procedure for start-up FinTech

Illustration 1

Company X is a start-up FinTech company that started operations in Uganda in January 2020. The company has been set up to offer switch services and wishes to apply for a license under the NPS Act. The company has two directors and has only UGX 50 million as capital.

In order to ensure a seamless application process, the company will need to put in motion mechanisms to raise the minimum capital from UGX 50 million to 500million through various options such as issue of shares, debt or other instruments to raise the capital to the required amount. Capital can also be evidenced by amount invested in systems and hardware. The company will also need to set aside the required amount for the license fees which will be paid if the application is approved by Bank of Uganda. Once this is done, then the company can proceed with complying with the other requirements relating to policies and procedures relevant for the switch license application.

The company can then apply for the switch license, using form A, attach evidence of payment of application fees of UGX 3 million and attach the requisite supporting documents specified in the regulations.

Bank of Uganda will have 60 days upon receipt of a complete application from Company X to respond.

Where Bank of Uganda is satisfied that the company has complied with all the requirements and a license is to be issued, Company X shall pay the license fee of UGX 25,000,000.

Illustration 2: licensing procedure for established FinTech

Illustration 2

Company Y is an established business with over 15 years of existence in Uganda market and is part of a group of companies with operations across Sub-Saharan Africa. The company operates a wallet and is interested in electronic money issuer license. The company has some foreign directors based in USA and Europe. The company has a large capital base of over UGX 2.5 billion and its trust account value is 250 billion.

In this case, the company already has established policies and procedures and capital is adequate to meet the requirements of the electronic money issuer license. The company will therefore spend more effort in ensuring compliance with the policies stipulated in the NPS regulations. The company can leverage on the group's policies to meet some of the requirements of the NPS regulations. Key to note is to ensure fit and proper form for foreign directors are obtained and trust deed is in place and in the form prescribed by the NPS Act.

Once the company has confirmed that they have all the supporting documents for application of electronic money issuer license, then they can proceed and apply for the electronic money issuer license, using form A, attach evidence of payment of application fees of UGX 3 million and attach the requisite supporting documents specified in the regulations.

Bank of Uganda will have 60 days upon receipt of a complete application from Company Y to respond.

Where Bank of Uganda is satisfied that the company has complied with all the requirements and a license is to be issued, Company Y shall pay the license fee of UGX 25,000,000.

Illustration 3: licensing procedure for application of multiple licenses

Illustration 3

Company Z is an established business with over 10 years of existence in Uganda market. The company operates a wallet and also offers switch services . The company is interested in obtaining two licenses, electronic money issuer license and switch license .The company has a capital base of UGX 800 million and its trust account value is 200 billion.

In this case, company Z is required to meet the minimum capital requirement of the highest class, which in this case is the capital requirement for electronic money issuer license. Since company Z has a capital base of UGX 800 million, they fall short of the minimum capital requirement of UGX 1billion. Company Z will have to put in place mechanism to raise the capital to UGX 1 billion after which they will ensure they have all the necessary supporting documents to apply for the license.

Once the company has confirmed that they have all the supporting documents for application of electronic money issuer license, and switch license, then they can proceed and apply for the electronic money issuer license and switch license, using form A, attach evidence of payment of application fees of UGX 6 million (UGX 3 million for electronic money issue license and UGX 3 million for switch license) and attach the requisite supporting documents specified in the regulations.

Bank of Uganda will have 60 days upon receipt of a complete application from Company Z to respond.

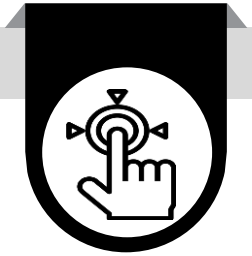
Where Bank of Uganda is satisfied that the company has complied with all the requirements and a license is to be issued, company Z shall pay the license fee of UGX 50,000,000.(UGX 25,000,000 for each license).

Part C - Business plan (1/2)

The regulator expects to see a concise and engaging summary of the business. Therefore, a FinTech must develop an excellent business plan that tells a compelling story and shows scalability. The plan should include:

Company Overview

A summary overview of the company



Mission/Vision of the Company

What is the mission and vision?

The Team

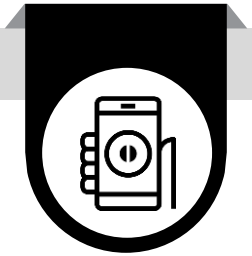
Who are key team players? What is their relevant background?

The Problem

What big problem are you trying to solve?

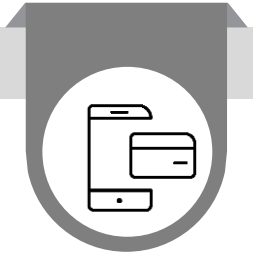
The Solution

What is your proposed solution? Why is it better than other solutions or products?



The Market Opportunity

How big is the addressable market



The Product

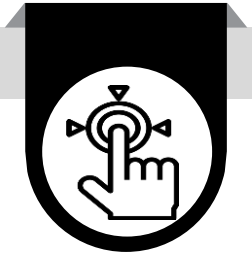
Give specifics on the product or service

Business plan(2/2)

The regulator expects to see a concise and engaging summary of the business. Therefore, a FinTech must develop an excellent business plan that tells a compelling story and shows scalability. The plan should include:

The Technology

What is the underlying technology? How is it differentiated? Is it defensible and difficult to replicate?



The Competition

Who are the key competitors? How will you be better than the competition?

Traction

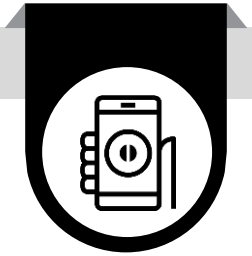
Early customers, early adopters, revenues, press, and partnerships

Business Model

What is the business and revenue model? Is it scalable? What are the acquisition costs?

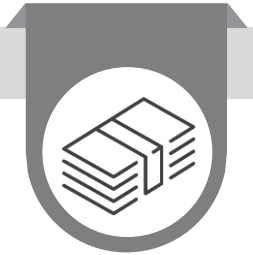
The Customers

Who are the target customers? Why will there be a huge demand from these customers?



The Marketing Plan

How do you plan to market? What is customer acquisition costs versus the customer's lifetime value?)



