ELECTRONIC TRANSACTIONS REGULATIONS 2019, (LI…….)

IN EXERCISE of the powers conferred on the Minister for Communications by section 143 and XXXXXX of the Electronic Transactions Act, 2008, (Act 772) and section xxx of the NITA Regulations these Regulations are made this ……day of ……..……2022

ARRANGEMENT OF REGULATIONS

Contents

PART ONE: TECHNOLOGY POLICY IMPLEMENATION OBLIGATIONS

Obligation of The Presidency and Public Services Institutions

1. Except as provided in these Regulations, there shall be no implementation of information technology and communications consultancy, vendor solicited infrastructure system development, application or infrastructure by any entity of the Presidency and/or Public Services Institution without

i. notification to NITA of such intent,
ii. submission of the proposed EOI and/or RFP and
iii. in the case of sole sourcing all document intended for such issue

for study modifications, amendment, rejection for stated cause, and approval

2(1) The Presidency and Public Services Institutions shall provide NITA with details of all, information technology and communications related Consultancies, systems implementations, including but not limited to details of hardware and software, network and systems designs, security policies, designs of planned and completed system implementations and infrastructure. Such information shall be subject to a compliance check against NITA defined standards, guidelines and interoperability frameworks prior to approval or otherwise.

(2) The Presidency and all Public Services Institutions shall within 90 days of the coming into effect of these Regulations provide NITA the same information as specified in 2 (1) for any existing, ongoing and planned projects.

(3) No Entity of the Presidency and/or Public Services Institution shall issue any tender or procurement request in respect of any design, implementation works which has any information technology based components, requirements, systems or designs howsoever construed without receipt of an approval notification from NITA.

(4) No Tender body set up for the purpose of any procurement evaluation shall commence any evaluation submitted procurement responses to bids issued by any Entity of the Presidency and all Public Services Institutions without receipt of an approval of compliance notification of existing National Information Technology Policy and identified Policy pillars and goals attainment from NITA.

(5) Where such tender or procurement is in excess of Gh¢1,000,000.00 a representative of NITA who shall be a holder of office determined by all the Divisional Heads shall be selected as part of the evaluation board in a manner consistent with the provisions of the Public Procurement Act, 2004 Act 663 as Amended by The Public Procurement (Amendment) Act, 2016, Act 914.

(6) Every Network operator and/or manager providing services to any Entity of the Presidency and/or Public Services Institution shall be subjected to periodic announced

and/or unannounced audits by NITA to ensure compliance with the standards, guidelines, data classifications, national security standards, National Cyber Security Policy and Directives issued by the Minister.

All entities of the Presidency, Public Service Institutions and Independent Network operators shall ensure compliance with the NITA audit findings within the period prescribed for breaches detected in such audit to be corrected.

Except for National Security classified contracts all entities of the Presidency, all Public Services Institutions shall deposit with NITA copies of all ICT related agreements, consultancies and vendor implementing solution to enable NITA monitor for compliance with:

a) all technology related laws,
b) Directives issued by the Minister and/or issued directives,
c) ICT Gazette publications,
d) Technology Transfer Agreements and
e) Digital Economy Policy goal realisation.

(7) Every Entity of the Presidency and/or Public Services Institution shall abide by the decision of NITA and where such decision is challenged, such entity of the Presidency and/or Public Services Institution shall in the case of Public Services Institution be entitled to appeal against the decision of NITA to the Minister and the decision of the Minister shall be final and in the case of the entities of the Presidency, the decision of the Minister shall be forwarded to the President and the decision of the President shall be final..

Information Technology Gazette Publication
There shall be a Gazette to be known as Information Communications Technology Gazette which shall be published by the body with responsibility for publication of legislation, regulations, Gazette notification with each publication numbered serially.

The Information Communications Technology Gazette shall be published digitally, and copies may be made available in Paper-based form upon pre-payment and request.

All Information Communication Technology Gazette Publication shall be made available for paid download on the website of the Publishing authority or as a non-downloadable document on the website sites of NITA, NCA, GIFEC, CSA and the MOCD.

Scope of Gazette Publication
The scope of matter for Gazette Publication shall include without limitation matters relating to:

(a) National ICT prevailing policy,
(b) the ETA
(c) the NITA
(d) directives of the Minister
(e) any matters which are policy relevant and/or derived and provides for certainty, digital and cyber related security enhancement and
(f) any other matter that the Minister may deem fit.

Gazette Publications Mandatory Compliance Issues

The Presidency, all Public Services Institutions, Private Sector Consultants, Selected Vendors, Entity owners, Network Operators and Data Controllers of the Presidency, all Public Services Institutions and/or areas under Regulatory Authorities shall comply with all Gazette Publication relating to all and any of the undermentioned areas:

i. critical databases
ii. protected systems
iii. protected computer
iv. guidelines, standards and security features impacting on core system
v. Critical Infrastructure guidelines, standards, protocols and related matters for protected computers, protected networks, protected systems and critical infrastructure
vi. computer, computer systems and computer networks holding information or through which critical database
vii. additions, modifications and removals made to any matter the subject of Gazette publication
viii. Types of data held, transmitted, encrypted or assessed which must be the subject matter of encryption by NITA and Cyber Security Authority published in the ICT Gazette
ix. Procedure relating to keeping of register of critical infrastructure declared as protected computers, protected systems, protected networks declared by the Minister
x. Person who can access critical infrastructure and Reporting Regime and issues relating to such access and breaches
xi. Procedure to petition the Minister for the declaration of any computer, computer systems, computer networks, technology infrastructure as critical infrastructure.
xii. The procedure for notification issued by the Minister in respect of declaration of any infrastructure as a critical infrastructure and the risk category of such infrastructure;
xiii. Classification of data for which public disclosure is not in the national security interest and holders and operators shall ensure that no person is given access to such national security classified disclosure except in compliance with protocols prescribed otherwise than by Gazette publication by the Minister.
xiv. The Minister shall, by notice in the Gazette, except in respect of classified information, publish such particulars as may be prescribed regarding infrastructure which has been declared as critical infrastructure and prescribed conditions under which the declaration of an infrastructure as a critical infrastructure shall be cancelled or lapse.
xv. Particulars of recognised foreign authentication service provider providing non-classified and non-state sensitive information to any entity and particulars of any revocations under Regulatory Authority
xvi. Particulars of recognised foreign authentication service provider providing non-classified and non-state sensitive information to any entity and particulars of any revocations which are not the subject matter of Regulatory authority
xvii. Particulars of recognised foreign authentication service provider providing non-classified and non-state sensitive information to any Entity of the Presidency and/or Public Service Institution and particulars of any revocations.

GAZETTE PUBLICATIONS AND VALUE ADDED SERVICE (VAS)

NITA in relation to Value Added Service and in line with directives of the Ministry and/or Industry Fora recommendations approved by the Minister shall by Gazette Publications Identify the broad range of Value Added Service requiring

(a) notification to be sent to NITA,
(b) registration with NITA and
(c) requiring certification from NITA

Non Upfront Contract

The Gazette shall provide the procedures to be followed by Metropolitan, Municipal and District Assemblies (MMDAs) in receiving competing Local VAS products at no cost to the MMDAs which can be used by residents within such MMDAs for accessing various services of the MMDAs.

NITA and PSIs Advertising Revenue

NITA shall be responsible for managing all advertising revenue relating to Digital Designs, Platforms along the entire digital ecosystem of entities of the Presidency and Public Services Institutions. Management of advertising revenue shall include without limitation:

(a) Ensuring that all advertising contracts conform with the terms and conditions of adverting revenue generation published by NITA in the Gazette
(b) Designing the payment platform which ensures that all payments are made through the Bank of Ghana accounts dedicated to receipt of advertising revenue and disbursement therein
(c) Ensure allotment of proceeds of advertising revenue in proportions consistent with percentages set out in the Gazette

No entity managing any Entities of the Presidency and /or Public Services Institutions Data Centre shall be entitled to proceeds arising from advertising revenue where such entity is being paid for provision of such management services except where the payment is exclusively determined to be paid from advertising revenue and the payment before tax does not exceed 2% of the Gross advertising revenue received in each month in respect of which management services are provided.

NITA shall be responsible for managing all advertising revenue attributable to the Governments of other participating AfCFTA country arising from NITA hosted Data Centre platforms and activities managed by NITA pursuant to contract and/or bilateral agreements.

The ratio of advertising revenue sharing between the Government of Ghana and other participating AfCFTA country shall be determined by bilateral Agreement between the Government of Ghana and the Governments of such other African countries.

No entity managing the Data Centre owned by any entity of the Presidency and/or Public Services Institutions shall be entitled to proceeds arising from advertising revenue for provision of any management services of the Data Centre.

NITA shall be responsible for managing all advertising revenue between private sector entities arising from the provisions of any bilateral agreement between Ghana and any participating AfCFTA country.

The ratio of advertising revenue sharing between the Government of Ghana and any participating AfCFTA country shall be determined by bilateral Agreement between the Government of Ghana and such participating AfCFTA country.

NITA NOTIFIED VAS

There shall be no compulsory notification regime required for entities engaged in any aspect of VAS except that no VAS entity shall benefit from the rights and benefits of NITA notified VAS entities without voluntary notification submitted to and approved by NITA under these Regulations and under the National Information Communication Technology Policy.

Entities which have provided NITA with notification as VAS and received approval of their notification shall be entitled to participate in and provide services which are not prescribed under these Regulations to be reserved for NITA Registered and/or NITA Certified entities to Entities of the Presidency and /or Public Services Institutions:

No activity of any entity shall be required to be NITA Notified which is wholly, exclusively and necessary under the statutory Regulatory scope of NCA, National Media Commission or a Regulatory activity under the Financial Sector Regulatory except where such entity seek to have NITA perform technical advisory services to such Regulators in technology related disputes between the entity and such Regulators

Every NITA approved VAS shall be required to renew their notification annually and such notification shall be deemed to have lapsed unless renewed before the period of its expiration or before the expiration of three (3) after the annual notification period whichever shall last occur.

On approval of a notification as a subject matter for the issue by NITA of a notification, the applicant shall be required to pay the prescribed statutory fee for the prescribe area of notification provided howsoever that no notification request shall be made in respect of any matter which is a statutorily assigned to any other Regulator Authority, Agency, Commission under the provisions of the 1992 Constitution and/or created by Statute

The Rights and Incentives of VAS entities with NITA issued notification

Certificates shall be prescribed by Gazette Publication and shall be consistent with:

a) the National ICT Policy, Strategy and Action Plan
b) progressively deepening the growth of the Local VAS sector and
c) facilitating Inter-Regulatory cooperation in areas engaged in by VAS with approved NITA notification certificate holders.

It is mandatory for all NITA Notified Certificate Local VAS entities holders in good standing to display on every electronic Homepage and in its Trade Circulars the status of its NITA Notified holding certificate and the date of expiration of same.

It is mandatory for all NITA Notified Certificate Local VAS entities holders not in good standing to remove every display in every electronic Homepage and in its Trade Circulars any status which may represent or cause any reasonable 3rd Parties to believe that such Local VAS is a holder of a Notified NITA issued certificate or that same has not expired and/or has been renewed.

It is an offence under these Regulations to retain on any electronic Homepage or Trade Circular any image or writing which may reasonably lead 3rd Parties or be construed as a representation that an entity is the holder of a NITA Notified issued certificate or that same has not expired and/or has been renewed. Any entity found guilty of this offence shall be liable upon summary trial and conviction to sentence of every Director to a term of imprisonment not exceeding six (6) months or to an entity penalty not exceeding Five Thousand Penalty Points or both.

No NITA Notified Certificate Local VAS shall provide services or solutions on any PSI network infrastructure or device on any critical infrastructure, critical systems, critical computers, in respect of any system on which data classified as Open Data, Sector Specific, Interoperable, Declassified and/or Non-Restricted is stored or accessed.

No Foreign VAS holder of a Notified Certificate shall provide services or solutions on any PSI network infrastructure or device on any critical infrastructure, critical systems, critical computers, in respect of any system on which data classified as Open Data, Sector Specific, Interoperable, Declassified and/or Non-Restricted is stored or accessed.

No holder of a NITA Certified Certificate shall be entitled to provide authentication services and related services on any PSI network infrastructure or device on any critical infrastructure, critical systems, critical computers, in respect of any system on which data classified as Open Data, Sector Specific, Interoperable, Declassified and/or Non-Restricted is stored or accessed.

Offences
Any entity holding a NITA Notification Certificate found guilty of providing services or product reserved for holders of NITA Registered and/or NITA Certified Certificate holders shall upon conviction be liable to a sentence of every Director to a term of imprisonment not exceeding Two (2) years or to an entity penalty not exceeding Ten Thousand Penalty Points or both.

NITA REGISTERED VAS

There shall be no compulsory registration regime required for entities engaged in any aspect of VAS except that no VAS entity shall benefit from the rights and benefits of NITA Registered VAS without voluntary application for registration in compliance with the provisions of these Regulations.

Entities Registered and approved by NITA as Registered VAS entities shall be entitled to the benefits set out as reserved for NITA Registered entities under these Regulations and under the National Information Communication Technology Policy.

Every NITA Registered VAS shall be required to renew the Registration once every two years and such Registration shall be deemed to have lapsed unless renewed before the period of its expiration or before the expiration of three (3) months after the two-year Registration period whichever shall last occur.

On approval of an application for Registration, the applicant shall be required to pay the prescribed statutory fee for the prescribe area for Registration.

No activity of any entity shall be required to be NITA Registered which is wholly, exclusively and necessarily under the constitutional and/or statutory Regulatory scope of any other Regulatory entity, Agency and/or Commission

The Rights and Incentives of VAS entities with NITA Registration entities may be deepened by Gazette Publication and shall be consistent with Policy goals and objectives under the National ICT Policy, Strategy and Action Plan.

Every NITA Registered Certificate Local VAS entity holder in good standing shall display on every electronic Homepage and in its Trade Circulars its status as a NITA Registered entity and the date of expiration of same.

Any Local VAS entity holding the status of a NITA Registered entity not in good standing commits an offence if it displays in any electronic Homepage and in its Trade Circulars any status which may represent or cause any reasonable 3rd Parties to believe that such Local VAS is a NITA Registered entity.

Every Director and employee of the company responsible for the publication shall be liable upon summary trial and conviction to be prosecuted and shall on conviction be liable to pay a fine of xxxx penalty points or to the sentence of xxx months imprisonment or to both.

Scope of Local VAS activities

No Local VAS not being a NITA Registered and/or NITA Certified entity shall provide services or solutions to any entity of the Presidency and/ or PSI network infrastructure or device on any critical infrastructure, critical systems, critical computers on which data is classified as Protected, Sector Specific, Interoperable, Multiple of such classifications unless same is :

i. a Ghanaian incorporated entity
ii. owned by Ghanaians who together own at least 40% of the equity of the incorporated entity
iii. an entity registered with the Data Protection Commission with a valid and unexpired DPA Certificate and remains DPA compliant
iv. an entity which has applied for, met the NITA, CSA and National Security prescribed criteria set out for Registered Local VAS and be issued with a NITA Registered Entity Certificate and is not in default of renewal

No Local VAS shall provide services or solutions on any GI network infrastructure or device on any critical infrastructure, critical systems, critical computers, authentication services and related services in respect of any system on which data is classified as Top Secret, Confidential, Restricted, Protected or Multiple is stored or accessed unless same is :

i. a Ghanaian incorporated entity

ii. Wholly owned by Ghanaians who together own at least 40% of the equity of the incorporated entity
iii. an entity registered with the Data Protection Commission with a valid and unexpired DPA Certificate and remains DPA compliant
iv. an entity which has applied for, met the NITA, CSA and National Security prescribed criteria set out for Certified Local VAS and be issued with a NITA Certified Entity Certificate and is not in default of renewal

No Foreign VAS shall provide services or solutions on any GI network infrastructure or device on any critical infrastructure, critical systems, critical computers, authentication services and related services in respect of any system on which data classified as Top Secret, Confidential, Restricted, Protected or Multiple is stored or accessed unless same is :

i. Incorporated as a Ghanaian incorporated entity or is registered as an External company under the Companies Code
ii. An entity with a registered Office in Ghana
iii. an entity which shall have no right to copy and/or retain any GI data on any of its devices and/or network or cause any data to be routed through any third country
iv. an entity which provides a credible structure which assures that all employees responsible for any aspect of its operations in relation to such matters are National Security vetted and approve
v. an entity registered with the Data Protection Commission with a valid and unexpired DPA Certificate and remains DPA compliant
vi. an entity which has applied for, met the NITA, CSA and National Security prescribed criteria set out for Certified Local VAS and be issued with a NITA Certified Entity Certificate and is not in default of renewal
vii. an entity which shall not be subject to the law of any foreign jurisdiction under which service to the Republic of Ghana is prohibited and in the event of such prohibition undertakes to incorporate an entity outside the control of the jurisdiction of the prohibiting country to provide same services or
    a) where same are incapable of being satisfied to renounce its interest in the service and solutions
    b) transfer to Ghana the non-exclusive right to use same at no cost to the Ghana Government and
    c) provide such source code related information as to enable Ghana to develop or engage 3rd Parties updates, patches, bug resolutions, modifications, reverse engineer and do all such things as to enable the Republic of Ghana to use same and protect it national and sovereign interests.

No Local VAS not being NITA Registered and/or NITA Certified shall provide services or solutions to any entity of the Presidency and/ or PSI network infrastructure on any system on which data classified as Open Data, Sector Specific, Interoperable, Declassified and/or Non-Restricted is stored or accessed unless same is :

i. a Ghanaian incorporated entity
ii. owned by Ghanaians who together own at least 40% of the equity of the incorporated entity

iii. an entity registered with the Data Protection Commission with a valid and unexpired DPA Certificate and remains DPA compliant
iv. an entity which has applied for, met the NITA, CSA and National Security prescribed criteria set out for Registered Local VAS and be issued with a NITA Registered Entity Certificate and is not in default of renewal

No Foreign VAS shall provide services or solutions on any entity of the Presidency and/or PSI network infrastructure or device on any critical infrastructure, critical systems, critical computers, in respect of any system unless such foreign VAS:

i. incorporates Ghanaian incorporated entity or is registered as an External company under the Companies Code
ii. Has a registered Office in Ghana
iii. Shall not copy and/or retain any GI data on any of its devices and/or network or cause any such data to be routed through any 3rd Country
iv. registered with the Data Protection Commission with a valid and unexpired DPA Certificate and remains DPA compliant
v. Has applied for, met the NITA, CSA and National Security prescribed criteria set out for Registered Local VAS and be issued with a NITA Registered Entity Certificate and is not in default of renewal
vi. Is not subject to the law of any foreign jurisdiction under which service to the Republic of Ghana is prohibited and in the event of such prohibition undertakes to incorporate an entity outside the control of the jurisdiction of the prohibiting country to provide same services or
    d) where same are incapable of being satisfied to renounce its interest in the service and solutions
    e) transfer to Ghana the non-exclusive right to use same at no cost to the Ghana Government and
    f) provide such source code related information as to enable Ghana to develop or engage 3rd Parties updates, patches, bug resolutions, modifications, reverse engineer and do all such things as to enable the Republic of Ghana to use same and protect it national and sovereign interests

No Foreign VAS shall provide services or solutions on any entity of the Presidency and/or PSI network infrastructure or device on which data classified as Open Data, Sector Specific, Interoperable, Declassified and/or Non-Restricted is stored or accessed unless such Foreign VAS:

i. incorporates Ghanaian incorporated entity or is registered as an External company under the Companies Code
ii. Has a registered Office in Ghana
iii. Shall not copy and/or retain any GI data on any of its devices and/or network or cause any such data to be routed through any 3rd Country
iv. registered with the Data Protection Commission with a valid and unexpired DPA Certificate and remains DPA compliant
v. Has applied for, met the NITA, CSA and National Security prescribed criteria set out for Registered Local VAS and be issued with a NITA Registered Entity Certificate and is not in default of renewal

vi. Is not subject to the law of any foreign jurisdiction under which service to the Republic of Ghana is prohibited and in the event of such prohibition undertakes to incorporate an entity outside the control of the jurisdiction of the prohibiting country to provide same services or

g) where same are incapable of being satisfied to renounce its interest in the service and solutions
h) transfer to Ghana the non-exclusive right to use same at no cost to the Ghana Government and
i) provide such source code related information as to enable Ghana to develop or engage 3rd Parties updates, patches, bug resolutions, modifications, reverse engineer and do all such things as to enable the Republic of Ghana to use same and protect it national and sovereign interests

Offences

It is an offence under these Regulations to retain on any electronic Homepage or Trade Circular any image or writing which may reasonably lead 3rd Parties or be construed as a representation that an entity is the holder of a NITA Registered issued certificate or that same has not expired and/or has been renewed.