Financials

Projected revenues, key assumptions, and EBITDA

Documents required for application of issuer of payment instruments

FinTechs applying for a license to operate as the issuer of payment instruments as per the NPS Act will be required to fill in **Form B** and attach accompanying documents as follows:

01

A copy of a payment service provider or payment system operator's license, in case of an applicant who is a licensee.

02

The description of the type of payment instrument intended to be issued.

03

A risk management framework that is appropriate to ensure safety and efficiency.

04

Terms and conditions of the issuance of a payment instrument.

05

Merchant and agent agreement, where applicable.

06

Proof of payment of application fees specified in Schedule IV.

07

Pricing policy should include the variables used to arrive at a price, and the nature and amount of charges or fees imposed on customers.

08

Any other information that the central bank may require.

Part D - Operational policies and procedures

FinTechs will need to confirm that they have the following key policies in place. While elements within the policies and procedures presented below are based on best practice, each FinTech need only address the elements applicable to its business .

To go to the section you are interested in, please click on any tab below.

(i) - Information systems and security

(ii) - Accounting and operational procedures

(iii) - Complaints handling

(iv) - Anti-money laundering & CFT

(v) - Human resources

(vi) - Settlement procedures

Part D(i) - Information security policy (1/2)

An information security policy (ISP) is a set of rules, policies and procedures designed to ensure all users and networks within an organization meet minimum IT security and data protection security requirements. Those looking to create an information security policy should review ISO 27001, the international standard for information security management. Although the Standard doesn't list specific issues that must be covered in an information security policy (it understands that every business has its own challenges and policy requirements), it provides a framework that you can build around. The policy should address the following key elements:

Purpose

Outline the purpose of your information security policy which could be to:

- Create an organizational model for information security
- Detect and preempt information security breaches caused by third-party vendors, misuse of networks, data, applications, computer systems and mobile devices.
- Protect the FinTech's reputation
- Uphold ethical, legal and regulatory requirements
- Protect customer data and respond to inquiries and complaints about non-compliance of security requirements and data protection

Audience

- Define who the information security policy applies to and who it does not apply to.

Information security policy (2/2)

Information security objectives

- These are the goals management has agreed upon, as well as the strategies used to achieve them.
- In the end, information security is concerned with:
- **Confidentiality:** data and information are protected from unauthorized access
- **Integrity:** Data is intact, complete and accurate
- **Availability:** IT systems are available when needed

Authority and access control policy

- This part is about deciding who has the authority to decide what data can be shared and what can't.
- It should outline how to handle sensitive data, who is responsible for security controls, what access control is in place and what security standards are acceptable.

Data classification

- An information security policy must classify data into categories.
- A good way to classify the data is into five levels that dictate an increasing need for protection:
- **Level 1:** Public information
- **Level 2:** Information your organization has chosen to keep confidential but disclosure would not cause material harm
- **Level 3:** Information has a risk of material harm to individuals or your organization if disclosed
- **Level 4:** Information has a high risk of causing serious harm to individuals or your organization if disclosed
- **Level 5:** Information will cause severe harm to individuals or your organization if disclosed

Part D(ii) - Accounting policy and procedures (1/2)

The purpose of this section is to describe the accounting policies and procedures currently in use and to ensure that the financial statements and procedures conform to generally accepted accounting principles; assets are safeguarded through adequate internal controls and finances are managed with accuracy, efficiency, and transparency. Some of the areas covered in the accounting manual include:

Essential sections required in the license application

Accounting policies and procedures	Revenue and costs	Financial internal controls	Financial reporting	Chart of accounts	Assets & Liabilities
Start with an overview of your accounting process and system. Give a review of the concepts.	Define and classify revenue streams and major expense categories	Comprised of control activities such as authorization, documentation, reconciliation, security, and the separation of duties	The disclosure of financial information to the various stakeholders about the financial performance and financial position of the company over a specified period of time	A financial organizational tool that provides a complete listing of every account in the general ledger of a company, broken down into subcategories.	Establishes the fundamental guidelines and practices for properly accounting and reporting assets and liabilities on the Company's Balance Sheet

Accounting policy and procedures (2/2)

Optional sections that will enrich the application but are not mandatory

Liabilities	Credit and Accounts Receivable	Purchasing	Accounts Payable and Cash Disbursements	Segregation of duties	Payroll
Provide guidelines to properly account for liabilities including categorization, valuation methods, and G/L account code tables	Define and classify types of expenses and expense credits at the Company	Describe how you buy goods, services, and assets at our organization.	Describes the procedures and forms used in accounts payable	A key principle in financial control, aiming to reduce the risk of fraud and error. It involves breaking down processes so that no single person is responsible for every stage in a process	Describes the payroll process as it relates to administration of salaries, timekeeping, payroll schedules and payment methods.

Part D(iii) - Complaints handling manual (1/2)

Financial consumer complaints handling mechanisms comprise two stages: complaints that financial service providers handle and complaints that, if not satisfactorily resolved, are handled by an alternative, out-of-court process. The timely resolution of complaints, including the provision of redress where warranted, should be the FinTech's primary responsibility. An internal complaints resolution mechanism is defined as a complaint handling function, unit, or dedicated team within the FinTech. The mechanism should be implemented with proper structure, policies, procedures, systems, and governance with the below considerations:

Establishing definitions	Independence, governance, resourcing, and training	Policies and procedures in place	Access to complaints: channels, visibility, and transparency
It is recommended, as a first step, that certain definitions for terms commonly used be established e.g. complaints, request for service, eligible complainant etc.	Fair and thorough handling of complaints is most likely to be achieved by a dedicated complaints handling unit that is independent from the operational business units of a FinTech to avoid any potential conflict of interest and ensure a fair and transparent process	The documented policies should, at a minimum: (i) ensure the accessibility, fairness, transparency, responsiveness, and independence of the complaints handling mechanism; (ii) be approved by the FinTech's board of directors or equivalent body; (iii)detail decision-making steps and escalation processes within the institution; and (iv) be disseminated proactively to all relevant staff	FinTech should make available channels for lodging complaints with the objective of making the channels functionally accessible, and efficient to their customers

Complaints handling manual (2/2)

The IDR mechanism should be implemented with proper structure, policies, procedures, systems, and governance with the below considerations

Timeline for resolution: establishing clear response times for resolving complaints

Mandatory time limits help ensure that all complaints are handled in a timely manner and can provide confidence to consumers that their complaints will be resolved by the FinTech in a reasonable time.