Any entity found guilty of this offence shall be liable upon summary trial and conviction to sentence of every Director to a term of imprisonment not exceeding Two (2) years or to an entity penalty not exceeding Ten Thousand Penalty Points or both.

No holder of a NITA Registered Certificate shall be entitled to provide authentication services and related services on any PSI network infrastructure or device on any critical infrastructure, critical systems, critical computers, in respect of any system on which data classified as Open Data, Sector Specific, Interoperable, Declassified and/or Non-Restricted is stored or accessed. Any entity found guilty of this offence shall be liable upon summary trial and conviction to sentence of every Director to a term of imprisonment not exceeding Two (2) years or to an entity penalty not exceeding Ten Thousand Penalty Points or both.

NITA CERTIFIED VAS

There shall be no compulsory certification regime required for entities engaged in any aspect of VAS except that no VAS entity shall benefit from the rights and benefits of NITA Certification VAS without voluntary application for registration in compliance with the provisions of these Regulations.

Entities approved by NITA as Certified VAS entities shall be entitled to the benefits set out under these Regulations in addition to all such specified benefits set out under Gazette publication pursuant to the provisions of the National ICT Policy.

Every NITA Certified VAS shall be required to renew the Certification once every two years and such Certification shall be deemed to have lapsed unless renewed before its expiration or before the expiration of three (3) months after the two-year Certification period whichever shall last occur.

On approval of an application for Certification, the applicant shall be required to pay the prescribed statutory fee for the prescribe area for Certification provided that no Certification request shall be entertained in any matter under the constitutional and/or statutory Regulatory scope of any other Regulatory entity, Agency and/or Commission. .

The Rights and Incentives of VAS entities with NITA issued Certified Certificate holders shall be prescribed by Gazette Publication and shall focus on Policy required NITA Certified activities under the National ICT Policy, Strategy and Action Plan which requires NITA to progressively deepen the growth of such VAS ecosystems and promote Inter-Regulatory cooperation in areas engaged in by VAS with approved NITA Certified certificate holders.

It is mandatory for all NITA Certified Certificate Local VAS entities holders in good standing to display on every electronic Homepage and in its Trade Circulars the status of its NITA Certified holding certificate and the date of expiration of same.

It is mandatory for all NITA Certified Certificate Local VAS entities holders not in good standing to remove every display in every electronic Homepage and in its Trade Circulars any status which may represent or cause any reasonable 3rd Parties to believe that such Local VAS is a holder of Certified type of NITA issued certificate or that same has not expired and/or has been renewed.

Offences
It is an offence under these Regulations to retain on any electronic Homepage or Trade Circular any image or writing which may reasonably lead 3rd Parties or be construed as a representation that an entity is the holder of a NITA Certified issued certificate or that same has not expired and/or has been renewed.

Any entity found guilty of this offence shall be liable upon summary trial and conviction to sentence of every Director to a term of imprisonment not exceeding Five (5) years, or to a fine not exceeding Twenty Thousand Penalty Points or both.

Offences
Any entity not being a NITA Notified status holder providing services or product reserved for holders of NITA Notified status holders under these Regulation, the National Information Communication Policy and/or Gazette Publication commits an offence.

Any entity which commits an offence shall upon conviction be liable to a sentence of every Director to a term of imprisonment not exceeding One (1) year or to an entity penalty not exceeding Five Thousand Penalty Points or both.

Any entity not being a NITA Registered, or NITA Certified Certificate providing services or product reserved for holders of NITA Registered and/or NITA Certified status holders under these Regulation, the National Information Communication Policy and/or Gazette Publication commits an offence.

Any entity which commits an offence shall upon conviction be liable to a sentence of every Director to a term of imprisonment not exceeding Three (3) years or to an entity penalty not exceeding Fifteen Thousand Penalty Points or both.

Multiple use Resident selection base Procurement
Metropolitan, Municipal and District Assembly (MMDA)

The Procurement Process for inviting multiple Local VAS entity product for resident users to determine their preferential product of choice shall constitute the contract selection and award process at no cost to the MMDA.

No MMDA shall process any application received from any Local VAS entity under the Multiple use Resident section based procurement programme unless proof is provided that:

i. The Local VAS is registered with the Data Protection Commission
ii. The Local VAS has a Notification Certificate issued by NITA and valid at the time of response to the issued bid
iii. The Local VAS product has been evaluated and confirmed by NITA that the product meets the GI platform security and other requirements
iv. The product is limited in use to access user information and related payments
v. displays District and Municipal related By-laws and notices,
vi. the product makes exclusive use of Open Data intended for general public use and/or digital entrepreneurial growth
vii. There is no MMDA related data input features, data retention feature held on the systems of such multiple Local VAS entity product, resident users may have the option to download such permitted records of the MMDAs on such user enable devices
viii. The product and/or service does not perform any functions which is reserved for NITA Registered and NITA Certified status holders
ix. No payment is required for use by MMDAs or Users and payments to such Local VAS shall be in accordance with the provisions of these Regulations advertising revenue sharing and payment revenue percentage sharing
x. Such products shall not have access monopoly rights to MMDA record interface consistent with the provisions of these Regulations.

Multiple Local VAS entity means any incorporated or persons trading under the Business Names which :

(a) provides any digital solution, design or products designed for use exclusively by MMDAs,
(b) meets the requirements of these Regulations and
(c) which is confirmed at the time of first use and subsequent annual renewals by NITA to have met the security and other requirements sets out by Gazette Publication issued by NITA
(d) and product has any or combinations of all or some of the undermentioned features and/or capabilities:
    i. users are limited to such MMDA documents publicly disseminated,
    ii. user records held by such MMDA,
    iii. capable of being use for payments to and receipt of receipts from the MMDA,
    iv. sending and receiving complaints and correspondence with such MMDA,
    v. capable of being used as a virtual platform for engaging in MMDA related meetings with residents,

vi. capable being used for the payment of utilities charges, Statutory taxes and levies to such Service Providers or Statutory taxes and levies receiving institutions within the MMDA
vii. enable user download of MMDA approved user records on users devices
viii. providing users with features for engaging at multiple levels and purposes with such MMDA permitted under these regulations and Gazette Publications issued by NITA

Local VAS products selected under the Multiple Products resident users selected programs at the MMDA levels shall be entitled to :

i. payment revenue sharing and
ii. advertising revenue sharing

arising wholly, necessarily and exclusively to the use of such Local VAS entity product in the payment to the MMDA and in proportions set out in the schedule of Fees passed as an annexure to this Regulations from time to time.

Public Services Institutions Providing Utility Services

The Procurement Process for inviting multiple Local VAS entity product for users of products of Public Services Institutions providing Utility services in matters relating to billing, payment, accounts tracking, and complaint processes and receipt of notices shall constitute the contract selection and award process of such Public Services Institutions providing Utility Service and at no cost to product design and/or use of such Utility service provider.

Any Local VAS entity applying to participate with multiple Local VAS entity bid products shall provide evidence to the receiving Utility provider that:

i. The Local VAS is registered with the Data Protection Commission
ii. The Local VAS has a NITA Certified status issued by NITA and valid at the time of response to the issued bid
iii. The Local VAS product has been evaluated by NITA and confirmed that the product meets the security and other requirements
iv. The product is limited in use to access user information and related payments
v. The product acknowledges and issues payment receipt notices issued by the Utility providing Public Service Institution
vi. The product reproduces and updates Open Data content issued information by the utility provider
vii. The product is compliant with the DPA and statutory, Gazette publications, Ministerial and NITA directives and all matters related to data input or access rights with any critical database, protected computers, protected network or protected system

Local NITA Certified VAS entity products selected under the Multiple Products residents selected programs for Public Services Institutions providing utility services shall be entitled to :

iii. payment revenue sharing and
iv. advertising revenue sharing

arising wholly, necessarily and exclusively to the use of such Local VAS NITA Certified status entity products in the payment to the Utility Provider and in proportions set out in the schedule of Fees passed as an annexure to this Regulations from time to time.

Entities of the Presidency and Public Services Institutions Revenue Sharing and Advertising Bids

PPA in collaboration with NITA shall by Gazette Publications determine such aspects of Entities of the Presidency and Public Services Institutions Bids that may be the subject matter of Revenue Sharing and Advertising Bids envisaged under the Policy.

PPA shall be responsible for sponsoring the necessary amendments to the PPA and Regulations thereunder to ensure Policy effectiveness and goal attainment

NITA Procurement Support and Collaboration Responsibilities

NITA shall provide to the PPA and requesting Entities of the Presidency and Public Services Institutions technical knowledge in all ICT impacting EOIs and RFPs.

The PPA shall not approve any EOI and/or RFP submitted by an entity of the Presidency and/or Public Services Institutions unless the PPA has prior to issue of such issue received prior confirmation from NITA in writing of the undermentioned matters:

i. That there is no duplicating consultancy and selected Vendor provided product within the GI ecosystem capable for providing the services and products required under the prospective EOI and/or RFP
ii. That the contents of the EOI and the RFP are sufficiently detailed to ensure that submitted responses would provide the required end-product solutions without a requirement for additional works, re-issue of EOI and RFP for lack of sufficiency in detail
iii. Content of the EOI and RFP are consistent with the Digital Policy, Strategy, Action Plan and Guidelines and the goal attainment
iv. Contents adequately address all implications for cyber security, relevant data classifications, authentication and all matters for which NITA is given the policy monitoring and implementation statutory responsibility.

NITA, PPA and Multiple Local VAS bids

All MMDAs shall submit their invitation for multiple Local VAS entity participation to NITA and the PPA for compliance approval before same shall be published.

All Public Services Institutions providing Utility services shall submit their invitations for multiple Local VAS entity participation to NITA and the PPA
for compliance approval before same shall be published.
.

BENEFITS OF NOTIFICATION, REGISTRATION AND CERTIFICATION

NITA shall in respect of VAS which have their notification, registration and certifications approved by NITA:

i. Compile a credible register for networking between Local VAS service providers,

ii. Create of a pool of stakeholders for engagement in digital policy penetration and goal attainment,
iii. Receive application and advocacy papers and notes from such approved entities seeking to deepen the Digital Ecosystem of entities within the Presidency and Public Services Institutions, Businesses and Consumers/Users of technology and
iv. Facilitating challenges identified as change management needful approaches of Regulators in areas of operations of such VAS entities.

Inter-Regulatory Cooperation

NITA shall be responsible for engaging with all Regulatory Authorities in all Inter-Regulatory required cooperation matters for the purposes of carrying out the prescribed goals and attaining the prescribed target set out under the Policy, Strategy and Action Plan of prevailing National ICT Policy.

The Minister shall be responsible for issuing directives to guide the meetings of all Inter-Regulatory cooperation under the National ICT Policy and the supervising Ministries of the Regulatory Authorities shall cooperate with the Minister in ensuring compliance with directives issued by the Minister of all Regulators under their respective Ministries.

The Minister shall have a Presiding role over Inter-Regulatory Cooperation meeting where issues are referred to the Minister by any of the parties in Inter-Regulatory meeting and discussions.

NITA shall have primary responsibility for the convening, monitoring and implementing decisions of Inter-Regulatory cooperation relevant to each Pillar goals under the National ICT Policy, Strategy, Action Plan and Guidelines.

NITA shall provide six monthly Reports to the Minister on the progress of Inter-Regulatory cooperation relevant to each Pillar which shall include without limitation, the following:

(b) Particulars of each Inter-Regulatory Committee composition
(c) Scope of Inter-Regulatory Committee discussions
(d) Heading of Inter-Regulatory Committee discussions relating to Local VAS Notification entities
(e) Heading of Inter-Regulatory Committee discussions relating to Local VAS Registration entities
(f) Heading of Inter-Regulatory Committee discussions relating to Local VAS Certification entities
(g) Heading of Inter-Regulatory Committee discussions relating to NCA Industry Forum entities
(h) Heading of Inter-Regulatory Committee discussions relating to CA Industry Forum entities Heading of Inter-Regulatory Committee discussions relating to ETA Industry Forum entities Heading of Inter-Regulatory Committee discussions relating to NITA Industry Forum entities Heading of Inter-Regulatory Committee discussions relating to new technology within Regulatory areas
(i) Conclusions of Inter-Regulatory Committee discussions
(j) In-conclusive matters under of Inter-Regulatory Committee discussions
(k) Deferred matters under the Inter-Regulatory Committee discussion
(l) Matters which seeming require Ministerial Directive

ENTITIES OF THE PRESIDENCY AND PUBLIC SERVICES INSTITUTIONS INTERSECTORIAL COMMITTEE

Entities of the Presidency and Public Services Institution shall constitute an Inter-sectorial Standing Committee dedicated to promoting and facilitating the attainment of full interoperability across the entire PSIs ecosystem in a manner consistent with the National ICT Policy, Strategy, Action Plans and Guidelines.

The Standing Committee shall be composed of such persons appointed by the Director General of NITA, NCA and GIFEC and headed by such person as the Minister shall direct.

The Standing Committee shall be assisted by the Chief Information Officers of Institutions identified under the Digital Strategy, Action Plan and Guidelines document and Check List thereunder as modified by the Minister from time to time.

The Standing Committee shall report to the Director General of NITA who shall study all Standing Committee Reports and make recommendations pursuant to such study to the Board of NITA for their deliberations and recommendation to the Minister.

The Minister shall be responsible for the issue of all Directives to the Entities of the Presidency and Public Services Institutions Inter-sectorial standing Committee and NITA shall ensure the implementation of the Directives by all CIOs and Entities of the Presidency and Public Services Institutions.

Consumer Protection Complaints

NITA shall provide Regulatory oversight over all consumer complaints in respect of eCommerce related transactions in goods and/or services in respect of which any resident in Ghana is a complainant.

Consumer Protection complaints shall exclude complaints in relation to matters which are within the scope of other Regulatory Bodies in Finance, Banking, Industry, Insurance and Pension

Registration of eCommerce Providers & Entities

There shall be no compulsion of on Local, AfCFTA and Foreign eCommerce providing entities to register with any Consumer Protection Complaint Association

There shall be no compulsion on Local, AfCFTA and Foreign eCommerce providing entities to register with NITA

Benefit of Consumer Association Registration

Consumer Protection Complaint Association shall be required to maintain an electronic list of such Local, AfCFTA and Foreign eCommerce registered providers with such Association on its website and shall ensure that the content of the website remain accurate and updated in timely manner.

All registered Consumer Protection Complaint Associations shall promote the advantage to users of eCommerce services to the advantage of dealing with registered Local, AfCFTA and Foreign eCommerce providing entities registered with such Consumer Protection Association for the resolution of disputes through Alternative Dispute Resolution.

Prohibition of exclusion of Ghana law

There shall be no exclusion of the Law of Ghana as the choice of law and the fora of Ghana as the place of adjudication in all eCommerce related conflict and dispute resolution and any provision to the contrary in any eCommerce standard agreement shall be null, void and of no effective where any aggrieved party commences any legal proceeding in the High Court in Ghana.

Where any Ghanaian incorporate entity engages in any ecommerce related sale of product or service, there shall be no exclusion of the Law of Ghana as the choice of law and the fora of Ghana as the place of adjudication in all eCommerce related conflict and dispute resolution and any provision to the contrary in any eCommerce standard agreement shall be null, void and of no effective where any aggrieved party commences any complaint process to any registered Consumer Protection Complaint Association and proceedings thereunder or any legal proceeding in the High Court in Ghana.

Bilateral Agreements under AfCFTA & Dispute Resolutions

Entities engaged in eCommerce trading transactions in AfCFTA areas which are the subject matter of Bilateral Agreements between Ghana and residents of such participating AfCFTA countries shall be bound by the provisions of such bilateral agreements relating to dispute settlement of technology mediated transactions relating to payment and delivery for goods and services to residents within such participating AfCFTA country.

Consumer Rights Publication

The consumer rights of persons receiving digital services shall be published by the Minister in the ICT Gazette in consultation with Consumer Associations registered and unregistered with Minister that shall respond to a publication by the Minister solicitating for views, suggestions and consumer right protection matters.

Irrespective of the terms and conditions related to any online purchase of goods and services to residents in Ghana, all suppliers of goods and services inclusive of foreign supplies delivered to residents in Ghana shall be bound by the terms and conditions relating to sales of goods set of in Gazette Publications by NITA.

All entities engaged in sales of goods and services to residents in Ghana shall comply with provisions of the Companies Act in relation to having a local presence in Ghana in a manner consistent with the External Companies Registration in Ghana or the incorporation of companies in Ghana.

Entities engaged in eCommerce relating trading incorporated in Ghana or registered as External companies in Ghana shall be entitled to be registered as VAS entities under the notification procedure and shall not be engaged in any activities reserved for entities subject to the NITA Registration and Certification activities set out in the ICT Gazette Publications.

Consumer Complaints Technology Platform

The Consumer Protection Complaints Associations under which NITA provides Regulatory oversight shall register their Consumer Complaints conflict resolution procedures with NITA

Consumer Protection Complaints Associations shall be entitled to opt for the use of the technology platform of the Technology Appeal Tribunal limited to the use of the filing, services, hearing and process related platforms.

Consumer Protection Complaint Association conflict resolution procedures shall be binding between eCommerce which associate with such Registered Associations and consumers of such eCommerce transactions.

Consumer Protection Complaint Associations shall as part of the registration with NITA provide details of Local, AfCFTA and Foreign eCommerce registered providers.