Threshold limits encourage FinTechs to manage complaints properly, as violations can be addressed with fines or moral suasion responses.

Consumer communication

The first step in investigating a consumer complaint is verifying eligibility and accepting the complaint.

This step requires FinTechs to acknowledge the complaint, give an appropriate time frame for investigation and response, communicate to the customers and resolution

Complaints data: ongoing analysis of root causes

In addition to the requisite investigation, all complaints should be analyzed to identify and examine underlying causes.

The information provided by complaints can be applied to identifying and remedying any recurring or systemic problem and improving policies, procedures, and products accordingly

Complaints data recording and reporting: accuracy, standardization, and classification

A complaints database is an important tool for ensuring consistency in complaints handling and decisions throughout the institution.

Part D(iv) - Anti-Money Laundering and CFT (1/4)

An anti-money laundering policy is a combination of measures used by a financial institution to stop reintroducing the proceeds of illegal activities. Business AML policy is often a combination of the Financial Action Task Force (FATF) recommendations and locally introduced laws. There are eight steps to follow in developing the AML policy:

01

To define the purpose of the AML policy, a business must introduce three main statements:

- Definition for money laundering and terrorist financing
- Reasons why the policy is necessary
- Regular regulatory reviews to stay within regulatory demands

02

Appoint an AML officer
At this point, a business needs to nominate a compliance officer — a FinTech employee responsible for everything concerning the business's AML program. State their name, qualifications, and responsibilities

03

Reporting to the Financial Intelligence Authority-Uganda (see link for relevant AML laws in Uganda). Here a FinTech describes how they will satisfy financial intelligence units and law enforcement requests for information on criminal activity. A FinTech must explain its actions and procedures to initiate upon such a demand from the authorities and to document the situations.

04

Sharing data with financial institutions
This part is dedicated to the process of sharing the accumulated AML data with other financial entities to identify and prevent money laundering elsewhere. The policy must describe a secure and confidential process that will not allow for data leaks

Anti-Money Laundering and CFT (2/4)

05

Screening across sanction lists
Before entering a business relationship or opening an account for a client, financial companies must verify that the person they are working with is not on any sanction or blacklist. A FinTech must state the standard procedure for checking their clients through these lists and establishing their awareness of the latest changes.

06

Verifying client's identity
Identity check is the central part of an AML compliance policy. Here a FinTech must specify a list of comprehensive and reliable measures that will help them accurately verify the identities of their clients upon opening an account or registering in their service

07

Performing customer due diligence (CDD)
This step is about the measures taken as a part of CDD for those identified as beneficial owners, senior management, and politically exposed persons (PEP). A FinTech should also specify the basis of its risk rating system, how it determines whether the case requires simplified due diligence, customer due diligence, or enhanced due diligence. Here, it would be necessary to add when a customer triggers adverse media or sanctions list checks, be subject to ongoing monitoring.

08

Filling out suspicious activity reports
Lastly, an essential part of an AML policy is to promptly respond to suspicious activity and correctly form a compliant declaration. A FinTech must specify the necessary information that needs to be mentioned in the report alongside the deadlines

Anti-Money Laundering and CFT (3/4)

A sound AML/CFT program should include the following interrelated components to address all critical aspects:

01 Governance	02 Risk identification	03 Policies and Procedures	04 Customer due diligence
Governance - A sound governance structure is the foundation of an effective AML/CFT program and will include the board of directors and senior management setting the tone at the top, hiring a qualified chief AML/CFT officer, and adequately resourcing the three lines of defense.	Risk identification, assessment, and mitigation – FinTech must have a thorough understanding of the specific ML/FT risks they face through a periodic enterprise-wide AML/CFT risk assessment.	Policies and procedures - AML/CFT policies and procedures should be in writing and serve the purpose of preventing, detecting, and reporting potentially suspicious activity, complying with local laws, and establishing a strong internal control and risk management environment.	Customer identification and due diligence - to manage ML/FT risks effectively, FinTechs must understand who their customers are. To achieve this, FinTechs must conduct customer identification and due diligence when onboarding a new customer and update CDD throughout the relationship with the customer.

Anti-Money Laundering and CFT (4/4)

A sound AML/CFT program should include the following interrelated components to address all critical aspects:

05 Transaction monitoring

Transaction monitoring involves manual or electronic scanning of transactions based on certain parameters (for example, customer and beneficiary names, volume, value, country of origin, or destination of transactions) to determine if they are consistent with the FinTech's knowledge of the customer.

06 Reporting

Reporting is an essential part of the anti-money laundering regimen is providing authorities reports on important financial transactions. These regulatory requirements typically include suspicious-transactions reports and large currency transaction reports.

07 Communication and training

Communication and training - effective AML/CFT risk management is not possible without clear and routine cross-organizational communication and the appropriate personnel training.

08 Internal and external audit

Internal and external audit - internal audit, as described, is the third line of defense that independently evaluates the AML/CFT program and processes carried out by the first and second lines of defense.

Part D(v) - Human resources policy and procedures (1/2)

Human resources policies and procedures are important as they provide the FinTechs with structure, control, consistency, fairness, and reasonableness. They also ensure compliance with employment legislation and inform employees of their responsibilities and the FinTech's expectations. The following categories are **essential** for the license application:

1. HR management policy statement

The HR management policy statement should encompass the HR policies for the FinTech and responsibilities of officers within the company.

2. Recruitment and appointment

Policies related to recruitment and appointment of officials in the company.

3. Conditions of appointment

The conditions of appointment to various levels should indicate the minimum requirements for the appointment.

4. Staff development

Policies related to staff development including training, professional membership, and other development attributes.

5. Staff career development

Policies related to growth, promotion, and external capacity building initiatives and other attributes such as secondment to other companies.

6. Performance evaluation

Policies related to individual performance appraisal, setting of goals, objectives and targets, and evaluation.