Arbitration in Digital Disputes

NITA shall in consultation with the Ghana Arbitration Centre and the Judicial Service of Ghana provide the technical expertise for the development of Digital Framework for receiving complaints and adjudicating on disputes between NITA approved VAS with NITA approved Notification, Registration and/or Certification.

of Arbitration developed by the Ghana Arbitration Centre and the Judicial Service of Ghana shall constitute the binding Rules of Mediation and/or Arbitration which shall be binding on all NITA approved VAS with NITA approved Notification, Registration and/or Certification.

The Rules of Arbitration shall be published in the Ghana ICT Gazette and shall be incorporated by all NITA approved VAS with NITA approved Notification, Registration and/or Certification as their dispute resolution process which shall be first accepted by users of their services as a precondition for access and use by consumers.

Business Sector Ecosystem

Subject to compliance with Regulatory Directives and statutory provisions inclusive without limitation of the Data Protection Act, Statutes and Regulations made thereunder the Private Sector Business ecosystem users shall be entitled for non-Entities of the Presidency and Public Services Institutions contract purposes and service to the use of

i. their preferential authentication service providers,
ii. network designers,
iii. network security arrangement,
iv. data classification,
v. terms and conditions for use,
vi. security features and designs,
vii. business and services products and
viii. other matters consistent with law and their business objectives

In all interface with Entities of the Presidency and Public Services Institutions, Private Sector Business and users of technology shall adhere to the standards, protocols, access control rights and prohibits of Entities of the Presidency and Public Services Institutions and all Cyber Security Protocols and the use of Entities of the Presidency and Public Services

Institution approved authentication service provider in all activities on Entities of the Presidency and Public Services Institutions digital platforms.

For purposes of this section, all Private Public Partnership digital infrastructure, network and services shall be deemed to constitute part of the Entities of the Presidency and Public Services Institutions ecosystem.

Consumer/ Users of Technology Ecosystem
Subject to compliance with Regulatory Directives and statutory provisions inclusive without limitation of the Data Protection Act, Statutes and Regulations made thereunder the Resident and Non Resident data subjects shall for purposes of private use of their networks and equipment in their engagement and interaction with non-Entities of the Presidency and Public Services Institutions be entitled to the use of

i. their preferential authentication service providers,
ii. network designers,
iii. network security arrangement,
iv. data classification,
v. terms and conditions for use,
vi. security features and designs,
vii. business and services products and
viii. other matters consistent with law and their social needs and preferences

In all interface with Entities of the Presidency and Public Services Institutions, consumers and users of technology shall adhere to the standards, protocols, access control rights and prohibits of Entities of the Presidency and Public Services Institutions and all Cyber Security Protocols and the use of Entities of the Presidency and Public Services Institution approved authentication service provider in all activities on Entities of the Presidency and Public Service Institutions digital platforms.

For purposes of this section, all Private Public Partnership digital infrastructure, network and services shall be deemed to constitute part of the Entities of the Presidency and Public Services Institutions ecosystem.

Universal Service and Universal Access
NITA shall be responsible for providing collaboration engagement with NCA and GIFEC for the purposes of evaluating issues relating to bandwidth and universal service and universal access necessary for enabling all residents in the territory to access full scope PSI digital services in line with the policy and goal set out in the prevailing Digital Policy Strategy and Action Plan

The NCA shall pursuant to such collaborative determination and progressive expansion of the definitional scope of universal service and universal access, ensure that the conditions of the license are updated in a manner which would enable the NCA to ensure Network Operators roll out Service Level Agreement which are consistent with such expanded scope of Universal Service and Universal Access.

GIFEC shall pursuant to such collaborative determination and progressive scope of universal service and universal access definitional expansion approved by the Minister, ensure that the

operations of GIFEC in rural communities, marginalised, deprived and urban poor communities are upgraded in a timely manner consistent with the expanded definitional scope of Universal Service and Universal Access at all times.

NITA shall be responsible for receiving quarterly reports from the Chief Information Officers of GIFEC and NCA on matters relating to the progressive penetration of universal service and universal access, the challenges encountered and the technical support if any, required from NITA.

NITA and GIFEC shall provide technical support to Digital Libraries in Educational Institutions and MMDAs in rural communities, marginalised, deprived and urban poor communities in order to progressively expand universal access and universal service availability to PSI digital services nationwide.

Public Digital Records and Archiving

NITA shall provide technical support to the Public Records and Archives Administration Department (PRAAD) in the development of a National Digital Archival Policy which shall be published in the Gazette and shall be binding on all PSIs.

PRAAD shall have primary responsibility for the authenticity of digital and paper-based records of PSI documents in the custody of PRAAD.

Chief Information Officers of all Entities of the Presidency and Public Services Institutions shall ensure that such Institution's legacy data access and storage:

i. does not suffer any degradation of data quality,
ii. does not suffer any reliability or loss of content,
iii. are capable of being accessed by authorised users along the PSI ecosystem at all times notwithstanding their encryption
iv. is incapable of being the subject matter of alteration and the integrity of the data remains unchanged.
v. underlining software to be used in data access by the PSI always assures data integrity at all times.
vi. issues relating to source codes access are made available to Government for storage and use for legacy data.

DATA BASE AND BIG DATA

NITA shall be responsible for the design, security protocols, digital forensic tracking, management and content originator authentication of the National Database for the improvement of interoperability within the Presidency and the Public Services Institutions.

NITA shall provide training and support to CIO of the Presidency and Public Services Institutions in the procedure for creation of databases, ensuring interoperability across the Presidency and Public Services Institutions consistent with the access control and other relevant protocol relevant to each sector classification under these Regulations

Except in matters relating to National Security in respect of which NITA is a subordinate Public Services Institution, NITA shall have responsibility for the :

(a) provision and assignment of standards, protocols, access control levels for all databases of the Presidency and all other Public Services Institutions in accordance with the classification of data in these regulations and the respective level of every employee within the Presidency and the Public Services Institutions

(b) design of interoperability standards and protocols within the database ecosystem of the Presidency and the Public Services Institutions to ensure database interoperability and content download without compromise to data integrity, source authentication, detection of changes made in any data record, prevention of data deletion amongst other matters that NITA shall deem necessary and consistent with opportunities provided by new technology and threats arising to existing and evolving technology
(c) progressively develop the distribute ledge technology database to maximise security of data, authentication of data, deepening of digital forensic ecosystem, minimisation of risk of wholesale data loss and/or compromise

Save for matters relating to national security and data and records classified as Top Secret, Secret, Confidential, Restricted and Protect under these Regulations, Interoperability Standards and protocols by NITA shall be the subject matter of Gazette Publication.

Save for matters relating to national security and data and records classified as Top Secret, Secret, Confidential, Restricted and Protect under these Regulations, Interoperability Standards and protocols by NITA shall have the status of Top Secret and shall be shared amongst persons entitled to Top Secret within the National Security, Presidency and Public Services Institutions.

Offences

Disclosure of standards, protocols and any matter classified as Top Secret, Secret, Confidential, Restricted and Protect under these Regulations to unauthorised persons shall constitute an xxxx degree offence under these Regulations and any person found guilty of this offence shall be liable upon summary trial to a fine not exceeding xxxx penalty point and not less than xxxx penalty points and/or a term of imprisonment not less than xxxx years and not more than xxx years.

Soliciting for standards, protocols and any matter classified as Top Secret, Secret, Confidential, Restricted and Protect under these Regulations by any unauthorised persons shall constitute an xxxx degree offence under these Regulations and any person found guilty of this offence shall be liable upon summary trial to a fine not exceeding xxxx penalty point and not less than xxxx penalty points and/or a term of imprisonment not less than xxxx years and not more than xxx years.

Designation of Operations

3(1) National Information Technology Agency shall for purposes of the discharge of its objects have divisional heads which shall be responsible for:

a) networks and connectivity infrastructure, security systems, hardware and software and related matters
b) Business Unit Services, Enterprise Resource Management, Customers Management Services, Standards & Systems applications approval, Guideline and Standards parameters, Project Management and such other related responsibilities
c) Financial, Regulatory, Corporate affairs and Administration and related matters

The divisional heads shall report to the Director General and hold office whose ranking shall be equivalent to that of the Deputy Director General.

(2) The Division of Operations shall be responsible for networks and connectivity infrastructure, security systems, hardware and software and related matters used by entities of the Presidency and the Public Services Institutions.

(3) The Division of Operations shall be responsible for Business Unit Services, Enterprise Resource Management, Customers Management Services, Standards & Systems applications approval, Guideline and Standards parameters, Project Management and such other related responsibilities used by entities of the Presidency and the Public Services Institutions.

(4) The Division of Operations shall be responsible for Financial, Regulatory, Corporate affairs and Administration and related matters consistent with the ETA, these regulations.

Each Divisional Head of NITA shall provide half yearly reports to the Board through the Managing Director.

(5) The Board shall define the scope of works and activities of the Divisional Heads and subsidiary offices and departments relevant to such divisions of operations in consultation with the Director General and in a manner consistent with the statutory objects of NITA and directives from the Minister.
Each Divisional Head of NITA shall provide half yearly reports to the Board through the Managing Director.

Reporting Regime for ICT implementations
7(1) NITA shall submit monthly reports to the Auditor General for information related to compliance approvals in relation to PPA issued tenders and shall notify the Minister of responses received from the Auditor General.

(2) NITA shall in respect of all approval given for which the Auditor General has power to audit under the provision of the Audit Service Act, 2000, Act 584 provide a unique Project identification code or number to such approved project and all implementing Entities of the Presidency and Public Services Institutions and shall incorporate such unique project specific identification code or number in all such projects and applications for release and payment of project funding relating to the unique Project identification code or number.

Core Systems
13(1) For the purposes of ensuring effective interoperability operations, promotion of effective digital security across entities of the Presidency and Public Services Institutions, NITA shall from time to time define, designate or select systems that are core to Government business, operations and or functions. NITA shall make these definitions, designations, or selections as part of its standards definition functions (process.) and its use or application will be mandatory.

(2) The President and Public Services Institutions core systems where so defined shall comply with such guidelines, standards and security features specified by NITA.

(2) Where any entity of the Presidency and/or Public Services Institution core designs are inconsistent with the NITA core system design specified under the guidelines, standards and security features, they shall submit details of the levels and extent of deviations of their

existing core system designs and provide in detail their transitional migration plan to the core system design for consideration and evaluation by NITA.

(3) Entities of the Presidency and Public Services Institutions shall comply with and implement the evaluation of NITA of such MDAs or MMDAs transitional migration plan.

(4) No Entity of the Presidency and/or Public Services Institution shall after the commencement of this instrument negotiate for or implement any aspect of any technology which is inconsistent with the NITA provided guidelines, standards and security features specified by NITA.

(6) Subject to issues related to national security and national interest NITA shall publish such guidelines, standards and security features impacting on core system in the Gazette for compliance by entities of the Presidency and Public Services Institutions and no procurement shall be approved by nor contract negotiated by any entities of the Presidency and Public Services Institutions inconsistent with such guideline, standards and security features.

(7) Guidelines, standards and security features, which promote and protect national security, cyber security and national interest shall be communicated directly by NITA to the relevant agency through the Minister to such entities of the Presidency and Public Services Institutions and the Chief Information Officer shall comply with such communicated guidelines, standards and security features and provide such classified reports to NITA in respect of audits required under this legislation.

Enterprise Solutions and License Agreements

15(1) NITA shall in consultation with the Minister, be responsible for the negotiation of and entry into agreement with third party organisations for Government wide Enterprise Solutions and license agreements which shall be compatible with core systems and shall not compromise the use and proper functions of the network and its security, and all Entities of the Presidency and Public Services Institutions shall ensure compliance with and use of the Enterprise Solutions and License Agreements as applicable to the discharge of their functions.

(2) Where such Enterprise Solutions and licensing agreements exist, all Entities of the Presidency and Public Services Institutions shall use such negotiated License Agreement in accordance with the terms and conditions.

(3) All Entities of the Presidency and Public Services Institutions shall provide NITA with details of their Enterprise Solutions and license costs,, related agreements and particulars of their renewal, termination or existing conditions of breach by any party in such Enterprise Solutions and License agreements contracted for my such Entities of the Presidency and Public Services Institutions.

(4) All Entities of the Presidency and Public Services Institutions shall provide NITA with details of any contemplated negotiations and on-going negotiations between such Entities of the Presidency and Public Services Institutions relating to Enterprise Solutions and License Agreements and shall not proceed further in such negotiations without approval from NITA and Entities of the Presidency and Public Services Institutions shall comply with the directions so given by NITA.

(5) Any complaint by any Entity of the Presidency and Public Services Institution on any NITA Enterprise Solution and License Agreement directive shall be made to the Minister who shall be required to convene a meeting with the relevant Minister or person responsible for such Entity of the Presidency and/or Public Services Institution and NITA to discuss the NITA directive.

(6) The Minister shall be responsible for taking the final decision on the complaint relating to the NITA directive and the Minister shall report to the final decision to the Office of the President within a period not exceeding 14 days after the decision is taken and the President shall within a period not exceeding 28 days confirm, modify or overrule the decision of the Minister and the decision of the President shall be final.

BANDWIDTH MANAGEMENT

NITA shall be responsible for the management of bandwidth for MDAs and the Arms of Government to ensure that standards relating to quality of service parameters are adhered to by all MDAs and Arms of Government and consistency in user experience

NITA shall be responsible for:

1. the processing of bandwidth challenges reported by Chief Information Officers and for the identification and monitoring of bandwidth redundancies along the value chain of all entities of the Presidency and Public Services Institutions in a manner relevant and necessary for overcoming the bandwidth challenges
2. providing bandwidth allocation of entities of the Presidency and Public Services Institutions to ensure that standards relating to quality of service parameters are adhered to by all entities of the Presidency and Public Services Institutions and consistency in user experience

NITA shall be responsible for the security of the networks of entities of the Presidency and Public Services Institutions and each entities of the Presidency and Public Services Institutions shall provide NITA with details of its Network Architecture, Disaster Management & Data Recovery Policy, Cyber Security Internal Procedures, Digital Forensic and intrusion detection procedures and monitoring and its policy on legacy data and archiving policy and compilation and the security procedures applicable thereto.

The Minster shall be responsible for giving directives for compliance with entities of the Presidency and Public Service Institutions Chief Information Officers on issues relating to Bandwidth Management relevant for the effective discharge of the functions of NITA under these Regulations.

REGISTER OF CRITICAL DATABASE

Holding of Register for Critical Database

8(1) NITA shall be responsible for holding and monitoring of the Register of Critical Databases and the Presidency and Public Services Institutions shall furnish the Agency with half yearly reports detailing the status of such critical databases inclusive of security breaches, password breach, protection against security and unlawful access and access control violations, interoperability challenges between entities of the Presidency and Public Services Institutions and relevant data sharing bodies and entities under their direct or indirect control or use.

(2) NITA shall be responsible for holding and monitoring of the Register of Protected Computers and the Presidency and Public Services Institutions shall furnish the Agency with half yearly reports detailing the status of such Protected Computers inclusive of security breaches, password breach, protection against security and unlawful access and access control violations, interoperability challenges between entities of the Presidency and Public Service Institutions and relevant data sharing bodies and entities under their direct or indirect control or use.

(3) NITA shall be responsible for holding and monitoring of the Register of Protected systems and the Presidency and Public Services Institutions shall furnish the Agency with half yearly reports detailing the status of such protected systems inclusive of security breaches, password breach, protection against security and unlawful access and access control violations, interoperability challenges between entities of the Presidency and/or Public Services Institution and relevant data sharing bodies and entities under their direct or indirect control or use.

Private entities whose systems, networks, computers contain critical databases shall register with NITA and shall furnish the Agency with half yearly reports detailing :

a) the status of such systems, networks, computers containing critical databases,
b) any security breaches,
c) any password breach,
d) any access breaches
e) existing policy for protection against security and unlawful access
f) details of access control consistent with critical database protection
g) access control internal violations,
h) interoperability challenges between private entities and relevant data sharing bodies and
i) particulars and purpose of any Third Party data sharing and/or accessing bodies and entities of such system, network, computers and critical databases.

Critical Databases

The contents specified in sub regulation (2) shall without limitation constitute part of the procedures for publication in the Gazette of computer, computer systems and computer networks holding information or through which critical database are held, transmitted, encrypted or assessed as critical database.

(2) The following without limitation shall constitute part critical databases and all persons holding such databases shall register with NITA .

(a) Databases which hold information of any Regulatory Bodies established under the laws of Ghana
(b) Databases which contain any information relating to the Government of Ghana financial accounts, business and activities whether classified as confidential or not
(c) Databases containing information of national security issues
(d) Databases of the Parliamentary service
(e) Databases of the Judiciary service
(f) Databases containing information which may be classified, sensitive public information relating to national interest, public health and safety, public

morality and of national importance in the reasonable estimation of the Minister.

(g) Databases of the National Health Insurance Authority, Ghana Health Service and the Registrar of Birth and Deaths
(h) Database of the Drivers Vehicles Licensing Authority
(i) Database of Ghana Revenue Authority
(j) Database of the Bank of Ghana
(k) Databases containing details of data subject processing exempted from the provisions of the Data Protection Act, 2012, Act 843
(l) Databases of the Ghana Police Service, Ghana Immigration Services, National Security and Intelligence gathering Institutions
(m) Databases of the Electoral Commission
(n) Databases of the National Identification Authority
(o) Computers of Ministries, Departments and Agencies and MMDAs
(p) Computers related to the operations of designated Critical infrastructures.

The Minister shall pursuant to the provisions of ETA have the right to add to such critical database by publication in the Gazette.

PROTECTED COMPUTERS AND SYSTEMS

Protected System

10(1) The following systems, network, information specified subject matter, processing target content, recording keeping data and equipment shall without limitation constitute protected systems.

(2) Any system of electronic input, information generation, access, storage, analysis report generation which contains, processes and/or stores or contains any information relating to:

(a) critical databases,
(b) National Security,
(c) Public Health and Safety,
(d) Crime Prevention and Monitoring,
(e) Administration of Justice,
(f) Public transportation Transport network and design
(g) Telecommunications network and design
(h) Operations, Banking and Financial transactions of Financial Regulators and companies and legal entities under Regulations
(i) Operations, transactions of Insurance Regulators and companies and legal entities under Regulations
(j) Operations, transactions of Security Industry Regulators and companies and legal entities under Regulations
(k) Computer of Ministries, Departments and Agencies
(l) movement of motorized and propelled objects on roads, inland waterbodies, rivers, lakes and Ghanaian territorial airspace and seas, exclusive economic zone. minerals vested in the State under the provisions of the 1992 Constitution.

The Minister shall pursuant to the provisions of ETA have the right to add to the class of protected systems by publication in the Gazette.

Reporting Regime for Protected Systems
6(1) The Presidency and Public Services Institutions shall provide half yearly report to NITA on compliance with all Gazette notifications required to be issued in respect of protected systems under the Electronic Transactions Act, 2008, Act 772..

Protected Computer
Without limitation, the following equipment and/or devices use for purposes connected in any manner with content of the sub section of this regulation shall constitute protected computers.