Human resources policy and procedures (2/2)

Optional sections that will enrich the application but are not mandatory:

7. Compensation package

Policies related to the remuneration of employees, non-cash benefits and other compensation matters.

8. Facilitation

Policies related to facilitation for company expenses incurred by employees and travel outside of company premises.

9. Discipline

Policies related to the conduct of employees within and outside the premises.

10. Leave

Policies on annual leave, compassionate leave, study leave, sick leave, and maternity and paternity leave.

11. Termination of service

Conditions for termination of service and obligations of both parties.

12. Safety and security

Safety and security of employees while working with the company. Policies of work injury benefits.

Part D(vi) - Settlement procedures (1/2)

01

Every participant in a payment system shall open and maintain settlement accounts in the books of the central bank or an authorized settlement agent, including the maintenance of minimum balances, on such terms and conditions as the central bank or payment system operator may specify.

Where a participant is unable to maintain a settlement account, the participant shall appoint another participant who has opened a settlement account as a settlement agent to:

- settle all obligations due from the first participant to any other participant; or
- receive all claims from the first participant from the other participant.

02

03

Where a participant appoints another participant under, the participant shall, before any obligation is settled on its behalf, give the payment system operator notice in writing of the appointment, accompanied by a written confirmation from the participant that is appointed

An electronic money issuer that holds a trust account with more than one financial institution or microfinance deposit-taking institution shall ensure that all settlement transactions between the accounts of the respective financial institutions are done through the interbank payment and settlement system or any other means that the central bank may determine.

04

Settlement procedures (2/2)

05 A settlement is final and irrevocable

06 The final discharge of any indebtedness between participants in a clearing and settlement system shall take place through the central bank or a financial institution

07 Where it is established that any amount, right, or property already paid or transferred was not, in fact, due, it shall constitute a fresh debt owed by the payee or transferee, as the case may be, to the person who made the payment or transfer.

08 Protection of settlement accounts - the balances on settlement accounts with a payment system shall not be attached, assigned or transferred to satisfy any debt or claim.

Part E - Risk, IT audit, and business practices

To go to the section you are interested in, please click on any tab below.

(i) - Risk management framework

(ii) - Business continuity planning

(iii) - Cybersecurity polices and framework

Part E(i) - Risk management framework

Evolving FinTech risk management functions are tasked with addressing the potential exposures created by their innovation. There is a need for FinTechs to elevate their risk management capabilities, including the development of an operational risk and compliance program to have a risk compliance framework that addresses their inherent risks as generated by their business.
FinTechs can tailor for their needs a broad-based risk management program using the following six steps:

1. Define roles and responsibilities: through a governance model - a defined risk and compliance governance program should establish minimum standards and guidelines for committee activities, including the development of committee charters and templates for meeting agendas and minutes

2. Understand applicable risks and rank them: like financial institutions, FinTechs are subject to multiple risk types, including credit, liquidity, operational, compliance, and reputation. To that end, attention should be given to identifying and scoring the inherent risks specific to activities undertaken

3. Evaluate the controls environment: Once FinTech understands the risks unique to its products and services and evaluates them according to its risk ranking methodology and framework, the next step is to determine what controls are in place to address exposures and identify gaps

4. Evaluate risk and response options: once risk assessments have been conducted, risk professionals can review the results for consistency and accuracy of ratings, and the scope and coverage of the identified controls, based on their understanding of the greater organization

5. Consider the organization's maturity level and technology use - risk and compliance maturity can be evaluated based on three classifications: existing, evolving, and mature

6. Engage management through effective reporting and communication - with the risk and compliance management program up and running, the management team can begin to formalize the metrics they measure their risk management practices.

Part E(ii) - Business continuity plan (1/3)

An effective business continuity plan lays out the instructions and procedures a FinTech must undergo when some kind of disaster occurs. Every FinTech should have such a plan in place to avoid losing money or halting operations. Business continuity planning is crucial for relatively new FinTech startups.

A business continuity plan should consider the following:

01 Identify important business services that, if disrupted, could cause harm to consumers or markets

02 Set impact tolerances for each important business service (i.e., thresholds for maximum tolerable disruption to achieve consumer protection)

03 Identify and document the people, processes, technology, facilities, and information that support your important business services (mapping)

04 Test your ability to remain within your impact tolerances through a range of severe but plausible disruption scenarios

05 Conduct lessons learned exercises to identify, prioritize, and invest in their ability to respond and recover from disruptions as effectively as possible

06 Develop internal and external communications plans for when important business services are disrupted

Business continuity plan (2/3)

Each FinTech need only address the elements applicable to its business, but if you do not include a specified element in your plan, your plan must document why it is not included. There are nine critical elements of a BCP.

Data backup and recovery (hard copy and electronic)	All mission-critical systems	Financial and operational assessments	Alternate communications between the FinTech and its customers and employees	Alternate physical location of employees
This encompasses a clear identification of where primary books and records, as well as backup files (hard copy and electronic) of the same, are kept or located.	What is deemed to be mission-critical systems vary based on each member's business. These would include online banking, access to customer accounts, and encryption	These assessments include a record of procedures to be undertaken, allowing for the FinTech to identify changes in its operational, financial, and credit risk exposures.	These encompass the provisions to be made to ensure an uninterrupted connection among everyone involved.	In the case of disruptions, there should be designated alternative sites for employees in the resumption of business operations.

Business continuity plan (2/3)

Critical business constituent, FinTech, and counterparty impact	Regulatory reporting	Communications with regulators	How the FinTech will assure customers' prompt access to their funds
This covers the effect significant business disruption can have on the FinTech's relationships with other counterparties, and other stakeholders, and how it will address such impacts.	This should spell out the capability of the FinTech to ensure compliance with regulatory reporting requirements in the event of business disruption.	This covers how the FinTech can communicate with the regulator during a significant disruption, and identifies designated business continuity plan contacts who will assist in the communication.	Comprises details on how the FinTech will make funds available to customers in the event of an extensive business disruption

The business continuity planning process should be a continuously evolving step and institution-wide responsibility. It must be resilient and current to be capable of efficiently responding to changes in business operations and potential threats, and must completely address all audit recommendations and test results.

Part E(iii) - Cybersecurity policies and framework (1/3)

The government of Uganda passed three critical laws, namely:

- Computer Misuse Act, 2011;
- Electronic Transactions Act, 2011;
- Electronic Signatures Act, 2011. Taken together, they are referred to as the Uganda Cyber Laws.

The Computer Misuse Act ensures the safety and security of electronic transactions and information systems, and the Regulation of Interception of Communications Act monitors suspicious communications.

The Uganda Computer Emergency Response Team provides information and assistance to its constituents in implementing proactive measures to reduce the risks of computer security incidents and respond to such incidents when they occur.

Also, Uganda has a National Information and Technology Authority that provides technical support and cybersecurity training. It also regulates standards and utilization of information technology in both the public and private sectors.

Regulators and supervisors are focusing on how FinTech affects the core risk governance competencies of identifying, managing, measuring and controlling risks across the three lines of defense, and having the appropriate resources, skills and expertise to deliver this effectively

Cybersecurity policies and framework (2/3)

The most frequently adopted frameworks are:

- PCI DSS (Payment Card Industry Data Security Standard) - It is a set of security controls required to implement to protect payment account security. It is designed to protect credit card, debit card, and cash card transactions
- ISO 27001/27002 (International Organization for Standardization) - Best practice recommendations for information security management and information security program elements.
- CIS Critical Security Controls - A prescribed arrangement of activities for cyber protection that give particular and noteworthy approaches to stop the present most inescapable and perilous attacks. A key advantage of the Controls is that they organize and center fewer activities with high outcomes
- NIST Framework - A Framework for improving critical infrastructure Cybersecurity with a goal to improve organization's readiness for managing cybersecurity risk by leveraging standard methodologies and processes

Cybersecurity policies and framework (3/3)

Using the framework could improve the critical infrastructure of an organization. The Framework can be implemented in stages and hence can be tailored to meet any organization's needs. Cybersecurity framework's five functions include:

Identify

- FinTech must first understand their environments to manage cybersecurity risk to systems, assets, data, and capabilities.

Protect

- FinTech must develop and implement the appropriate safeguards to limit or contain the effects of possible cybersecurity events.

Detect

- FinTech must implement the appropriate procedures to identify cybersecurity events as soon as possible.

Respond

- FinTech must be able to develop response plans to contain the impacts of cyber incidents.

Recover

- FinTech must develop and implement effective methods to restore the capabilities or services that were damaged by cybersecurity events.

Part F - Governance and internal control

FinTechs are required to evidence the following:

- A fully developed organizational structure with clear roles and responsibilities
- A demonstrated segregation of duties

In line with this, the regulator will be assessing the following:

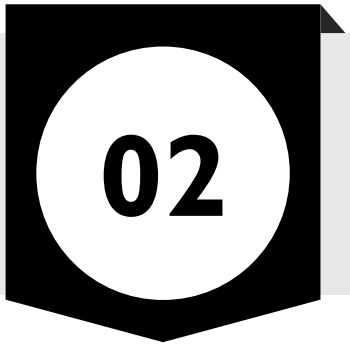
- Suitability of the members of the management body - members of the management body must have sufficient knowledge, skills and experience to fulfil their functions. This includes adequate knowledge, skills and practical and theoretical experience in banking and/or financial business. Since FinTechs have technology-driven business models, technical knowledge, skills and experience are just as necessary as sufficient banking knowledge, skills and experience to enable the members of the management body to fulfil their tasks.
- Suitability of shareholders - shareholders should have management and technical competence in the area of financial activities, including financial services. Additionally, the financial soundness of shareholders should be sufficient to ensure the sound and prudent operation of the FinTech.
    - The regulator will assess the reputation of shareholders (in terms of both integrity and professional competence), taking into account the degree of influence each shareholder intends to exercise over the FinTech. The existence of good corporate governance structures (e.g. independent non-executive board members) will also be considered in this assessment.
    - The regulator will also assess the financial soundness of shareholders against the funding needs of the FinTech

Governance and internal control

This section contains the regulation's governance and internal control guidelines:

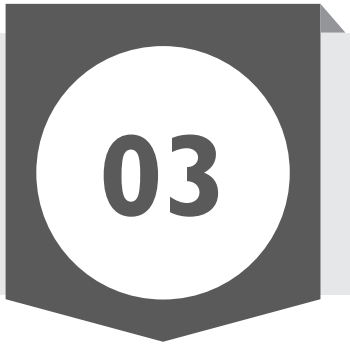
Governance arrangements

FinTechs should have governance arrangements, including administrative and accounting procedures, demonstrating that these governance arrangements and control are proportionate, appropriate, sound, and adequate.



Introduction of governance roles

FinTechs must map the growth of their business and introduce crucial governance roles at the right time. Hiring risk, compliance, legal, audit, and cybersecurity professionals will ensure the FinTech's rapid growth is underpinned by strong processes and controls



Fit and proper for directors

FinTechs should ensure that the shareholders with significant shareholding, directors, and senior management are individuals of good repute and are fit and proper. The FinTechs should periodically provide fit and proper documents of the directors and key shareholders to ensure that they continuously meet the fit and proper requirements.

Part G - Safeguarding of customer funds

Please click on any tab below to go to the section that you are interested in.