(2) Any equipment and/or device howsoever designed or referred to, used for, capable of and/or previously used for electronic input, information generation, access, storage, analysis, report generation by the undermentioned institutions, agencies, entities shall constitute protected computers:
    (a) National Security,
    (b) Public Health and Safety
    (c) Crime Prevention and Monitoring,
    (d) Administration of Justice,
    (e) Public transportation Transport network and design
    (f) Telecommunications networks and design operation
    (g) Institutions under Regulatory bodies providing any form of services in the Financial, Insurance, Pension and Securities sectors
    (h) Statutory Regulators
    (i) Entities of the Presidency
    (j) Entities holding, providing, regulating and monitoring any information relating to movement of motorised and propelled objects in Ghanaian territorial land, airspace and waters
    (k) Entities holding, providing, regulating and monitoring any information relating to minerals vested in the State under the provisions of the 1992 Constitution.

The Minister shall pursuant to the provisions of ETA have the right to add to such protected computer by publication in the Gazette.

Reporting Regime for Protected Computers
4(1) Entities of the Presidency and all Public Services Institutions shall provide half yearly reports to NITA on compliance with all Gazette notifications required to be issued in respect of protected computers under the Electronic Transactions Act, 2008, Act 772.

Protected Network
Without limitation, the following technology based design use for purposes connected in any manner with content of the sub section of this regulation shall constitute protected networks.

(3) , any technology based design howsoever constituted or composed of, which together with the combination of any devices, equipment, infrastructure, transmits, retains, stores or provides any passage for any electronic record, data whether in part, in

association with or sole by the undermentioned institutions, agencies, entities shall constitute protected network:

(a) National Security,
(b) Public Health and Safety
(c) Crime Prevention and Monitoring agencies,
(l) Administration of Justice,
(d) Public transportation Transport network and design
(e) Telecommunications networks and design operation
(f) Institutions under Regulatory bodies providing any form of services in the Financial, Insurance, Pension and Securities sectors
(g) Statutory Regulators
(h) Entities of the Presidency
(i) Entities holding, providing, regulating and monitoring any information relating to movement of motorised and propelled objects in Ghanaian territorial land, airspace and waters
(j) Entities holding, providing, regulating and monitoring any information relating to minerals vested in the State under the provisions of the 1992 Constitution

The Minister shall pursuant to the provisions of ETA have the right to add to such protected Network by publication in the Gazette.

Reporting Regime for Protected Networks

4(1) Entities of the Presidency and all Public Services Institutions shall provide half yearly reports to NITA on compliance with all Gazette notifications required to be issued in respect of protected Networks under the Electronic Transactions Act, 2008, Act 772..

CRITICAL INFRASTRUCTURE

Critical Infrastructure is any computer, computer system, computer network and/or protected system used directly in connection with or for any of the undermentioned purposes:

(a) the security, defence or international relations of the country;
(b) the existence or identity of a confidential source of information related to the enforcement of criminal law;
(c) the provision of services directly related to communications infrastructure, banking and financial services, public utilities, public transportation or public key infrastructure;
(d) the protection of public safety and public health, including systems related to essential emergency services;
(e) foreign commerce or communication affecting a citizen of Ghana or business in which a citizen of Ghana or the Government has an interest; or
(f) the legislative, executive or judicial service, the public services and security agencies.

All critical infrastructure holder and operators shall comply with the provisions of these Regulations regardless of ownership of the infrastructure

All critical infrastructure whether declared as protected computers, protected systems, protected networks by the Minister shall comply with the provision of these Regulations.

NITA shall provide regulatory oversight over all critical infrastructures and provide directives, security standards and reporting regimes relating without limitations to the following :

(a) securing critical infrastructure against threats;
(b) ensuring that information pertaining to security measures applicable to critical infrastructure remains confidential and in accordance with law;
(c) ensuring that objective criteria are developed for the identification, declaration and protection of critical infrastructure;
(d) ensuring public-private cooperation in the identification and protection of critical infrastructure;
(e) securing critical infrastructure in a manner which fosters public safety, public confidence in the use of technology in the rendering of services to persons relying on such critical infrastructure:
    (i) through the implementation of measures aimed at securing critical infrastructures; and
    (ii) by mitigating risks to critical infrastructures through assessment of vulnerabilities and the implementation of appropriate measures;
(f) promoting cooperation and a culture of shared responsibility between various role-players in order to provide for an appropriate multi-disciplinary approach to deal with critical infrastructure protection;
(g) enhancing the collective capacity of persons who are responsible for the protection of critical infrastructure to mitigate possible security risks;
(h) ensuring that every critical infrastructure holder and/or operator complies with regulatory measures aimed at securing such critical infrastructure against threats;
(i) providing for the powers and duties of persons in control of critical infrastructure; and
(j) supporting integration and coordination of the functions of various persons involved in the securing of critical infrastructure.

REGISTER OF CRITICAL INFRASTRUCTURE

NITA shall keep a register of critical infrastructure declared as protected computers, protected systems, protected networks declared by the Minister and publish same in the Gazette

REGISTRATION OF CRITICAL INFRASTRUCTURE

All persons and entities whose computers, systems, networks and infrastructure constitute critical databases under these regulations shall within a period of not exceeding six months after the coming into force of these Regulations, register with NITA as critical infrastructure holders and/or operator

All critical infrastructure holders and/or operator shall meet the security standards and protocols set out by NITA in the Directives issued under these Regulations

All registered Critical Infrastructure holders and/or operators other than protected computers, protected systems and protected networks declared by the Minister shall notify NITA of any security breaches which occur to their network, protected computers, protected system within a period not exceeding twenty-four (24) hours discovery of such breach and shall report daily to NITA:

1. on the status of the success in overcoming the breach, indicating
2. the steps taken and the basis for the conclusion that the breach has been neutralised
3. details of the damage, risks and digital forensics relating to the breach and tracing of the persons responsible for the breach

All registered holders of protected computers, protected systems and protected networks declared by the Minister shall notify NITA and CERT of any security breaches which occur to their network, protected computers, protected system within a period not exceeding six (6) hours discovery of such breach and shall report daily to NITA:

1. on the status of the success in overcoming the breach, indicating
2. the steps taken and the basis for the conclusion that the breach has been neutralised
3. details of the damage, risks and digital forensics relating to the breach and tracing of the persons responsible for the breach

Property Holding Critical Infrastructure

Every property within which any critical infrastructure is located shall be kept secured at all times using modern, reliable and efficient surveillance equipment which shall be combined with corresponding access control devices and security protocols necessary for the safety and protection of such critical infrastructure at all times.

Duty on Operators of Critical Infrastructure

Every operator of critical infrastructure shall ensure that provision is made for, and monitoring conducted on all matters relating to

(a) physical security of critical infrastructure;
(b) personnel security at critical infrastructure;
(c) contingency plans applicable to critical infrastructure; and
(d) measures aimed at protecting critical infrastructure;

All operators of Critical Infrastructure shall ensure that all cyber security standards and protocols of NITA issued in respect of critical infrastructure are complied with and shall ensure that security standards are consistent with international best practices at all times

A person shall be presumed to be in control of a critical infrastructure where such person or entity

(a) owns any part of a critical infrastructure or is an employee, agent, representative or authorised pursuant to any contract or howsoever described given lawful access to such critical infrastructure;
(b) by the operation of law, occupies, possesses, is in control of, or is responsible for the operation or administration of such a critical infrastructure

Breach of Security relating to Critical Infrastructure

A breach in security shall include all unauthorised access, intrusions, data breaches, compromise to ability of infrastructure to mitigate, absorb or withstand any damage, disruption, disturbance or interference in order to maintain the functionality, integrity and structural capacity of that infrastructure

Applications relating to Persons relating to Critical Infrastructure
NITA shall consider an application from a person in control of an infrastructure for recommendation to the Minister of infrastructure as critical infrastructure within the meaning of these regulations.

NITA General Policy Implementing Powers
NITA shall in furtherance of its objects under the Electronic Transactions Act, xxx Act, xxx to implement the ICT policy

(a) conduct or facilitate any physical security assessment of critical infrastructure or potential critical infrastructure;
(b) make recommendations to the Minister on the declaration and risk categorisation of such critical infrastructure or potential critical infrastructure;
(c) evaluate, monitor and review the application and operational effectiveness of policy, guidelines or legislation related to the protection of critical infrastructure and submit same to the Minister,
(d) evaluate and review physical security assessments, resilience reports and any designation as critical infrastructure, and advise the Minister accordingly;
(e) consider any draft of a prescribed security policy or plan for consideration by the Minister

Petition for classification as a Critical Infrastructure
NITA shall consider any application from any entity in control of an infrastructure for the classification of such infrastructure as part of the national critical infrastructure.
NITA determines that such application has merit, NITA shall make a recommendation to the Minister for the classification of such infrastructure as a critical infrastructure and publication of same in the Gazette

Inspection of Critical Infrastructure
NITA shall upon the issue of a security inspection notice of not less than 24 hours to the operator or owner of any critical infrastructure at any reasonable time, conduct an inspection at a critical infrastructure to—

(a) verify whether the person in control of that critical infrastructure has taken satisfactory steps to secure any critical infrastructure under their control;
(b) verify any information relating to the declaration as critical infrastructure as well as the physical security assessment report provided or requested
(c) review the physical security assessment and evaluating the status of the physical security of the critical infrastructure;
(d) verify compliance with these regulations and
(e) compile a report for CERT and the Minister

(2) An inspector shall—

(a) preserve, or aid in preserving, confidentiality with regard to all matters concerning the operational activities of the critical infrastructure that may come to his or her knowledge in the performance of his or her duties and shall not communicate any such matter to any person except NITA, or unless a court of law orders such communication, or insofar as such communication is necessary to properly carry out the inspection;
(b) carry out his or her duties and exercise his or her powers—
(i) subject to any prescribed procedure;

(ii) in accordance with any directives issued by the Minister;
(iii) in a manner that does not hamper or endanger the operational activities of the critical infrastructure where an inspection is being conducted; and
(iv) with strict regard to decency and order.

(3) Any person in control of a critical infrastructure who fails or refuses to allow an inspector access to the critical infrastructure commits an offence and shall upon summary trial and conviction be liable to a fine of xxx penalty points or to a term of imprisonment not exceeding xxxx months or to both.

(4) If an inspector has reasonable grounds to believe that any method or practice of safeguarding or securing the critical infrastructure in question or any failure or refusal to comply with these regulations, may negatively affect the physical security measures of that critical infrastructure, the inspector may, by written notice in the prescribed form order the person in control of that critical infrastructure to take, within a period specified in the notice, such steps in respect of the security of the critical infrastructure as may be specified in the notice.

Where any person fails to comply with the written notice in the prescribed form, NITA may apply to the court upon serving the party with notice of the application for an order compelling the person in control of critical infrastructure—

(i) to comply with any provision of legislation, directives, gazette publication
(ii) to comply with any NITA issued notice or take all other reasonable steps necessary to secure the critical infrastructure;
(iii) to cease any method or practice causing or capable of causing any compromise to such critical infrastructure; and/or
(iv) any other order the court considers appropriate.

Critical Infrastructure Standards, Guidelines and Protocols

Critical Infrastructure guidelines, standards, protocols and related matters for protected computers, protected networks, protected systems and critical infrastructure defined under these Regulations of entities declared by the Minister shall be published in the Gazette

Critical Infrastructure guidelines, standards, protocols and related matters for protected computers, protected networks, protected systems and critical infrastructure defined under these Regulations of entities providing notification of equipment being critical infrastructure within the definition of these regulations and not being entities declared by the Minister shall be published in the Gazette

Prohibited Persons in managing Critical Infrastructure

(7) No person shall be appointed by any entity to manage, protect and ensure protection of any critical infrastructure designated by the Minister as a critical infrastructure under these regulations where such person:

i. Has been convicted of any offence relating to dishonesty within 10 years preceding the date of notification under these regulations
ii. Has been convicted of any technology related offence under any legislation in Ghana or similar legislation in any jurisdiction
iii. does not have a valid security clearance issued by the National Security pursuant to an investigation concerning the security risks or otherwise assessed by the National Security pursuant to National Security classified

criteria which shall be final, binding and in respect of which such person shall have no right of appeal or request for review

iv. Does not have a medical report confirming fitness to perform such services on account that there are no mental conditions affecting such person and confirms that there is no element of mental incapacitation affecting such person or condition affecting the person for which plea of insanity may be considered as a defence in the prosecution of any offence under these regulations and any other legislation relating to technology

v. Is disqualified under any law from holding the position of director in Ghana under any provisions of the Companies Act, 2019, Act 992

No person shall have access to any critical infrastructure unless such person satisfies the security protocols set out in the Gazette publication.

Critical Infrastructure and Restricted Access

All premises where critical infrastructure is laid, traverse, or are held constitutes restricted premises and no person shall be given access to such premises, without lawful authority, the proof which shall rest upon such person.

Any person seeking to enter restricted premises or access laid critical infrastructure shall where required produce proof of his or her appointment and identity to the satisfaction of the person in control of the critical infrastructure or an appointed security manager.

Audit of Critical Infrastructure

NITA shall provide an annual audit report to the Minister on the state of the critical infrastructure during any year of review on the undermentioned:

i. Particulars of security breaches in the year under review
ii. Particulars of actions taken in respect of security breaches and the outcome of such action
iii. Particulars of assessment of the cause, issues which could have prevented such security breaches,
iv. recommendations made in respect of :
    a) such causes and their prevention,
    b) monitoring,
    c) digital forensic generation,
    d) cross border cooperation,
v. infrastructure damage arising from such security breaches,
vi. data protection violations or potential breaches arising from such breaches,
vii. notifications given to the Data Protection Commissioner in respect of such breaches,
viii. technology related damage not being infrastructure in nature or impact arising from such security breaches,
ix. steps taken in the reversal of such damage and status of step and project outcome of such steps,
x. classification of damage whether
    a) permanent,
    b) temporal,
    c) incapable of fully classified,

xi. classification of remedial action as being completely restored, partially restored, incapable of restoration at the time of the report,
xii. recommendations to the Minister on the evaluation, monitoring and reviewing of the implementation of policy, protocols, standards and legislation related critical infrastructures under these regulations in respect of which directives are relevant and applicable

i. protection of critical infrastructure;
ii. any other matters require by the Minister in any directive given pursuant to these regulations,

Critical Infrastructure Mandatory Information
The entity holding critical infrastructure shall submit details of aspect of such critical infrastructure and provide information of aspects of the infrastructure within the classification definition of

i. a low-risk,
ii. medium-risk or
iii. high-risk category,

and any other classification issued by the Minister additional to these inclusive of classifications which constitute classified information under any legislation for which public disclosure shall not be made.

Petition for declaration of Critical Infrastructure Status
Any entity and/or person shall have a right to petition the Minister for the declaration of any computer, computer systems, computer networks, technology infrastructure as critical infrastructure under these regulations and the Minister shall within a period not exceeding 60 days make a decision on the petition.

Directives shall include such conditions as may be prescribed regarding any steps and measures the person in control of the critical infrastructure must implement to safeguard the critical infrastructure in question.

Where the Minister declares any infrastructure as a critical infrastructure under these regulations or protected computer, protected network, protected systems under the Electronic Transactions Act, the Minster shall by written notification inform such entity of the declaration and upon such notification the entity shall comply with these regulations.

The notification shall provide information to the entity of the undermentioned:

(a) the declaration of the infrastructure as a critical infrastructure;
(b) the risk category of such declaration;
(c) the obligations and conditions relating to such notification are being the subject matter of issued directives, the onus of content awareness and compliance which shall fall on the recipient of such notification
(c) the obligations and conditions relating to such notification are being the subject matter of Gazette publication, the onus of content awareness and compliance which shall fall on the recipient of such notification
(d) the period within which the person in control of that critical infrastructure must ensure full compliance and certification of compliance issued by NITA.

The Minister shall determine as aspects in respect of publications required in the Gazette which constitute classified information for which public disclosure is not in the national

security interest and same disclosed to the entity for compliance and entity shall ensure that no person is given access to such national security classified disclosure except in compliance with protocols given by the Minister.

Certificate of declaration as critical infrastructure
Where an infrastructure is declared a critical infrastructure, the Minister shall issue a certificate of declaration, in the prescribed form and manner, to the person in control of that critical infrastructure, setting out—

(a) the risk categorisation as determined by the Minister;
(b) the premises or complex where the critical infrastructure is located;
(c) the conditions which the Minister may deem necessary to impose for purposes of securing the critical infrastructure;

Certificate of Critical Infrastructure
The Minister shall issue a certificate for each of the premises on which any such critical infrastructure, forming part of a complex, is located after prior assessment of the premises by NITA and the determination by NITA that such premises meet the criteria of hosting critical infrastructure. .

The certificate for the premises where critical infrastructure is located shall be issued in the name of the entity in control of that critical infrastructure and state the location for which the validity of the Certificate holds.

Every critical infrastructure holder and/operator shall notify NITA of any changes to the premises holding such critical infrastructure whether such changes arise by alteration, modification or relocation of critical infrastructure to another premise.

The declaration of a critical infrastructure shall not exempt a person or entity in control of critical infrastructure from having to comply with the provisions of any other law applicable to the critical infrastructure in question.

Publication and Entry Particulars
NITA shall enter the particulars of any declaration as critical infrastructure or the termination of such declaration, into the prescribed register, which except for classified content shall be accessible to the public in the prescribed manner or form.

The Minister shall, by notice in the Gazette, except in respect of classified information, publish such particulars as may be prescribed regarding infrastructure which has been declared as critical infrastructure and when such declaration is terminated.

Amendment or variation of information or conditions by Minister
Every holder of critical infrastructure shall notify the Minister and NITA of any change in the circumstances of any critical infrastructure and shall comply with such directives issued by the Minister in respect of such notification and all NITA related standards, publications, notifications and relevant matters.

The Minister may in respect of notification of change in circumstances of any critical infrastructure:

(a) amend the risk categorisation or

(b) vary any or all of the information or conditions on a certificate of declaration as critical infrastructure

(c) revocation of the status of critical infrastructure or any component of such critical infrastructure

And the entity shall be provided within a period not exceeding 21 days of the response of the Minister with respect to such notification of change in circumstances of any critical infrastructure.

The entity receiving such notification shall be entitled to petition the Minister for a review of the classification or conditions in a manner consistent with the provisions of these regulations and national security interest and the Minister shall not be required to make any classified disclosures in response to such petition.

The decision of the Minister to the Petition shall be final without prejudice to the right of such entity to petition the President for a reconsideration of the Minister's decision

Termination and revocation of declaration

The Minister shall have power to terminate or reverse the declaration of any critical infrastructure or component thereof

(a) where the person in control of a critical infrastructure ceases the activities which formed the basis upon which the Minister declared the infrastructure as a critical infrastructure; or

(b) any critical infrastructure or component thereof is retired from use and does not form a part or used in respect of any purpose for which critical infrastructure declarations relates.

Notification of changes in critical infrastructure

Any person in control of a critical infrastructure must notify the NITA and the Minister in writing within 30 days of any change—

(a) with regard to any information that was submitted in respect of the application for declaration as a critical infrastructure;

(b) in the control or ownership of the critical infrastructure; or

(c) that impacts on the ability of the critical infrastructure or the person in control of a critical infrastructure to comply with all or any of the obligations under these regulations

NITA shall, in respect of such notification and after study make recommendation to the Minister as to:

(a) revocation of the declaration as critical infrastructure

(b) the infrastructure in question having been declared as critical infrastructure on the

(c) basis of incorrect or false information provided by the entity; or

(d) breaches and/or failures by the entity in control of the critical infrastructure fails to comply with any—

(i) condition of declaration; or

(ii) of the provisions of these regulations, directives issued by the Minister, Gazette publication and any other matters affecting the critical infrastructure .