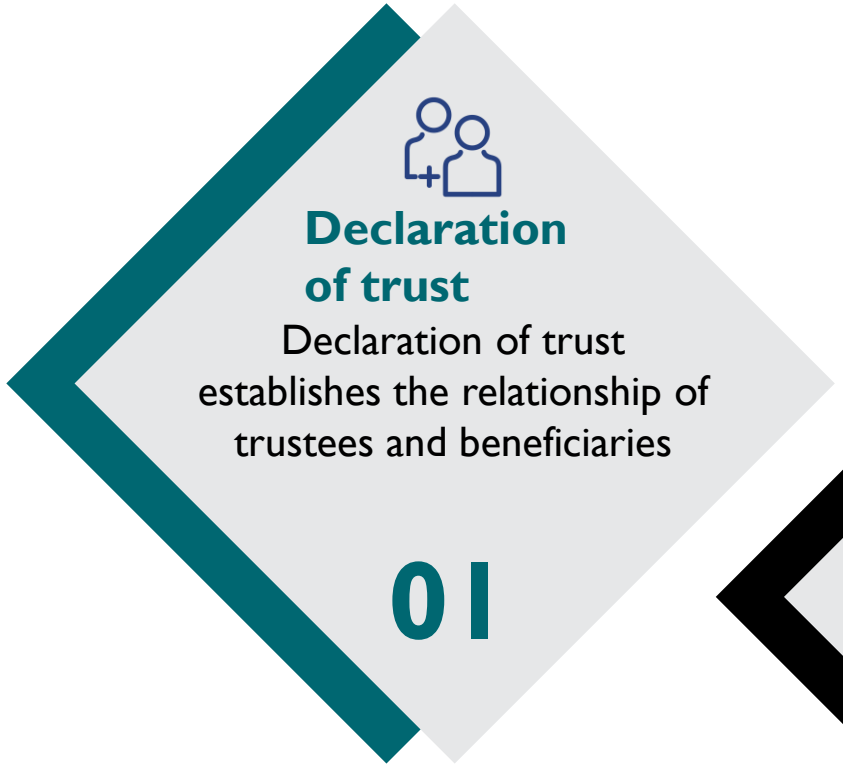
(i) - Key elements of a trust deed

(ii) - Selection of trustees

(iii) - Conditions to be met by appointed trustees

(iv) - Duties of trustees

Part G(i) - Key elements of a trust deed



Declaration of trust

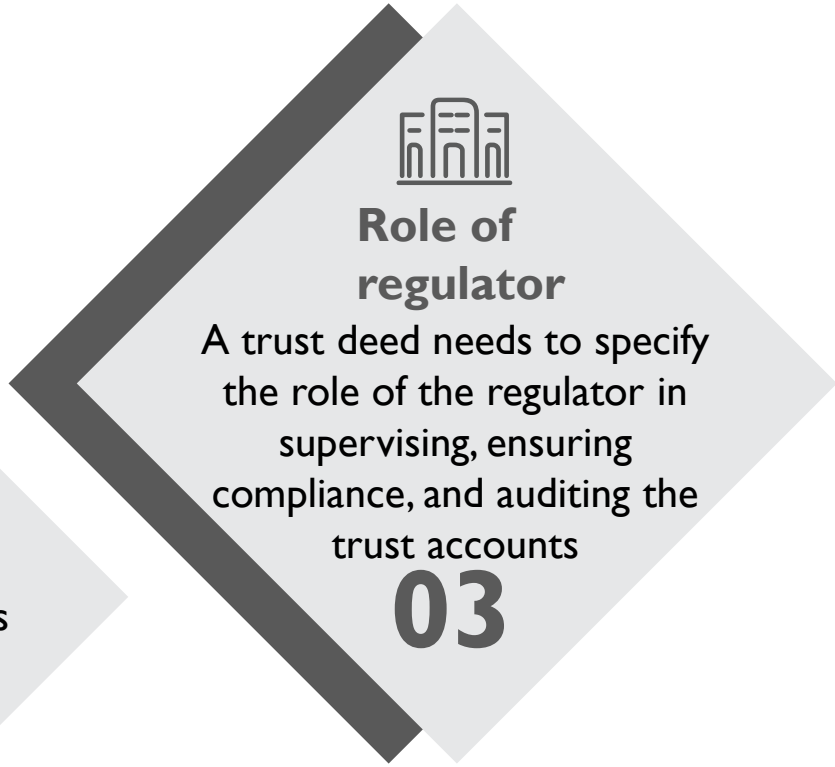
Declaration of trust establishes the relationship of trustees and beneficiaries

01

Customer protection

Specifies principles on restriction on the use of funds and safeguarding of customer funds

02



Role of regulator

A trust deed needs to specify the role of the regulator in supervising, ensuring compliance, and auditing the trust accounts

03

Part G(ii) - Selection of trustees

01 Technical capacity

When selecting trustees, FinTechs should consider the technical capacity of the trustees. Trust accounts need to be in a financial institution or deposit-taking microfinance as per Sec 49 of the Act. The selection will depend on the technical capacity of the selected firm to handle the trust.

02 Reputation

The selection of the trustees to run a trust will be based on the reputation of firms. This influences the confidence of stakeholders that the FinTech is involved with. Trustees with questionable reputation or firms with pending litigation or bankruptcy or insolvency proceedings may not be ideal as trustees.

03 Legal requirements

The selection of trustees will be based on the legal framework that prescribes trust relationships. Other regulations, such as Anti-Money Laundering regulations, will also influence the selection of trustees.

Part G(iii) - Conditions to be met by those to be appointed as trustees

- The FinTechs shall accompany the list of the trustees' proposed names with a copy of the trust agreement between the electronic money issuer and the proposed trustees.

- The electronic money issuer shall, for each trustee submitted to the central bank for approval, indicate the following
  - The citizenship of the trustee
  - A duly filled **Fit and Proper Person Form**, for trustees as set out in Schedule III to these Regulations
  - In case of the corporate trustee
    - the date of incorporation of the trustee
    - the names and qualifications of the directors of the corporate trustee
  - The trustee's ability to perform the functions of a trustee
  - Certificate of good conduct for each trustee proposed
  - Whether the trustee is the subject of any insolvency or bankruptcy proceedings in any country
  - Any other information that the central bank may require to determine a trustee's approval.

Part G(iv) - Duties of trustees

01

Manage trust account

› Trustees manage the trust account and interest account on behalf of the customer

02

Monitor trust account

› Trustees monitor trust accounts to ensure funds in the trust account are equal in value to the electronic money issued

03

Safeguard measures

› Trustees establish safeguard measures to protect funds deposited on a trust account from risks that may occasion loss to beneficiaries of the funds

04

Distribution of interest

› Trustees ensure interest earned on trust account is distributed for the benefit of customers

05

Any other duties

› Trustees perform any other duties as the issuer of electronic money may prescribe

Part H - Access to sensitive payment data

Please click on any tab below to go to the section that you are interested in.

(i) - Compliance with Uganda Data Protection and Privacy Act

(ii) - Access rights and policies concerning sensitive payment data

(iii) - Measures to secure sensitive data

Part H(i) - Compliance with Uganda Data Protection and Privacy Act (1/2)

Introduction of Data Privacy Act

- On 28 February 2019, the President assented to the Data Protection and Privacy Act, 2019. The date of commencement was March, 2019.
- The Act gives effect to Article 27(2) of the Constitution, which protects citizens' rights to privacy. The Article provides that "No person shall be subjected to interference with the privacy of that person's home, correspondence, communication or other property."