DUTIES OF PERSONS IN CONTROL OF CRITICAL INFRASTRUCTURE

Powers and duties of person in control of critical infrastructure

An entity in control of a critical infrastructure shall take such steps as may be prescribed to secure such critical infrastructure at that entity's expense.

Any person in control of critical infrastructure that is under the control of a Government department or any other organ of state, must take steps to ensure that such critical infrastructure is protected by the employees of that government department or organ of state. The Chief Information Officers of every MDA and Arm of Government shall be responsible for ensuring compliance with the provisions of these regulations and related legislations affecting critical infrastructure.

In the event that an entity in control of a critical infrastructure fails to take the steps to protect such critical infrastructure, the Minister shall take or cause steps to be taken in respect of the security of that critical infrastructure and the State must recover the reasonable cost levied by the NITA from the entity in control of that critical infrastructure during each monthly period that the entity fails to protect such critical infrastructure.

An entity in control of a critical infrastructure shall appoint a person in its employment to the protection, security and management of the critical infrastructure with responsibility amongst others to:

(a) implement and monitor, on behalf of the entity in control of the critical infrastructure, the prescribed security policy and plan compiled for that critical infrastructure;
(b) authorise access to critical infrastructure or oversee the authorisation of such access by security personnel working under his or her direction;
(c) liaise with any security service provider appointed by the entity in control of that critical infrastructure;
(d) implement the directives, Gazette publication and all other related matters as they impact on the critical infrastructure;
(e) provide monthly reports to the entity in control of that critical infrastructure on all matters relevant to these regulations and laws relating to critical infrastructure
(f) perform such other functions related to the securing of that critical infrastructure as may be assigned to him or her by the entity in control of that critical infrastructure:

No person shall be appointed by such entity with responsibility for the protection, security and management of critical infrastructure unless such person has been cleared by the National Security as a person who qualifies under the levels required of persons who access classified matters of state

Access to critical infrastructure

Every entity in control of a critical infrastructure shall—

(a) take such lawful steps as necessary, for the securing of a critical infrastructure and the contents thereof, as well as for the protection of the persons present at the critical infrastructure;
(b) issue a notification in the prescribed form that the critical infrastructure may only be entered upon in accordance with the provisions of these regulations and that persons or vehicles may be searched upon entering or leaving the premises and
(c) ensure that a notification is placed at the entrance to that critical infrastructure.

No person may, without the permission of the security manager, or the security personnel under the direction of the security manager enter into or upon any critical infrastructure affected by any provision in these regulations

For the purpose of granting permission, the security manager or the security personnel under the direction of the security manager, shall not permit entry of unauthorised persons unto the premises unless such persons shall provide the following documents for inspection and verification and entry is made of the records provided:

(i) address and any other relevant information required by the authorised person;
(ii) produce proof of identity;
(iii) inspection for mandatory storage at the security post of any security prohibited device in his or her possession or under his or her control whether remotely or otherwise;
(iv) inspection at the post of the contents of any vehicle, suitcase, bag, handbag, folder, envelope, parcel or container of any nature, in their possession, custody or control;
(v) examination by an electronic or other apparatus, in order to determine the presence of any security prohibited or technology related device; and
(vi) particulars of the person doing the entry, storage and inspection
(vii) particular of returned items the subject matter of mandatory storage.

Where the security manager or the security personnel under the direction of the security manager grants permission to a person enter the person may enter subject to conditions regarding—

(a) the carrying or displaying of proof that the necessary permission has been granted;
(b) restrictions relating to persons with whom he or she may come into contact in or on the critical infrastructure;
(c) restriction of access to certain parts of the critical infrastructure;
(d) the duration of his or her presence on or in the critical infrastructure;
(e) being escorted while he or she is on or in the critical infrastructure; and
(f) other requirements as the security manager or the security personnel may consider necessary.

REMOVAL OF PERSONS FROM CRITICAL INFRASTRUCTURE
The security manager may, at any time, remove any person from any critical infrastructure if—

(a) that person enters the critical infrastructure, or any part of the critical infrastructure concerned, without the required permission
(b) that person refuses or fails to observe a condition relating to the permissions granted for entry or
(c) it is necessary for the securing of the critical infrastructure concerned or the contents thereof or for the protection of the people therein or thereon.

The person in control of a critical infrastructure shall ensure that persons and vehicles leaving that critical infrastructure have been searched in a manner consistent with respect for the right to privacy and dignity and best practices relating to security checks with classified areas.

The person in control of a critical infrastructure must indicate in a notice, in the prescribed form and manner, at every entry point of a critical infrastructure that the critical infrastructure may only be entered upon in accordance with the conditions determined by the security manager which shall be consistent with these regulations.

Reporting Regime for Critical Database
5(1) The Presidency and Public Services Institutions shall provide half yearly report to NITA on compliance with all Gazette notifications required to be issued in respect of critical databases under the Electronic Transactions Act, 2008, Act 772..

Offences
Any persons who without lawful excuse the proof which shall lie on him who accesses any critical infrastructure contrary to the provisions of these regulations commits an offence and shall upon summary trial and conviction be liable to a fine of xxxx penalty points or an imprisonment not exceeding xxxx years or both

Digital Innovation Fund for Underserved & Marginalised Communities

NITA shall collaborate with and provide technical support to GIFEC in all matters relating to the passage of required legislation for the establishment and operation of the Digital Innovation Fund for Underserved & Marginalised Communities under every prevailing ICT Policy, Strategy and Action Plan

NITA shall facilitate efforts of Industry Fora related bodies in all matters relating to the passage of required legislation for the establishment and operation of the Digital Innovation Fund for Underserved & Marginalised Communities under the Digital Policy, Strategy and Action Plan

INTER-REGULATORY COOPERATION

NITA shall collaborate with Regulatory Authorities in finding solutions, development of technical standards, development of New Generation technology Regulatory practices, standards, license applications, prudential requirements adopted to application of technology to products of non-traditional industry players in the Local VAS sector competing with existing industry players regardless of such services and products being capable of single or multiple Regulatory areas services delivery.

NITA shall be the facilitator of meetings between recognised Industry Fora groups under the ETA and ECA seeking solutions, development of

(a) technical standards,
(b) New Generation technology Regulatory practices, standards, license applications, prudential requirements
(c) Local VAS registered and/or certified challenges with Regulatory entities in the Financial, Insurance, Securities, Pension, Aviation, Shipping & Logistics and Utilities services
(d) Local VAS sector challenges arising from unfair practices, monopolistic and uncompetitive behaviour of existing industry players regardless of such services and products
(e) Local VAS sector challenges arising from product single or multiple Regulatory areas services scope.

.

NON INFRASTRUCTURE BASED VALUE ADDED SERVICES –

eGOVERNMENT UNIVERSAL ACCESS

Digital Education Laboratories

NITA shall collaborate with and provide technical support to GIFEC in all matters relating to the setting up of Digital Educational Laboratories in educational Institutions and Underserved & Marginalised Communities under any prevailing National ICT Policy, Strategy and Action Plan

NITA shall facilitate efforts of Industry Fora related bodies in all matters relating to the setting up of Digital Educational Laboratories in educational Institutions and Underserved & Marginalised Communities under any prevailing National ICT Policy, Strategy and Action Plan.

Bandwidth and Spectrum Continuing Rationalisation

NITA shall collaborate with the NCA in finding solutions to spectrum related needs and challenges of Local VAS entities registered, certified and/or which have provided notifications approved by NITA engaged in activities, product and service delivery outside the regulatory scope of the NCA.

NITA shall facilitate efforts of Industry Fora related bodies in all matters relating to finding solutions to spectrum related needs and challenges of Local VAS entities registered, certified and/or which have provided notifications approved by NITA engaged in activities, product and service delivery outside the regulatory scope of the NCA.

NITA shall be the convenor of meetings between recognised Industry Fora groups under the ETA and ECA seeking implementation of the policy initiative of in all matters relating to finding solutions to spectrum related needs and challenges of Local VAS entities registered, certified and/or which have provided notifications approved by NITA engaged in activities, product and service delivery outside the regulatory scope of the NCA.

eGOVERNMENT SERVICE LEVELS STANDARD

NITA shall provide the minimum quality of services which every technology product and/or solution within the entities of the Presidency and the Public Services Institution shall be required to meet.

The eGovernment service levels shall be published in the Gazette and shall include without limitations the undermentioned areas:

a) Terms and conditions of use
b) Data Protection Policy
c) Technical support for users
d) Digital signature access and use
e) QR code access and use
f) Disability friendly access and use
g) Multiple local languages translations
h) Quality of Service parameters

Offences and penalties

21(1) A person who,

(a) engages in any conduct or activity with knowledge that such action has the reasonable effect of preventing any of the Divisions of NITA from functioning properly

(b) engages in any conduct or activity with knowledge that such action has the reasonable effect of preventing any of the Divisions of NITA from discharging its mandate;

commits an offence and is liable upon summary trial and conviction to a fine of not less than two hundred and fifty penalty units and not more than five hundred penalty units or to a term of imprisonment of not less than twenty-four months and not more than thirty-six months or to both.

(2) A person who without due authority or lawful excuse, the proof of which shall be on the person,

(a) fails to comply with the provisions of this legislation

(b) makes, alters, imitates or imports or assists in making, altering, imitating any publication of the Agency;

(c) approves any consultancy services the subject matter of any ICT based Request for Proposals or Expression of Interest whose specifications fail to comply with the standards, designs and protocols determined by NITA to be used by MDAs; or

(d) participates in any procurement process which fails to have the statutorily prescribed input of NITA in the process as defined by this legislation,

commits an offence and is liable upon summary trial and conviction to a fine of not less than five hundred penalty units and to a fine of not more than one thousand penalty units and/or to a term of imprisonment of not less than twenty-four months and not more than thirty-six months or to both.

(3) A person who

(a) hinders or obstructs an inspector from performing a function or discharging a duty under this legislation; or

(b) impersonates an inspector;

commits an offence and is liable upon summary trial and conviction to a fine of not less than fifty penalty units and not more than two hundred and fifty penalty units or to a term of imprisonment of not less than three months and not more than twenty-four months or to both.

.

Forms.
The forms in the Schedule to Part One of these Regulations are prescribed for use under Part One of these Regulations.
Fees.
(1) The fees in the Schedule to Part One of these Regulations are prescribed for the purposes of Part One of these Regulations.

(2) The fees shall be paid to the Agency by such means and in such manner as the Agency may direct

Interpretation

23. In this Regulations the following have the following meanings:

"Agency" means the National Information Technology Agency established under section 1(1) of the National Information Technology Agency, 2008, Act 771

"Computer" has the same meaning as defined by section 144 of the Electronic Transactions Act, 2008, Act 772.

"Critical database" shall have the same definition as under section 144 of the Electronic Communications Act, 2008, Act 772

"

"Entity and/or Entities of the Presidency" shall have the same definition, scope and meaning to the entities, persons and administrative composition and Presidential Staffers of the President exercising the Powers vested in the President under the provisions of the 1992 Constitution of the Republic of Ghana

MDA's means Ministries, Departments and Agencies which form part of the civil and public services together with all District, Municipal, Metropolitan and Regional Assemblies.

"Protected Computer" means any computer, computer system, computer network declared by the Minister under section 55(1) of the Electronic Transactions Act, 2008,Act 772 to be a protected computer.

"Protected System" means any computer, computer system, computer network declared by the Minister under section 55(1) of the Electronic Transactions Act, 2008,Act 772 to be a protected system.

Public Services Institutions shall have the same Institutional inclusions, definition, scope and meaning as are intended under Article 190 of the 1992 Constitution of the Republic of Ghana.

The President shall have the same definition, scope and meaning as are intended under Articles 57 of the 1992 Constitution of the Republic of Ghana

PART TWO CERTIFYING AGENCIES REGIME

Type of licence.
(1) There shall be two licenses in respect of any service provided under these regulations, namely an establishment license and an operational licence.
(2) The establishment licence shall be for duration of five years which gives the entity the registration right to carry out such business activity set out in the part of these regulations.

(3) The Operational licence shall be for two years and unless renewed shall expire.

(4) An application for an operational licence shall be made before the period of expiration of the establishment license.
(5) An application for an Establishment licence and Operational License shall be accompanied by:

(a) the prescribed fee and
(b) a declaration by the directors that there are no circumstances which would affect the liquidity or effective compliance by the entity of any provisions of this law and
(c) that the directors shall bring any future such occurrences to the attention of the Agency any such occurrences.

(6) The appropriate licence shall be issued upon receipt of payment.

(7) No previously licensed entity shall be entitled to operate during any period for which its license has expired, and no application has been submitted for renewal.

(8) Any person who provides any services under these regulations without a license commits an offence and shall upon summary trial and conviction be liable to a term of imprisonment not exceeding two years or a fine not exceeding ……penalty units or both.

Renewal of licence.
(1) An establishment license shall be renewed once every five years and no application for the renewal of an operation license shall be made whilst the Establishment License has expired.

Information required for establishment licence.
An application for an establishment licence shall contain the following information:

(a) the particulars of the applicant;
(b) the business plan;
(c) details of the qualifications of the personnel intended to be employed;

(d) the proposed operating procedure inclusive of repository of advanced electronic signatures schemes; and
(e) the various services to be provided and applicable fees..

Information required for an operational licence.
An application for the operational licence shall contain -

(*a*) all information submitted for the establishment licence;

(*b*) all additional information and any changes to the information submitted for the establishment licence, if any;

(*c*) suitable guarantee; and

(*d*) a report from a qualified compliance auditor certifying that the prescribed licensing, standards and technical requirements have been satisfied.

(e) particulars of the compliance auditors and a copy of contract of engagement between the applicant and the compliance auditor.

(g) Audited accounts the periods for the date of incorporation to the year immediately preceding the application provided that the account shall not extend beyond five (5) years preceding the date of application.

Application for licence.

(2) An application under sub regulation (1) shall be accompanied by -

(a) the information required in the statutory forms, as applicable;

(b) the prescribed fee; and

(c) such other information or document as the Agency may require.

(3) The Agency may, on an application for an operational licence, require the applicant to demonstrate any part of its operating procedure and may require independent testing of the software, hardware, technical components, algorithms, standards and other pertinent parameters and other equipment to be used by the applicant, at the applicant's expense, for the purpose of ascertaining its security and trustworthiness.

The Agency may on application for an establishment license require the applicant to provide documentary evidence of

a) The personnel in full employment with the requisite skills and technical knowledge to provide services under this part of the regulations for which the application is brought,
b) copies of each agreement between the applicant and such third parties providing technical support or to be relied upon in the discharge of services the subject matter for which operational license would be applied
c) such other documents which the forms may prescribe.

(4) If any information or document required under these regulations is not provided by the applicant or any demonstration or test required is not complied with within the time specified in the

requirement or any extension thereof granted by the Agency, the application shall be deemed to be withdrawn and shall not be further proceeded with, without prejudice to a fresh application being made by the applicant.

Withdrawal of application for Operational licence

(1) An application for an operational licence shall be deemed to be withdrawn and shall not be further proceeded with except by fresh application of an establishment licence by the applicant, if -

(*a*) the applicant fails to provide all particulars required for an operational licence before the expiration of the establishment licence; or

(*b*) an application for the operational licence is rejected.

Initial application for Operational licence

Nothing in these Regulations shall be construed so as to require an applicant to apply for the establishment licence as a condition for applying for the operational licence where the applicant is able to satisfy the prescribed requirements to apply for the operational licence and demonstrates that it satisfied all the conditions for an establishment licence.

Suitable guarantee.

(1) A suitable guarantee shall satisfy the following requirements:

(*a*) it is in a form acceptable to the Agency;

(b) it is in an amount specified in approved operational license;

(c) it states that it is issued for the purposes of the Act and these Regulations; and

(d) it specifies a term of effectiveness extending at least as long as the term of the licence to be issued to the provider.

Application for recognition of Foreign Authentication Service Provider

The statutory Form prescribed in these regulations shall be used in an application for recognition by a Foreign Authentication Service Provider.

Foreign Authentication Service Providers shall be entitled to apply for the establishment license and the Operational license at the same time and unless both are approved by NITA, such Foreign Authentication Service Provider shall not be recognised to provide authentication services under these Regulations.

No application for Foreign Authentication Service Providers shall be approved where any persons named in the document provided in support of the Establishment Licenses and/or Operational License are determined by National Security to be

a) persons who pose a security risk to the national interest,
b) persons who have been convicted of fraud or dishonesty in the 10 years preceding the application
c) any shareholder controlling more than twenty (20) percentage of voting rights of such applying entity is a person determined to pose a security risk to the national interest

Unless the Foreign Authentication Service Provider is able to demonstrate that such persons have been removed from the applicant and would not be employed by the applicant during the period where the National Security assessment and determination remains unchanged

Implied conditions.

Every licence granted under these regulations shall contain the following minimum conditions that the holder of the licence shall: -

(a) keep and maintain working capital reasonably sufficient to carry on or operate as a authentication service provider;

(*b*) keep its operating procedures under review and shall not make any substantial changes to its operating procedures without the Agency's prior written approval;

(*c*) only use the approved advanced electronic signature scheme submitted for approval to the Agency;

(*d*) make, keep and maintain the necessary arrangements with a recognised repository and a recognised date/time stamp service for its own use and for the use of its subscribers if it does not also provide those services;

(*e*) establish and maintain a secure system and infrastructure to safeguard where applicable its private key and for key distribution, key management, key storage and key disposal;

(*f*) establish and maintain a secure system and data base for the storage of information and documents obtained from a subscriber under the Act and these Regulations;

(*g*) maintain at all times the confidentiality of information and documents obtained from a subscriber under the Act and these Regulations and be subject to the directions of the subscriber in relation to the release or disclosure of such information and documents or to such relevant and applicable provisions of law and/or a Court of competent jurisdiction requiring disclosure;

(*h*) keep and maintain the suitable and valid guarantees during the period of the license and such periods under the Limitation Decree NRCD 54 and other applicable legislation

(*i*) provide to its customers and/or subscriber at least one hundred and eighty days written notice of such intention to discontinue its operations and lodge a copy of each notification electronically to NITA

(*j*) keep and maintain detailed written records of its transactions as required under these Regulations;

(*k*) keep and maintain books of account as required under these Regulations; and

(*l*) comply with any directions of the Agency issued under the Act and these Regulations.

(m) file annually audited accounts with the Agency

(n) file annually compliance audit reports.

Replacement of licence.

(1) The Statutory Forms provided in these regulations shall be used in an application for a replacement licence where the provider furnishes evidence of the loss or destruction of an original licence to the satisfaction of the Agency.

(2) If the Agency is satisfied as to the reasons for the loss or destruction of the licence, the Agency shall issue a replacement licence with the words "DUPLICATE" endorsed on the licence.

(3) An application for a replacement license shall be accompanied by a statutory declaration to the effect that the licence issued to the provider is lost, destroyed or mutilated or by a statement specifying the reasons for the application, as the case may be and in the case of the loss of the licence, an additional police report addressed to the Agency and released to the licensed authentication service provider of the loss and the stage of investigation or otherwise by the police.

(4) A provider shall surrender to the Agency the discovery of a lost original licence or recovery of any part of the destroyed licence.

Amendment of licence on request.
(1) A licensed authentication service provider may where applicable and consistent with the Electronic Transaction Act and these regulations apply to the Agency to amend -

(*a*) the particulars of a licence; or

(*b*) the conditions attached to a licence.

(2) An application under sub regulation (1) shall be made with the requisite statutory form and shall be submitted to the Agency and supported by all relevant evidence.

(3) If the Agency approves the amendment, the Agency shall amend the licence accordingly and allow the licence to continue to have effect, as amended, until its original expiry date.

Power to amend, etc. conditions of licence.
(1) Subject to the provisions of this regulations the Agency may, during the currency of a licence, amend, vary, add to, revoke, suspend or revive any condition attached to the licence or attach new conditions arising from new technology developments inclusive without limitation of security threats, and shall notify the licensed authentication service provider in writing accordingly.

(2) The Agency shall, before taking any action under sub regulation (1), take into consideration -

(*a*) the estimated cost to be incurred by the licensed authentication service provider to comply with the varied or new conditions; and
(*b*) the nature and size of the business being carried out in the business premises.
(c) the period required for reasonable compliance with any variation, addition, or amendment of any condition of a licence.

(3) Before the Agency amends, varies, adds to or attaches any condition to a licence under sub regulation (1), the licensed authentication service provider shall be given a hearing and the purpose for the amendment, variation, additional conditions explained to the applicant.

(4) No variation, addition or amendment shall have retroactive effect or require retroactive compliance.

Transfer or assignment of licence.
(1) A licence from the Agency shall not be transferable.

(2) A licensed entity may upon application for approval by the Agency make provision for the transfer of its contractual obligations to its customers to another licensed entity.

(3) An application under sub regulation (2) shall be accompanied by the prescribed fee and provide all documents in support of its application for the transfer of the customers and evidence of the transferee ability to comply with the provision of the regulation.

(4) If the licensed entity -

(*a*) in the case of a company, is wound up; or

(*b*) in the case of a partnership, is dissolved,

the Agency may, on application in writing, and subject to such conditions as the Agency deems fit consent to the transfer of customers to licensed third parties with similar objects upon terms that the Agency may deem fit

(5) No entity appointed under this license shall be liable upon summary trial and conviction for any cause of action existing against the wound-up company or dissolved partnership.

Partnerships in licence.

(1) If any change occurs in the partnership, the remaining partners or any of them shall, within one month of such change, notify the Agency in writing.

(2) If the Agency is satisfied that the partnership has not been dissolved and, in the case of an addition of a partner to the partnership, that the new partner is a fit and proper person, the Agency shall amend the licence accordingly and allow the licence to continue to have effect, as amended, until its expiry.

(3) Every partner shall be deemed to be jointly and severally liable for the acts and omissions of the other partners unless the partner proves to the satisfaction of the court that -

(*a*) the act or omission was committed without that partner's knowledge, consent or connivance; and

(*b*) the partner took all reasonable precautions and had exercised due diligence to prevent the act or omission.

Register of Licence.

(1) The Agency shall keep and maintain a physical and electronic Register of Licences in such form as it thinks fit.

(2) Any person upon the payment of the prescribed fee may inspect the Register of Licences and make copies of or take extracts from the Register.

(3) The Agency shall publish a list of licensed entities under these regulations in such form and manner as it may determine.

Authentication Service Provider

No person shall carry on or operate, or hold himself out as carrying on or operating, as a licensed authentication service provider (hereafter referred to as a provider) unless that person has been issued with an operational licence.

Qualification requirements.

(1) A person intending to carry on or operate as a provider shall satisfy the following requirements:

(a) it is an incorporated body;

(b) it maintains a registered office in Ghana;

(c) it has working capital reasonably sufficient to enable it to carry on or operate as a authentication service provider;

(d) it files with the Agency a suitable guarantee;

(e) it uses a trustworthy and reliable system for the generation and management of encryption, decryption, identification, authentication, verification, data tampering and certificates for advanced electronic signatures issued to subscribers;

(f) in the case of digital signatures, it uses an approved digital signature scheme for the generation of key pairs and for the creation and verification of digital signatures;

(g) In the case of advanced electronic signature, it scheme of signature generation and use provides certainty of identification, time and place of use and incapable of generation by unauthorised persons other than the holder of such advanced electronic signature

(h) it has an operating procedure that includes a certification practice statement, the measures to be taken to check the identity of subscribers to be listed in certificates, and the repositories and date/time stamp services to be used;

(i) it employs as operative personnel only persons who -

(i) have not been convicted in any jurisdiction within the past ten years of an offence involving fraud, dishonesty or false representations; and

(ii) have demonstrated knowledge and proficiency in following the requirements of the Act and these Regulations;

(iii) would comply with the licensing, standards and technical requirements under these Regulations and any additions and amendment thereto;

(j) would comply with such other requirements as the Agency may deem fit.

Obligations of Providers.

(1) A provider shall maintain a website or digital portal services which shall contain the following matters on its home page:

(a) Particulars of all licences, renewals, expirations notification received from the Agency

(b) Particulars of all notifications of sanctions and breaches received from the Agency and the outcome of such notifications.

(*c*) a statement indicating the location of the provider's certification practice statement, the method or procedure by which it may be retrieved, its form and structure, its authorship and its date;

(*d*) the date and result of the last compliance audit filed by the Provider;

(*e*) the repository used by the provider;

(*f*) the procedure of independent verification of any licensed Provider

(g) the particulars of Providers whose certificates has been revoked or is suspended and the date and time of such revocation or suspension;

(*h*) any event that substantially affects the provider's ability to conduct its business or the validity of a certificate published in the repository provided by the Agency or in a recognised repository; and

(*j*) any other particulars relating to the provider prescribed by the Agency.

(2) The officers or director of any provider which operates without a licence commits an offence and shall upon summary trial and conviction liable to a term of imprisonment for a period not exceeding ten years or to pay a fine of …penalty units, or both.

Contents of Provider disclosure record.

(1) The Agency shall maintain a disclosure record of a provider which shall contain the following particulars and may be available on payment of prescribed fees.

(*a*) the business name and registered address of the Provider;
(*b*) the landline, mobile numbers and help desk facilities of the Provider,;
(*c*) the electronic mail, social media handles or other acceptable formats by which the Provider may be contacted electronically,;
(*d*) the brand name if any;
(*e*) the licence number, the date and time of the issue, and the date and time of the expiry, of the licence issued to the Provider;
(*f*) any restrictions imposed on the licence issued to the Provider, if any;
(*g*) if the revocation of a licence which has taken effect, the fact of the revocation and its effective date;
(*h*) if a licence has been surrendered, the fact of the surrender and its effective date;
(*i*) if the Provider has given any intention of not renewing or surrendering its licence, a statement to that effect;
(*j*) the current public key or keys of the provider by which its digital signatures on published certificates may be verified;
(*k*) the procedure for verification of any advanced electronic signatures
(*l*) the amount of the Provider's suitable guarantee;
(*m*) the total amount of all claims filed with the Agency for payment from the suitable guarantee filed by the provider;
(*n*) a brief description of any limit known to the Agency and applicable to the provider's liability or legal capacity to pay damages in tort or for breach of a duty under the Act or these Regulations;

(2) The Provider shall furnish the Agency with any particulars required to be published in the provider disclosure record.

(3) A person who contravenes sub regulation (2) commits an offence and shall upon summary trial and conviction be liable to a fine not exceeding ……..penalty points or to imprisonment for a term not exceeding one year or to both.

DIGITAL & ELECTRONIC SIGNATURES

Approved digital signature or advanced electronic scheme to be used.

(1) A digital signature scheme shall be approved by the Agency if it is to be used for the purpose of generating a key pair, or creating, using or verifying a digital signature under the Act.
(2) An advanced electronic signature scheme shall be approved by the Agency if it is to be used for generating, creating, using or verifying advance electronic signatures under the Act.

Approved digital signature scheme.
(1) A digital signature scheme shall be approved for the purposes of the Act and these Regulations if -

(*a*) the digital signature scheme uses a secure public-key algorithm for the generation of the key pair and a secure public-key algorithm and hash function for the creation of the digital signature;
(*b*) the digital signature scheme satisfies the technical component requirements under this regulation; and
(*c*) the digital signature created is not capable of being modified to enable unauthorised access.

(2) A key pair used to create and verify a digital signature shall not be used to encrypt and decrypt any messages.

Storage of private keys.
(1) The data storage medium for the private key may be hardware based or software based.

(3) There shall be a backup storage of a private key with an escrow to be stored in a secure place and in a secure manner.

(3) If the data storage medium of the private key is hardware based, the holder of the private key shall ensure that the token, smart card or other external device in which the private key is stored is kept in a secure place and in a secure manner.

(4) If the data storage medium of the private key is software based, the holder of the private key shall ensure that the computer system in which the private key is stored is reasonably secure.

(5) The personal identification numbers or other data used for the identification of the rightful holder of the private key in conjunction with the data storage medium for the private key shall be kept secret.

Key length.
A Provider and a subscriber shall ensure that the key length of its key pair is adequately secure for its purposes and consistent with international practise and conventions.

Prohibition against duplication of private key.
(1) No person, except the rightful holder of the private key, shall make or cause to be made any copy of a private key.

(2) A person who contravenes sub regulation (1) commits an offence and shall upon summary trial and conviction be liable to imprisonment for a term not exceeding five years or to a fine not exceeding ……..penalty units or to both.

Disposal of key pairs.
(1) If a key pair is no longer in use or to be used, or if the private key of the key pair is compromised, the holder shall take steps to have it disabled and shall notify the provider.

(2) Notwithstanding sub regulation (1), if the holder desires to retain a key pair that is no longer in use or to be used, or that has been compromised, the holder shall ensure that the key

pair is stored by a reasonably secure method and the holder shall remain fully liable to third parties who bonafide and in good faith rely on any document in respect of which the key pair is used.

(3) A Provider shall keep a register of all keys disabled and shall confirm the destruction of such keys upon any third party bonafide inquiry.

(4) A subscriber shall where it generated the key pair notify the provider of any key destruction.

(5) No unauthorised person shall use any disabled key for any purposes and any unauthorised person who uses any such keys commits an offence and shall upon summary trial and conviction be liable to imprisonment for a term not exceeding five years or a fine not exceeding …….penalty points or both.

Key generation.

(1) A subscriber's key pair may be generated by -

(*a*) the subscriber; or

(*b*) the provider for the subscriber on a written request by the subscriber and on payment of the approved fee.

(2) If the subscriber generates the key pair, the provider shall reasonably ascertain whether the subscriber has used the prescribed technical components for the generation of the key pair and for the storage of the key pair.

(3) If the provider generates a key pair for the subscriber, the provider shall ensure that -

(*a*) it uses a secure protocol that incorporates adequate safeguards and security features for the distribution or transmission of the private key to the subscriber; and

(*b*) no copy of the subscriber's private key is retained or otherwise kept by the licensed authentication service provider.

(4) A provider that contravenes sub regulation (3) commits an offence and shall upon summary trial and conviction be liable to a fine not exceeding …….penalty point or to imprisonment for a term not exceeding five years or to both.

CERTIFICATION PRACTICE STATEMENTS

Certification practice statement.

(1) A provider shall issue or make available to a subscriber before or at the time the subscriber applies for a certificate from the provider a copy of its certification practice statement.

(2) A certification practice statement shall contain all the particulars required under these regulations

(3) Nothing in sub regulation (2) shall prevent the provider from adopting a more comprehensive certification practice statement provided it is not inconsistent with the Act and these Regulations.

(4) The certification practice statement shall be in such form as the Agency may determine.

OBLIGATIONS OF CERTIFICATION PROVIDERS

Duty of instruction.

(1) A Provider shall inform an applicant for a certificate concerning -

(*a*) the measures necessary to contribute to secure advanced electronic signatures and their reliable verification;

(*b*) relevant technical details required to be fulfilled under this regulation ;

(*c*) the attribution of digital signatures created with the subscriber's private key and

(d) with information relating to advanced electronic signatures which may need to be re-signed before the security value of such signatures decreases with time.

(3) In relations to digital signatures where data are re-signed the new digital signature shall include the earlier digital signature or signatures and shall bear a time-stamp.

APPLICATIONS AND CERTIFICATES

Application for certificate.

(1) An application for a certificate shall be made in writing to the Provider and shall contain the following particulars:

(*a*) the name and address of the subscriber;

(*b*) the landline, mobile numbers and help desk facilities of the Provider,;

(*c*) the electronic mail, social media handles or other acceptable formats by which the Provider may be contacted electronically,;

(*d*) the brand name whether registered or unregistered of the subscriber where applicable;

(*e*) any pseudonym to be used to preserve the anonymity of the subscriber;

(*f*) the public key corresponding to the subscriber's private key, if the subscriber generates his own key pair;

(g) particulars required from the subscriber where the advanced electronic signature scheme approved by the provider requires information different from or additional to those required under this subsection.

(h) a statement of the period for which the certificate is required;

(i) a statement of any limitations on the authority of the subscriber who is to be the signer;

(*j*) the recommended reliance limit required for the certificate; and

(*k*) particulars of the method or repository by which notice of revocation or suspension of the certificate is to be given or verification made.

(2) An application under sub regulation (1) shall be accompanied by -

(*a*) the approved fee; and

(*b*) such other information or document as the provider may require.

(3) The provider may, at its discretion, refuse to allow a subscriber to use a pseudonym.

Issue of certificate.

(1) If a provider is satisfied after it has taken reasonably steps to verify the identity of the subscriber, the provider may issue a certificate to the subscriber, with or without conditions.

(2) A certificate issued by a provider under sub regulation (1) shall include the following particulars:

(*a*) a statement that the type of the certificate is in accordance with this regulation;
(*b*) the provider's licence number, the date and time of the issue, and the date and time of the expiry, of such licence;
(*c*) the serial number of the certificate, that must be unique among the certificates issued by the provider;
(*e*) the name by which the subscriber is generally known or the pseudonym to be used;
(*f*) the brand name of the subscriber whether registered or unregistered;
(*g*) the brand name of the provider issuing the certificate whether registered or unregistered;
(*h*) the public features relevant for disclosure for purpose of identification of an exclusive holder of an advanced electronic signature,;
(i) any relevant and applicable security features of the advanced electronic signature scheme relevant to trust of such certificate.
(j) the date and time on which the certificate is issued and accepted;
(*k*) the date and time on which the certificate expires;
(*l*) any limitations or qualifications in respect of the certificate;
(*m*) particulars inclusive of any brand name of the repository responsible for publication of notice of revocation or suspension of the certificate
(*n*) Particulars where applicable of the method by which notice of revocation or suspension of the certificate is to be given; and
(*o*) the website address and link where the provider's certification practice statement, the method or procedure by which it may be retrieved, its form and structure, its authorship and its date.

(3) A certificate issued by a provider under sub regulation (2) may, at the option of the subscriber and the provider, contain or incorporate by reference all or any of the following particulars:

(*a*) where a public key is the subject matter of the advanced electronic signature, one or more additional, secondary public keys;
(*b*) where a public key or security feature is the subject matter of the advanced electronic signature, identifiers or usage indicators related to public keys or necessarily required in respect of the security feature;
(*c*) references incorporating any applicable certification practice statements;
(*d*) any other available documents material to the certificate, the issuing provider or the accepting subscriber.

(4) The data in a certificate shall be in such form as the Agency may determine.

(5) A certificate shall be signed with an advance electronic signature by the issuing provider.

(6) The provider shall keep and maintain a Register of Certificates containing a list of the

certificates issued by it in such form as the Agency may determine.

(7) If the provider refuses a certificate under sub regulation (2), the provider shall immediately notify the applicant in writing and shall immediately refund the approved fee.

(8) The provider may classify the certificates issued by it according to designated levels of trust and may issue certificates accord to such classification.

Certificate of Revocation List.

(1) A provider shall keep and maintain a Certificate of Revocation List that shall contain a list of all certificates revoked by the provider together with the date and time of revocation.

(2) A Certificate Revocation List shall be signed with an advanced electronic signature by the provider.

(3) The provider shall publish the Certificate Revocation List in at least one recognised repository.

(4) The provider shall keep the Certificate Revocation List under constant review and shall enter all relevant information as soon as possible after it is received or determined but no later than the end of the business day on which it is received or determined.

(5) The provider shall publish an up-dated Certificate Revocation List at least once in every twenty-four hours on its website in addition to giving notice to the Agency.

REPOSITORY SERVICES

Qualification requirements for repository.

(1) A person intending to carry on or operate as a repository shall satisfy the following requirements:

(*a*) it is an incorporated body registered in Ghana

(*b*) it maintains a registered office in Ghana;

(*c*) it has working capital reasonably sufficient, according to the requirements of the Agency, to enable it to conduct business as a repository;

(*d*) it employs as operative personnel only persons who -

(i) have not been convicted within the past ten years of an offence involving fraud, dishonesty or false representation; and

(ii) have demonstrated knowledge and proficiency in following the requirements of the Act and these Regulations;

(*e*) the repository includes a data base that is capable of containing -

(i) authentication service provider disclosure records for licensed certification authorities;

(ii) certificates to be published in the repository;

(iii) notices of suspended or revoked certificates to be published by a licensed authentication service provider or any person suspending or revoking certificates;

(iv) notices of termination of suspension of certificates to be published by a licensed authentication service provider or any person suspending certificates;

(v) advisory statements, written defences thereto and decisions made by the Agency thereon to be published by the Agency under the Act and these Regulations; and
(vi) such other information as the Agency thinks fit;

(*f)* it operates by means of a trustworthy and reliable system;
(*g*) the repository contains no significant amount of information that the Agency finds is known or likely to be untrue, inaccurate or not reasonably reliable;
(*h*) the repository contains certificates published by ***certification authorities*** that are required to conform to rules of practice that are similar to or more stringent than the requirements of the Act and these Regulations;
(*i*) it keeps and maintains an archive of certificates that have been suspended or revoked, or that have expired, within at least the preceding ten years;
(*j*) it complies with the certification, standards and technical requirements under the Act and these Regulations;
(*k*) it complies with such other requirements as the Agency thinks fit.

Functions of a license repository.
(1) A licensed repository shall -
(*a*) maintain a publicly accessible data base for the purposes of publishing the information required to be published under the Act and these Regulations;
(*b*) publish the authentication service provider disclosure records for licensed certification authorities as the Agency may require;
(*c*) publish such advisory statements, written defences thereto and decisions by the Agency thereon and such other information as the Agency may require;
(*d*) publish such information as a licensed authentication service provider may require; and
(*e*) publish such other information as the recognised repository deems fit.

(2) A licensed repository shall publish all information received and requested to be published not later than one business day after receipt of the request and information.