Objectives of Data Protection Act

- The objective of the Act is to protect the privacy of individuals by regulating the collection and processing of personal information in Uganda and outside Uganda if the information relates to Ugandan citizens; to provide for the rights of the persons whose data is collected and the obligations of data collectors, data processors, and data controllers; and to regulate the use or disclosure of personal information.

Application of the Act

- The Act gives individuals whose personal information has been requested, collected, processed, or stored powers to exercise control over their data, including consent to the collection and processing, request for the correction and deletion of personal data.
- The Act applies to any person, institution, or public body collecting, processing, holding, or using personal data within Uganda; and outside Uganda for those who collect, process, store, or use personal data relating to Ugandan citizens.

The Act is in line with many international conventions, including the Universal Declaration of Human Rights, to which Uganda is a signatory

Compliance with Uganda Data Protection and Privacy Act (2/2)

The Data Protection Officer

The head of every institution that handles personal data is required to appoint a Data Protection Officer. This is the person in the organization who is the central point of contact and responsible for all data protection compliance issues.

Mandatory requirements for collecting and processing data according to section 7

A person should not collect or process personal data without the prior consent of the data subject except where the collection is; authorized by law, for the performance of public duty, for national security, for the prevention, detection, investigation, prosecution, or punishment of an offense or breach of law, for medical purposes and for compliance with a legal obligation to which the data controller is subject. Section 10 of the Act protects the data subject's right to privacy by prohibiting the collection or processing of personal data in a manner that infringes on the privacy of the data subject. Personal data must be collected directly from the data subject.

Rights of data subjects according to section 24

A data subject who provides proof of identity may request a data controller to give him or her access to the data controller's personal information.

Offenses and penalties

The Act provides for three types of offenses in sections 35 to 37 of the Act, namely;

- unlawfully obtaining, disclosing, or procuring the disclosure to another person of personal data held by a data collector, data controller, or data processor; unlawfully destroying, deleting, misleading, concealing, or altering personal data
- selling or offering for sale any personal data.

Principles of data protection

There are seven principles for the lawful processing of personal data. Processing includes the collection, organization, structuring, storage, alteration, consultation, use, communication, combination, restriction, erasure or destruction of personal data. Broadly, the seven principles are :

Lawfulness, fairness and transparency	Purpose limitation	Data minimization	Accuracy	Storage limitation	Integrity and confidentiality	Accountability
It requires that personal data are processed in a lawful, fair and transparent manner in relation to data subjects.	It means that personal data are to be collected only for specified, explicit and legitimate purposes and it is not allowed to process them further in a way that is not compatible with those	Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.	Ensure that personal data are accurate and are kept up to date where it is necessary	Personal data must be kept in a form that makes it possible to identify data subjects for no longer than is necessary for the purposes of the processing.	In the processing of personal data appropriate security of personal data is ensured.	The data controller shall be responsible for compliance with the principles and shall be able to demonstrate its compliance with them.

Part H(ii) - Access rights and policies concerning sensitive payment data

Data protection, confidentiality, and information security policy should include the following:

Policy Statement

A policy statement in place on data

Responsibilities

Specification on responsibilities within the organization

Definition of personal data

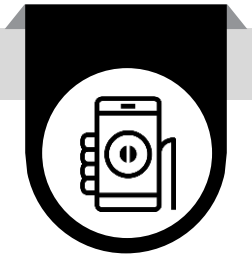
Definition of personal data as per Data Privacy Act

Compliance with data protection Act

Procedures to ensure compliance with Data Privacy Act

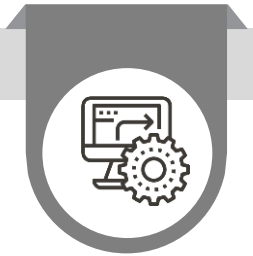
Personal information

Procedures on sharing of personal information



Disclosure rules

Rules on disclosure of sensitive data without consent



Subject access

Procedures on subject access requests

Part H(iii) - Measures to secure sensitive data (1/2)

The regulator will review a FinTech's procedures to protect the data of employees, customers, business partners, and its networks and systems. Questions they may ask include:

01 What is the inherent cybersecurity risk of the FinTech's business model?

02 Does the FinTech have a written cybersecurity program that establishes administrative, operational, and technical controls to mitigate security risks?

03 Are there appropriate policies, including information security policy, an employee-facing acceptable use policy, data classification and handling policy?

04 Does the FinTech conduct regular risk assessments, and vulnerability and penetration testing of its systems?

05 Does the FinTech have dedicated security personnel?

06 Does the FinTech perform an annual risk assessment related to privacy and cybersecurity?

Measures to secure sensitive data (2/2)

07 Does the FinTech train its employees and contractors on privacy and security best practices?

08 Does the FinTech have a comprehensive incident response plan, and is it tested?

09 Does the FinTech manage vendor risk?

10 Does the FinTech have a business continuity and disaster recovery plan and backup protocols?

11 Does the FinTech protect the physical security of its facilities and assets?

12 Does the FinTech implement "reasonable" technical security controls anti-virus software, encryption, access controls, network monitoring?

13 Does the FinTech have an insider threat program to detect the potential theft of proprietary information or intellectual property?

14 Does the FinTech require privacy impact assessments when implementing new systems or processes and has the FinTech suffered past data breaches? What were the consequences?

Sandbox Regulations

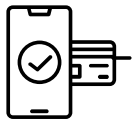
Regulatory sandbox

The regulatory sandbox is a set up to allow small scale, live testing of innovations in a controlled environment.
The objectives of the regulatory sandbox framework are as follows:

Access to payment ecosystem

The regulatory sandbox aims to give limited access to payment system ecosystem for testing of innovative financial products without obtaining a license

01



Increase competition

The regulatory sandbox aims at increasing competition and widen consumer choice by allowing testing of innovative solutions

02

Consumer protection

The regulatory sandbox institutes the appropriate protection safeguards in innovative products and services

03

The sandbox framework is intended to be used by innovators whose proposed solution involves an innovative financial product/service which is not covered under existing regulations and can only be accommodated after regulatory amendment.