(3) If for any reason the licensed repository is unable to comply with the time limit specified in sub regulation (2), the repository shall immediately upon receipt of the request and information notify the requester in writing of that fact.

(4) A person who contravenes sub regulation (3) commits an offence and shall upon summary trial and conviction be liable to a fine not exceeding ……penalty points.

Surrender of license.
(1) A recognised repository may surrender its license to the Agency provided that such surrender is accompanied with a written notice of its surrender.

(2) The surrender shall take effect on the date the Agency receives the license and the surrender notice or if a later date is specified in the notice, on that date.

(3) On receipt of a surrender notice the Agency shall immediately cause such surrender to be published in such form and manner as he may determine.

(4) A recognised repository intending to voluntarily surrender its license shall, not less than one hundred and eighty days before the date the surrender is intended to take effect, notify all its clients in writing of its intention.

(5) No recognised repository shall during such period conduct business with new clients

(6) A recognised repository that contravenes sub regulation (4) commits an offence and shall upon summary trial and conviction to imprisonment for a term not exceeding five month or a fine not exceeding …..penalty points or both.

(7) A recognised repository shall not voluntarily surrender its license unless it has taken steps to ensure that it has made arrangement satisfactory to its clients for:

(a)The transfer with the prior written consent of the Agency to another repository with an existing operational license or a repository which the Agency has consented of clients of the repository being terms which the Agency finds protects the interest of existing customers;

(b) the migration of all documents and items lodged with it in a manner which shall not disrupt the normal business operations of existing customers and

(c) the compliance auditor's report confirms the adequacy of such arrangements to the Agency.

Register of Recognised Repositories.

(1) The Agency shall keep and maintain a Register of Recognised Repositories in such form as it deems fit.

(2) Any person may inspect the Register of Recognised Repositories and make copies of or take extracts from the Register upon payment of the prescribed fees.

DATE TIME STAMP AUTHENTICATION SERVICES

Use of time-stamps.

A time-stamp by a recognised date and time stamp service shall be appended or attached to a message, advance electronic signature or other document if -

(*a*) a time-stamp is required under any written law; or

(*b*) a particular time may be significant with regard to the use of advanced electronically signed data.

Effect of time-stamp by recognised date and time stamp service.

(1) The date and time time-stamped on a document and advanced electronically signed by a recognised date/time stamp service shall, unless it is expressly provided otherwise, be deemed to be the date and time at which the document is signed or executed.

(2) The date and time time-stamped on a document and advanced electronically signed by a recognised date/time stamp service shall be admissible in evidence in all legal proceedings without prejudice to the weight or otherwise the Court may attach to the contents of the document.

Operational license for date and time stamp services.

(1) No person shall carry on, operate, or engage in any activity which constitutes date and time stamp services to any other person or entity unless that person has an establishment license and been issued with an operational licence.

(2) An application for a date and time stamp licence shall be deemed to be withdrawn and shall not be further proceeded with, without prejudice to a fresh application being made by the applicant, if -

(*a*) the applicant fails to apply for the operational licence before the expiry of the establishment licence; or

(*b*) on an application for the operational licence having duly been made within the period specified in these regulations the applicant is not issued with the operational licence.

Qualification requirements for license.

(1) A person intending to carry on or operate as a date and time stamp service provider shall satisfy the following requirements:

(*a*) it is an incorporated body under the laws of Ghana

(*b*) it maintains a registered office in Ghana;

(*c*) it has working capital reasonably sufficient, according to the requirements of the Agency, to enable it to conduct business as a date/time stamp service;

(*d*) it employs as operative personnel only persons who -

(i) have not been convicted within the past ten years of an offence involving fraud, dishonesty or false representation ; and

(ii) have demonstrated knowledge and proficiency in following the requirements of the Electronic Transactions Act and these Regulations;

(*e*) it operates by means of a reliable and trustworthy system;

(*f*) it uses a reasonably secure and tamper-proof mechanism as it's time-stamping device;

(*g*) it keeps and maintains an archive of documents that have been time-stamped, irrespective that the contents of the document itself are not disclosed, within at least the preceding ten years;

(*h*) it complies with the certification, standards and technical requirements under the Act and these Regulations;

(*i*) it complies with such other requirements as the Agency thinks fit.

Functions of recognised date/time stamp service.

(1) A recognised date/time stamp service provider shall -

(*a*) on receipt of a document for time-stamping, immediately time-stamp the date and time of its receipt on the document and digitally sign the time-stamp; and

(*b*) at the end of each business day cause to be published in at least one recognised repository all documents time-stamped by it in that day.

(2) For the purposes of paragraph (1) (*b*), only the hash result of the document shall be published.

(3) The date and time time-stamped on the document shall be the date and time at which the

document is received by the recognised date/time stamp service.

(4) If for any reason the recognised date/time stamp service provider is unable to comply with the time limit specified in sub regulation (1), the recognised date/ time stamp service shall immediately upon receipt of the document and the request for a time-stamp notify the requester in writing of that fact.

(5) A person who contravenes sub regulation (4) commits an offence and shall upon summary trial and conviction be liable to imprisonment for a term not exceeding five years or a fine not exceeding ……..penalty points or both.

Chargeable fees.
A recognised date/time stamp service provider may impose such fees and charges for its services as may be approved by the Agency.

Application for date/stamp service license.
An application by the date/time stamp service provider under these regulations shall be by application for a licence under these regulations.

Information required for operation license.
An application for the operation license shall contain -

(*a*) all valid information submitted for the establishment license;
(*b*) all new information and all the changes to the information submitted for the establishment license, if any; and
(*c*) a report from a qualified auditor certifying that the prescribed certification, standards and technical requirements have been satisfied.

Issue and renewal of licence.
(1) On receipt of an application for a license to provide date/time services, the Agency shall consider the application.

(2) If the Agency is satisfied as to the qualification and suitability of the date/time stamp service, the Agency may upon an application for an establishment licence issue an establishment licence in accordance with these regulations.

(3) If the Agency is satisfied as to the qualification and suitability of the date/time stamp service, the Agency may upon an application for an operational license issue an operational licence in accordance with these regulations.

(4) The Agency shall specify the duration of the licence and its serial number.

(5) If the Agency refuses to renew an operational licence on account of partial or non-compliance finding in the compliance audit the Agency shall immediately notify the applicant in writing of his refusal.

(6) An application for the renewal of a licence shall be made in Form 1.

(7) An application under this sub regulation shall be accompanied by -

(*a*) the prescribed fee; and
(*b*) a report from a qualified auditor certifying that the prescribed certification, standards and technical requirements have been satisfied.

Surrender of licence.
(1) A recognised date/time stamp service may surrender its licence to the Agency provided that such surrender is accompanied with a written notice of its surrender.

(2) The surrender shall take effect on the date the Agency receives the licence and the surrender notice or if a later date is specified in the notice, on that date.

(3) On receipt of a surrender notice the Agency shall immediately cause such surrender to be published in such form and manner as he may determine.

(4) A recognised date/time stamp service intending to voluntarily surrender its licence shall, not less than one hundred and eighty days before the date the surrender is intended to take effect, notify all its clients in writing of its intention.
(5) No recognised date/time stamp service shall during such period conduct business with new clients

(6) A recognised date/time stamp service that contravenes sub regulation (4) commits an offence and shall upon summary trial and conviction to imprisonment for a term not exceeding five month or a fine not exceeding …..penalty points or both.

(7) A recognised date/time stamp service shall not voluntarily surrender its licence unless it has taken steps to ensure that it has made arrangement satisfactory to its clients for:

(i)The transfer of clients would be made with the prior written consent of the Agency to another repository with an existing operational licence or a date/time stamp service which the Agency approves and has made a finding the nature of the transfer appears to provide satisfactory protection of the interest of existing customers;
(ii) the migration of all documents and items lodged with it in a manner which shall not disrupt the normal business operations of its clients and
(iii) the compliance auditor's report confirms the adequacy of such arrangements to the Agency.

Register of licensed Date/Time Stamp Services.
(1) The Agency shall keep and maintain a Register of Date/ Time Stamp Services and issued certificates of recognition in such form as the Agency deems fit.

(2) A person may inspect the Register of Recognised Date/Time Stamp Services and make copies of or take extracts from the Register upon payment of prescribed fees.

PROVISION RELATING TO COMPLIANCE AUDITS
Qualification and registration of compliance auditors.
(1) An auditor qualified with the Agency determined ISO information technology standards and the requirements of the Act and these Regulations shall be appointed by a licensed entity to prepare compliance audits under these regulations.

(2) A licensed entity prior to the commencement of a compliance audit shall notify the Agency of the particulars of its appointed compliance auditor. .

(3) A qualified auditor under these Regulations shall not operate as or in any way participate in the operation of or be concerned in a provider, a repository or a date/time stamp service in respect of which it conducts a compliance audit.

(4) The Agency shall keep and maintain a Register of Qualified Auditors in respect of which notification has been received.

(5) Any person may inspect the Register of Qualified Auditors and make copies of or take extracts from the Register at a fee to be determined by Agency.

Procedure for annual compliance audit.
(1) The licensed entity shall make available any information, document or personnel as may be required by the qualified auditor.

(2) Based on the information gathered in the audit, the qualified auditor shall categorise the provider's compliance as one of the following:

(*a*) full compliance, if the licensed entity appears to comply with all the requirements of the Act and these Regulations;
(*b*) substantial compliance, if the licensed entity appears generally to comply with the requirements of the Act and these Regulations but one or more instances of non-compliance or of inability to demonstrate compliance were found in the audited sample, that were likely to be inconsequential;
(*c*) partial compliance, if the licensed entity appears to comply with some of the requirements of the Act and these Regulations but was found not to have complied with or not to be able to demonstrate compliance with one or more important safeguards; or
(*d*) non-compliance, if the licensed entity complies with few or none of the requirements of the Act or these Regulations, or fails to keep adequate records to demonstrate compliance with more than a few requirements or) refuses to submit to an audit.

(3) A licensed entity shall submit itself for re-audit within a period of 14 days where there is a finding of partial or non-compliance by a compliance auditor.

Auditor's report.
(1) The qualified auditor shall within fourteen days from the completion of a compliance audit submit a written report to the Agency.

(2) The auditor's report shall contain -

(a) particulars of the audits qualifications to provide compliance audits
(*b*) the date of the audit;
(*c*) a list of the information or documents studied or of the personnel interviewed;
(*d*) the extent of compliance with the Act and these Regulations;
(*e*) the results of the audit;
(*f*) the categorisation of the provider; and

(*g*) such other information as the qualified auditor thinks fit.

Additional compliance audits.
The Agency may conduct unscheduled audits of a provider at any time.

Consequence of failing annual compliance audit.
(1) The Agency shall take into consideration the results of annual compliance audits when evaluating an application to renew a licence under these regulations.

(2) A finding of partial, or non-compliance may be a ground for:
(a) the refusal in an application for renewal of a license
(b) the revocation or suspension of a licence issued under these regulations.
(3) The Agency may impose sanctions on a licensed entity where such entity fails to comply with recommendations made by a compliance auditor in respect of findings of partial or non-compliance.

Criteria for recognition of foreign certification authorities.
(1) A foreign authentication service provider shall satisfy the following requirements to qualify for recognition by the Agency:
(*a*) it shall be licensed or otherwise authorised under the laws in the country of incorporation to carry on or operate as a authentication service provider or certification authority in that country;
(*b*) the certificate issued by the foreign authentication service provider demonstrates a level of security equal to or more stringent than the level of security of a certificate issued by a licensed authentication service provider in Ghana;
(*c*) it has registered as an external agency in Ghana in compliance with the provisions of the companies code;
(*d*) in respect of any business conducted in Ghana it shall comply with the standards and technical requirements under the Act and these Regulations; and
(*e*) it shall comply with such other requirements as the Agency thinks fit.

(2) In addition, a foreign authentication service provider shall also be eligible for recognition by the Agency if an international treaty; agreement or convention concerning the recognition of its certificates has been concluded to which the Government of Ghana is a party.

(3) Notwithstanding sub regulation (1), the Agency may, if the Agency thinks fit to do so, and with the approval of the Minister, grant recognition to a foreign authentication service provider where the country of its incorporation does not require a licence or other governmental authority to carry on authentication certification services but it otherwise satisfies all other requirements under these regulations.

FOREIGN AUTHENTICATION SERVICE PROVIDERS
Application documents for Foreign Authentication Service Provider
(1) An application for the recognition of a foreign authentication service provider shall be made to the Agency in writing.

(2) An application under sub regulation (1) shall be accompanied by -

(*a*) proof that the requirements under this regulation have been satisfied, including a report from a qualified auditor certifying that the prescribed standards and technical requirements have been satisfied;
(*b*) the prescribed fee; and
(*c*) such other information or document as the Agency may require.

Grant of recognition
(1) On receipt of an application from a foreign authentication service provider, the Agency shall consider the application.

(2) If the Agency is satisfied as to the qualification and suitability of the foreign authentication service provider, the Agency may recognise the foreign authentication service provider, with or without conditions, or may refuse the recognition.

(3) If the Agency refuses to recognise a foreign authentication service provider under sub regulation (2), the Agency shall immediately notify the applicant in writing of his refusal.

Revocation of recognition.
(1) The Agency may revoke the recognition granted under this regulation to a foreign authentication service provider: -

(*a*) if the Agency finds that the recognised foreign authentication service provider no longer satisfies the requirements specified under these regulations; or
(*b*) if the recognised foreign authentication service provider applies for a revocation of the recognition under this regulation.

(2) A revocation of recognition under sub regulation (1) shall be by order published in the *Gazette and the Agency shall publish all Gazette publication of the Agency on the Agency's website...*

(3) A revocation under paragraph (1) (*b*) shall be without prejudice to a fresh application for recognition being made by the foreign authentication service provider.

Application for revocation of recognition.
(1) A recognised foreign authentication service provider may apply to the Agency in writing for the revocation of its recognition.

(2) A recognised foreign authentication service provider intending to apply for the revocation of its recognition shall, not less than one hundred and eighty days before the date the application is made, notify all its clients in writing of its intention and shall provide on its website notice of its application to the Agency for the revocation of its recognition. Such foreign authentication service provider shall provide the Agency with a declaration at the time of application confirming full compliance with this provision.

(3) A recognised foreign authentication service provider that contravenes sub regulation (2) commits an offence and shall upon summary trial and conviction be liable to imprisonment for a term not exceeding one year or to an entity penalty not exceeding …….penalty points or both.

(4) A recognised foreign authentication service provider shall not voluntarily apply for revocation of its recognition unless it has taken steps to ensure that it has made arrangement satisfactory to its clients in Ghana for:

(a)The transfer with the prior written consent of the Agency to another repository with an existing license as an authentication service provider;
(b the migration of all documents and items lodged with it in a manner which shall not disrupt the normal business operations of its clients and
(c) the compliance auditor's report confirms the adequacy of such arrangements to the Agency.

Register of Recognised Foreign Certification Authorities.
(1) The Agency shall keep and maintain a Register of Recognised Foreign Certification Authorities in such form as he thinks fit. The Agency shall maintain an electronic copy of the Register on its website.

(2) A person may inspect the Register of Recognised Foreign Certification Authorities and make copies of or take extracts from the Register upon payment of the requisite fee.

(3) The Agency shall publish a list of recognised foreign certification authorities in such form and manner as he may determine and consistent with these regulations.

MULTIPLE SERVICES APPLICATION
Multiple services allowed.
Nothing in these Regulations shall be construed as requiring the operation as an authentication service provider or repository or date/time stamp service to be carried out by different persons if the person intending to operate as an authentication service provider, repository or date/time stamp service or any combination of such services is otherwise able to satisfy the requirements of the Act and these Regulations.

An application for multiple services if approved shall require that the applicant pay separate fees of each of the services approved by the Agency.

LICENSE ENTITIES DIGITAL RECORDS OBLIGATIONS
Record-keeping.
(1) A holder of an establishment license and operational license shall keep and maintain detailed written records documenting -

(*a*) the security measures taken to comply with the Act and these Regulations;
(*b*) if the provider generates a key pair or advance electronic signature creating procedures for a subscriber, the relevant time at which and the manner in which the private key or procedure is distributed or transmitted to the subscriber;
(*c*) the relevant time at which and the manner in which a certificate is issued and distributed or transmitted to the subscriber;
(*d*) the certificates issued by it in such a way that the data and its authenticity may be verified at any time; and
(*e*) all other measures taken to comply with the Act and these Regulations.

(2) The records required under sub regulation (1) shall include evidence demonstrating that the licensed authentication service provider has -

(*a*) confirmed the identification of the person named in a certificate that the Provider has issued;
(*b*) confirmed the identification of the person requesting revocation of each certificate that the Provider has revoked;
(*c*) confirmed all other facts listed as confirmed in a certificate that the Provider has issued; and
(*d*) complied with the Act and these Regulations in issuing, publishing, suspending and revoking a certificate.

(3) A holder of an establishment license and operational license shall require a subscriber or the agent of a subscriber to submit documentation and other evidence reasonably sufficient to enable the licensed authentication service provider to comply with this regulation.

(4) A recognised repository and a recognised date/time stamp service provider shall keep and maintain detailed written records documenting -
(*a*) the security measures; and
(*b*) all other measures,
taken to comply with the Act and these Regulations.

Books of account.
(1) A holder of an establishment license and operational license shall keep and maintain books of account in the manner determined by the Agency.

(2) Books of account shall be kept in the English language.

Retention and custody of records.
(1) A holder of an establishment license and operational license , shall, unless the Agency otherwise directs, retain -
(*a*) the records required under these regulations;
(*b*) the books of account required under these regulations; and
(*c*) all records of the issuance, acceptance and any suspension or revocation of any licence issued under these regulations
.
(2) All the records referred to in sub regulation (1) shall be retained in the custody of the provider generating the records unless the provider:
(*a*) contracts with another person for the record retention as required under this regulation and such contract is approved by the Agency; or
(*b*) surrenders the records to the Agency upon ceasing to act as a provider.

(3) A holder of an establishment license and operational license shall keep its records in a secure place and in a secure manner.

TECHNICAL COMPONENTS COMPLIANCE
Technical components.
(1) The technical components required for the purposes of the Act and these Regulations shall be the technical components specified in the Fourth and Fifth Schedule.

(2) The technical components referred to in sub regulation (1) shall be sufficiently examined under the state of the art and the fulfilment of the requirements shall be verified by the

Agency in writing.

(3) If the technical components are placed in circulation or legally manufactured in accordance with the requirements under the Act and these Regulations and which guarantee the same level of security, it may be assumed that the requirements referred to in sub regulation (1) regarding technical security are fulfilled.

(4) In individual cases and when there is a good reason, the Agency may require a demonstration that the requirements referred to in sub regulation (1) have been fulfilled.

(5) Any security-relevant changes in technical components shall be made apparent to the lawful user.

(6) The technical components used for the purposes of the Act and these Regulations shall be protected from unauthorised access and unauthorised modification.

(7) The Agency shall keep and maintain a catalogue of suitable security measures that shall be taken into account in the design of the technical components.