It is also meant for innovators whose proposed solution involves a business model that is not currently covered under the existing regulations and requires issuance of new regulations.

The framework excludes technologies that are not at sufficient stage of maturity or development since the sandbox framework is not intended as an accelerator or incubator.

The framework also excludes products that have been rejected by other authorities.

Regulatory sandbox application

Entities intending to operate an innovation in the sandbox shall apply to Bank of Uganda for approval and attach the following documents:

01 Certificate of incorporation

02 Certificate of good conduct for each shareholder and director

03 Proof of payment of application fees

04 Copy of dispute resolution policy

05 Description of innovative concept

06 Testing plan

07 Risk management framework

08 Exit plan from the sandbox

Application process to be followed to operate an innovation in the sandbox.

01 Submission of documents and application fees

Entities operating innovations will be required to submit the application form together with the required supporting documents and pay application fees of UGX 1 million.

Current licensees, financial institutions and microfinance deposit institutions are exempted.

02 Processing and evaluation of applications

Bank of Uganda will upon receipt of applications evaluate the applications to either approve or revoke the request. In consideration, Bank of Uganda will check for:

- Genuineness of innovation
- Ensure consumer safeguards are in place
- Product readiness testing plan
- Suitability of exit plan

03 Approval to operate a sandbox

Bank of Uganda will give their feedback on approval within 60 days of receipt of a proper application from an entity with the proposed innovation.

The approval is valid for 6 months from date of grant and can be extended for a maximum of 6 months.

In case of revocation/suspension, BOU will give reasons for the same and applicant will have a right to be heard.

Annexures

Annexures

APPLICATION FOR A LICENCE OF PAYMENT SYSTEMS PROVIDER OR AN OPERATOR OF A PAYMENT SYSTEM FORM A

FORM A

Annexures

APPLICATION FOR A LICENCE OF AN ISSUER OF A PAYMENT INSTRUMENT

FORM B

Annexures

FIT AND PROPER PERSON FORM

FIT AND PROPER PERSON FORM

Sample outlines for the key policies

Information systems and security policy

This is what you should include in your policy:

1. Policy Objectives
2. Scope of the Policy
3. Policy Maintenance
4. Policy Enforcement
5. User Responsibilities
6. Security Weaknesses and Vulnerabilities
7. Password Requirements
8. Proper Use of Email
9. Acceptable Use of the Internet/Social Media
10. Data Encryption
11. Anti-Virus Software
12. General Software
13. Physical/Hardware Security
14. Responding to Security Breaches
15. Non-Compliance

Cybersecurity policy

This is what you should include in your plan:

Organization
- Roles and responsibilities
- Governance
- Risk assessment
- Exception management

Physical security
- Facilities and data centers
- Badges and visitors
- Office and remote work
- Clean desk

Asset management
- Inventories
- Information classification
- Secure destruction

Suppliers
- Managing third parties

Human resources
- Background checks
- Termination

Acceptable use
- Social media and the web
- Use of assets privacy

Access control
- Add, change, delete access
- Lockout and dormancy
- Passwords
- Remote access

Infrastructure
- Patch management
- Vulnerability management
- Anti-virus
- Log management
- Backup
- Network (IDS/IPS, firewalls)
- Data loss prevention (DLP)
- Web content filtering
- Mobile devices

Incidents
- Reporting incidents and events
- Contact with authorities

Accounting policies and procedures manual

This is what you should include in your manual:

1. Introduction
2. Division of Responsibilities
    a) Board of Directors
    b) Executive Director
    c) Third Party Accountant
    d) Administrative Assistant
3. Accounting
4. Chart of Accounts and General Ledger
5. Receipts
6. Accounts Receivable
7. Procurement
8. Disbursements
9. Internal Control
10. Bank Reconciliations
11. Property, Plant and Equipment
12. Depreciation
13. Financial Reporting
14. Time Reporting
15. End of Month and Fiscal Year End Close
16. Documentation and File Retention

Complaints handling manual

This is what you should include in your manual:

1. Definitions
2. Purpose of this complaints policy
3. What this complaints policy covers
4. Making a complaint
5. How we handle your complaint
6. Confidentiality and data protection
7. Questions and further information
8. Policy responsibility and review

Anti-Money Laundering and CFT policy

This is what you should include in your policy:

1. Objectives
2. Money Laundering and Terrorism Financing
3. Organization of the AML/CFT function
    a. Corporate organization
    b. Policy implementation requirements
    c. Enterprise-wide risk assessment
4. Minimum standards
    a. Customer identification and verification (KYC)
    b. Risk Profile calculation
    c. Customer acceptance policy
    d. Ongoing customer due diligence
    e. Ongoing transaction monitoring
    f. Embargos and sanctions screening
5. Organization of internal control
    a. Suspicious transactions reporting
    b. Procedures
    c. Record keeping
    d. Training
    e. Auditing

Human resources policy and procedures manual

This is what you should include in your manual:

Policies and Procedures

- Personal safety
- Sexual harassment
- Drug and alcohol
- Attendance
- Hours of work
- Meal and rest periods
- Overtime
- Timekeeping
- Personnel records
- Payroll deductions
- Performance reviews
- Promotions
- Transfers
- Termination: reduction in force, layoff/recall

Benefits

- Holidays
- Vacation
- Sick leave
- Bereavement leave
- Paid time off
- Health insurance
- Life insurance
- Retirement and pension plans

Employee and employer responsibility for safety

- Commitment of the company
- Emergency procedures
- Medical services
- Personal protective equipment
- OSHA requirements: safety rules, reporting accidents

Procedures

- Standards of conduct
- Progressive discipline
- Exit process

Summary and acknowledgment

- The importance of the policies and procedures
- Acknowledgment of receipt

Business continuity plan

This is what you should include in your plan:

1. Introduction
2. Risk assessment
3. Critical business functions
4. Plan activation procedures
5. Internal communication procedures
6. Alternate facilities
7. Orders of succession and delegations of authority
8. Plan deactivation
9. Employee contact list
10. Vendor contact list
11. Insurance considerations