(8) For the purposes of these Regulations, the expressions "unauthorised access" and "unauthorised modification" shall have the meaning assigned to them under these Regulations

Review of software, etc.
(1) The Agency shall keep the suitability of software, hardware, technical components, algorithms, standards and other pertinent parameters relating to the generation of advanced electronic signatures, the hashing of the data to be digitally signed and the creation and verification of digital and/or advanced electronic signatures under review, and may periodically publish reports of the reviews.

(2) The period of suitability of the software, hardware, technical components, algorithms, standards and other pertinent parameters reviewed under these regulations shall be specified in the report.

(3) Suitability shall be considered present if throughout a specified period, being not less than six years after the time of assessment, any detectable forging of digital and/or advanced electronic signatures or manipulation of digitally and/or advanced electronically signed data can be ruled out with near certainty by means in accordance with current scientific and technological standards and taking relevant international standards into account.

(4) The reports referred to in sub regulation (1) may be made available to the public on payment of the prescribed fee.

(5) The Agency shall take into consideration the matters published in its reports in the granting of application for licence and renewals of licence under these regulations.

DATA PROCESSING ADDITIONAL OBLIGATIONS

Data protection.

(1) A holder of an establishment license and operational license of services under these regulations shall collect personal data only directly from the affected persons and only in so far as it is necessary for the purposes of the Act and these Regulations.

(2) Data from a third party may only be collected if the person affected gives that person's prior written consent or collection is consistent with the Data Protection legislation in force in Ghana at the time of such collection.

(3) Data collected under the Electronic Transactions Act and these Regulations shall only be used for the purposes of the Act and these Regulations unless -

(*a*) it is permitted by laws of Ghana or an order from the High Court to be used for other purposes; or

(*b*) the person affected has given that person's written consent for the data to be used for other purposes.

(4) If a subscriber uses a pseudonym with the approval of any licensed entity, such entity shall transmit data concerning the subscriber's true identity on the request of the proper authorities in so far as it is necessary to prosecute offences or to protect against threats to public safety or public order. No licensed entity shall register a subscriber solely upon a pseudonym and the licensed entity shall require particulars of subscriber’s true identity prior to processing any application.

(5) If information is transmitted under sub regulation (4), such information shall be documented by the relevant authority.

Liquidation and Assignment of Statutory Records:

(1) There shall be established a Data Trustee who shall receive statutory records required to be maintained by any entity under these regulations which is the subject matter of official liquidation where the Agency is not satisfied that sufficient provision has been made by the Directors of such company to ensure transfer of such records to third parties licensed under these regulations.

(2) The Data Trustee shall be a temporal custodian of such records pending the transfer of such records to such appropriate entities licensed under these regulations.

(3) The Data Trustee shall not be liable to any third party for any claim it may have against the licensed entity in liquidation.

ISSUE OF GUIDELINES, AUDITS, DIRECTIVES AND ORDERS

Directives and administrative orders.

(1) The Agency may issue directives and other administrative orders to providers and qualified auditors in relation to the implementation and enforcement of the Act and these Regulations as the Agency considers necessary.

(2) A person who contravenes a directive or order issued under shall be liable upon summary trial and conviction to pay an administrative fine not exceeding …….penalty points.

Guidelines.
(1) The Agency may issue guidelines to licensed certification authorities, subscribers, recognised repositories, recognised date/time stamp services and qualified auditors in respect of -

(*a*) what constitutes or satisfies the requirements for a trustworthy system;
(*b*) suitable security measures;
(*c*) the determination of recommended reliance limits;
(*d*) qualified auditors and audits required under the Act and these Regulations; and
(*e*) such other matters as the Agency thinks fit.

Forms.
The forms in the Schedule to Part Two of these Regulations are prescribed for use under Part Two of these Regulations.
Fees.
(1) The fees in the Schedule to Part Two of these Regulations are prescribed for the purposes of Part Two of these Regulations.

(2) The fees shall be paid to the Agency by such means and in such manner as the Agency may direct.

Interpretation.

In these Regulations, unless the context otherwise requires -
"advanced electronic signature" means an electronic signature -

(a) which is uniquely linked to the signatory,
(b) which is capable of identifying the signatory,
(c) which is created using means that the signatory can maintain under his sole control, and
(d) which is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable; and includes digital signatures which satisfy these criteria.

"qualified auditor" means a person qualified to provide a compliance audit in accordance with the provisions of these regulations.;

"certificate" means an electronic attestation which links signature-verification data to a person and confirms the identity of that person;
"certification-service-provider" means a person who issues certificates or provides other services related to electronic signatures;
“digital signature " means an advanced electronic signature which satisfies the criteria of regulation 29;

"brand name" means a set of data that identifies a legal or natural person in a computer-based context;

"electronic signature" means data in electronic form which are attached to or logically associated with other electronic data, and which serve as a method of authentication;

"hardware based" means in a token or smart card or other external device;

"hash function" means an algorithm mapping or translating one sequence of bits into another generally smaller set, known as the hash result, such that -

(a) a message yields the same hash result every time the algorithm is executed using the same message as input;

(b) it is computationally infeasible that a message can be derived or reconstituted from the hash result produced by the algorithm; and

(c) it is computationally infeasible that two messages can be found that produce the same hash result using the algorithm;

"hash result" means the output produced by a hash function upon processing a message;

"licensed" means to be issued with the operation stage of the licence;

“prescribed fee" means a fee or charge imposed under the provisions of this regulations;

"public-key algorithm" means an algorithm designed to create different signing and verification keys where the verification key can be made public and the signing key cannot in a reasonable amount of time be calculated from the verification key;

"qualified certificate" means a certificate which meets the requirements in Schedule ….. and is provided by a certification-service-provider who fulfils the requirements in Schedule ……;

"qualified auditor" means a qualified accountant or an accredited computer security professional registered as a qualified auditor under regulation 41;

"qualified right to payment" means an award of damages against a licensed certification authority by a court or adjudicating body having jurisdiction over the licensed certification authority in a civil or criminal action;

"signatory" means a person who holds a signature-creation device and acts either on his own behalf or on behalf of the person he represents;

"signature-creation data" means unique data (including, but not limited to, codes or private cryptographic keys) which are used by the signatory to create an advanced electronic signature;

"signature-creation device" means configured software or hardware used to implement the signature-creation data;

"signature-verification data" means data (including, but not limited to, codes or public cryptographic keys) which are used for the purpose of verifying an advanced electronic signature;

"signature-verification device" means configured software or hardware used to implement the signature-verification data;

"software based" means in the computer system or programmes;

"subliminal channel" means a channel within a digital signature that allows subliminal text to be sent within the digital signature;

"suitable guarantee" means a suitable guarantee under regulation 23.
“the Agency” means National Information Technology Agency performing the role of the Certifying Agency under the provisions of section 3(1) (a) of the Electronic Transactions Act, 2008, Act 772.
"voluntary accreditation" means any permission, setting out rights and obligations specific to the provision of certification services, to be granted upon request by the certification-service-provider concerned by the person charged with the elaboration of, and supervision of compliance with, such rights and obligations, where the certification-service-provider is not entitled to exercise the rights stemming from the …….

PART THREE: OPEN DATA AND THE STATE
Open Data
14(1) NITA shall be responsible for the monitoring of all entities of the Presidency and/or Public Services Institution implementation to ensure compliance with the Ghana Open Data policy and roll out.

(2) NITA shall be responsible for creating the open data policies and limitations on use of data of Entities of the Presidency and Public Services Institutions in respect of all data, which are classified as open data under the open data policy.

(3) NITA shall be responsible for providing regulatory oversight over compliance of each Entity of the Presidency and Public Services Institution implementation of the Government of Ghana open data policy and shall receive complaints and give compliance directive of the Chief Information Officer pursuant to determination made by NITA on open data related complaints received from complainants.

NITA and Public Records and Archives Administration Department
NITA shall provide technical support to the Public Records and Archives Administration Department as part of the Policy implementing statutory obligation of NITA

NITA shall be responsible for setting the technical scope and definition of matters which shall be Open Data content.

NITA shall be responsible for the development, design, provision of technical assistance and support, standards, security protocols, and maintenance of the Open Data network of the President and the Public Service Institution in respect of records and information classified under these Regulations as Open Data which meet the criteria for posting in electronic format shall be published.

PRAAD shall be responsible for Open Data content uploading in accordance with provisions of these Regulations.

NITA and PRAAD shall publish in the electronic Gazette the Government of Ghana Open Data which may constitute information for research, commercial and/or non-commercial use,

entrepreneurial digital product and services development, general information and other permitted uses under the laws of Ghana.

The electronic Gazette publication of the Government of Ghana Open Data Network shall provide details on:

(i) content directory of the Presidency and the Public Services Institutions.
(ii) Nature, Scope, Terms and conditions for permitted use and permitted reuse of Open Data information
(iii) Prohibited conducts and uses relating to Open Data information
(iv) Particulars of user information collected and retained by the Open Data network
(v) Procedure for notification of content inaccuracy
(vi) Criteria for Open Data records General Grouping into Historical, Contemporary, Legacy and Ancient.
(vii) Excluded Presidency and Public Services Institutions open data information not available or accessible on the Open Data network of the Government of Ghana
(viii) Categories of Network Open data clearly defining dynamic data, research data, high value commercial data, Local VAS entities by NITA Registered and NITA certified entities
(ix) The application procedures, approval and notification process and the general license to use types relating to request for reuse of Open Data of the PRAAD which shall have the sole responsibility for coordinating with the source provider of the document the subject matter for reuse
(x) Terms and condition for access, download and reuse of information shall incorporate principles of fairness, proportionate and non-discriminatory conditions for the re-use of such information and requirement for compliance with the DPA by users at all times

PRIVATE SECTOR OPEN DATA

NITA shall have Regulatory oversight responsibilities over entities managing and providing Open Data network content posting and management

All private sector Open Data network and/content providers shall notify NITA of their intention to provide Open Data network and/or content in respect of information relating to any category specified by such applicant and provide proof of meeting the criteria for the establishment of Open Data network and/or content upload set of in the electronic Gazette published by NITA.

No person or entity shall operate establish manage an Open Data network or upload content on Open Data network unless, they have received approval from NITA pursuant to their notification application that such person or entity has satisfied notification approval criteria set out in the electronic Gazette relating to Open Data Networks and/or content developers

The electronic Gazette publication relating to Private Sector Open Data Networks and/or content developers shall include without limitation matters which ensure that private sector Open Data Networks

(i) is registered with the DPA and provide proof of renewal of DPA certificate as a precondition to the annual notification renewal with NITA and the issue of a NITA Notification Certificate

(ii) Ensures content accuracy at the time of receipt for posting and procedure for archiving content which accuracy has been affected by circumstances after the initial posting
(iii) Adheres to provisions of the ETA
(iv) terms and condition for access, download and reuse of information incorporate principles of fairness, proportionate and non-discriminatory conditions for the re-use of such information and requirement for compliance with the DPA by users at all times
(v) adheres to all security standards and protocols provided as part of the notification procedure and such additional standards and protocols approved by NITA
(vi) adheres to all security standards and protocols required under the CSA
(vii) Include such additional matters which may be set out in Gazette Publications

PART FOUR: DIGITAL FORENSIC AND INTERCEPTION

General provision on interception

Unlawful and authorised interception

1. (1) A person shall not intentionally and without lawful authority intercept any communication in the course of its transmission by means of

(a) a public communication system;
(b) a communication system not owned by a person or;
(c) a private communication system.

(2) An interception of communication which is carried out at any place with the consent expressly or impliedly of a person who has the right to control the operation, or the use of a private communication system is actionable at the instance of the sender, recipient, or intended recipient of the communication:

(a) if it is without lawful authority and is
(b) an interception of communication in the course of its transmission by means of a private system; or
(c) an interception of communication in the course of its transmission, by means of a public communication system, to or from an apparatus comprised in a private communication system.

(3) Where a state is a party to an international agreement which

(a) relates to a provision of mutual assistance in connection with the interception of communications, and

(b) requires the issue of a warrant, order or equivalent instrument in cases in which assistance is given,

the law enforcement agency shall ensure that a request for assistance in accordance with the agreement is not made on behalf of a person in Ghana to the competent authorities of another country except with lawful authority.

(4) A person intercepts a communication lawfully if the interception
(a) is authorised by or under these Regulations;

(b) is done pursuant to any statutory authority conferred under any enactment..

(5) A person may intercept communication in the course of its transmission by means of a private communication system if that person has

(a) a right to control the operation or the use of the system; or

(b) the express or implied consent of the sender to make the interception.

Interception by means of a communication system

2. (1) A person intercepts communication in the course of its transmission by means of a communication system if without lawful authority, that person

(a) modifies or interferes with the system, or its operation,

(b) accesses or monitors transmissions by means of the system, or

(c) accesses or monitors transmissions made by wireless telegraphy to or from an apparatus comprised in the system,

(d) makes some, or part of the contents of the communication available while being transmitted to a person other than the sender or intended recipient of the communication.

(2) The interception of communication by any communication broadcast for general reception shall not be construed as an interception of communication.

(4) The interception of an electronic communication takes place under these Regulations if the interception

(a) involves the modification, interference, access or monitoring of communication transiting through, sent by or intended for a person in Ghana;

(b) affects communication which is intercepted in the course of its transmission by means of a public communication system; or

(c) occurs in the course of transmission by means of a private communication system in a case in which the sender or intended recipient of the communication is in Ghana.

(5) Reference in these Regulations to the interception of a communication in the course of its transmission by means of a communication system does not include references to

(a) conduct that takes place in relation to a communication which consists in any traffic data being attached to a communication by the sender by means of a communication system;

(b) conduct that falls within paragraph (a), which gives a person who is neither the sender nor the intended recipient access to a communication that is meant to identify traffic data attached; or

(c) any conduct authorised by any enactment or rule of law .

(6) For the purposes of these Regulations

(a) references to the modification of a communication system include references to the attachment of any apparatus or modification or interference with any part of the system or any wireless telegraphy apparatus used to make transmissions to or from apparatus comprised in

the system;

(b) the time during which communication is being transmitted by means of a communication system include any time within which communication transmitted, is stored in a manner that enables the intended recipient to collect it or otherwise to have access to it; and

(c) the mode by which the contents of communication are made available to a person while being transmitted includes instances where the contents of the communication, while being transmitted, are diverted or recorded so as to be available to a person subsequently.

Lawful interception

3. (1) The interception of a communication by a person is lawful if

(a) the sender or the intended recipient has consented to the interception;

(b) the communication is one sent by, or intended for a person who has consented to the interception;

(c) surveillance by means of that interception has been authorised by law;

(d) it takes place for purposes connected with the provision or operation of a service permitted under any enactment or rule of law

(2) Interception of a communication in the course of transmission by means of wireless telegraphy is lawful if it takes place

(a) with the authority of a designated person under an enactment relating to wireless telegraphy; and

(b) for purposes connected with

(i) the issue of licences under any enactment related to wireless telegraphy;

(ii) the prevention or detection of anything which constitutes interference with wireless telegraphy; and

(iii) the enforcement of a provision of an enactment that relates to the interference.

Authorised Interception of external Communication

4. (1) Interception by a person of a communication in the course of its transmission by means of a communication system is authorised if

(a) the interception is carried out for the purpose of obtaining information about the communication of a person who the interceptor has reasonable grounds to believe, is in a country or territory outside Ghana;

(b) the interception relates to the use of

(i) public communication service or would be a public communication service if it is provided to persons in a country or territory other than Ghana; or

(ii) a communication service that would be a public communication service if the persons to whom it is offered or provided are members of the public in Ghana; and

(c) the person who provides that service is required by the law of that country or territory to carry out, secure or facilitate the interception in question;

(2) The interception of communication is authorised in the course of transmission using a service or an apparatus used by the interceptor wholly or partly in the normal course of business.

Statutory conduct

These Regulations do not derogate from the exercise of a power

(a) conferred by or under any rules made under the Prisons Service Act 1972, (NRCD 46). or

(b) conferred under the Mental Health Act 1972, (NRCD 30).

(2) Interception of communication which takes place in a public hospital is authorised if the interception is reasonably necessary and is in accordance with any directive made under any enactment.

Warrants

Issue of interception warrant

Any Law enforcement agent may apply to any High Court Judge at any time for the issue of an interception warrant to :

(a) intercept communication which is transmitted by means of a communication system of the communication described in the warrant;

(b) make a request for the provision of assistance in connection with, or in the form of an interception of communication described in the warrant in accordance with an international mutual assistance agreement;

(c) provide, in accordance with an international mutual assistance agreement to the competent authorities of a contracting country, an assistance in connection with an interception of communication described in the warrant;

(d) disclose an intercepted material obtained by an interception authorised or required by the warrant;

(e) require a communication operator in possession of or capable of obtaining, any communication data to obtain the data in a manner consistent with its normal operations and to disclose specified required data

(2) The Court shall issue an interception warrant where it is satisfied by the applicant that an interception warrant is:

(a) necessary, and

(b) proportionate to what is sought to be achieved.

(3) Without limiting the generality of sub regulation (2)(a) an interception warrant is necessary:

(a) in the interest of national security;

(b) to prevent, detect or prosecute a criminal offence;

(c) to safeguard the economic well-being of Ghana; or

(d) to give effect to any international mutual assistance agreement.

(4) A Court prior to the issue of an interception warrant shall consider whether the information which is sought to be obtained under a warrant could be reasonably obtained by other means when considering whether the requirements related to the issue of an interception warrant are satisfied.

(5) An interception warrant is not necessary in relation to safeguarding the economic wellbeing of citizens unless the information which is sought to be obtained is information related to the acts of persons which would undermine the economic interest of Ghana.

(6) An interception warrant is authority for any of the following acts if, any of them occurs in the course of the execution of a warrant.

(a) engagement in conduct including the interception of a communication not identified by the warrant, which is necessary to execute an order which is expressly authorised or required by the warrant;
(b) engagement in conduct to obtain related communication data; and
(c) explanation on a person to whom the warrant is addressed to provide assistance to give effect to the warrant; and
(d) examination and conduct of forensic examination of any computer or any network connected to or accessed by a computer identified in an interception warrant in the execution of the warrant or pursuant to any collaborative effort or international, bilateral or multilateral agreement or convention.
(e) soliciting technical knowledge and assistance from any relevant law enforcement agency to assist the law enforcement agency executing the interception warrant in the interception of communication.
(f) using of real-time monitoring procedure reasonably consistent with prevailing technology available to the law enforcement agency.

(7) A communication operator who fails to comply with an order under sub regulation 1(e) commits an offence and is liable upon summary trial and conviction to a term of imprisonment not exceeding five years or to a fine not exceeding five hundred penalty units or to both.

(8)(1) A Court which issues an interception warrant shall ensure that the warrant is limited to:

(a) the person who has knowledge about the communication to be intercepted;
(b) the extent to which any of the material or data is copied; and
(c) the number of copies requested.

. (2) The Court shall make appropriate orders to ensure that each copy of the intercepted material or communication data is stored in a secure manner for as long as is needed.

(3) Where arrangements in relation to interception warrants are surrendered to an authority of a country or territory outside Ghana the interception warrant shall be required to be affected by the minimum exposure obligations under these Regulations.

(4) The applicant shall ensure that where an intercepted material or communication data is transferred to an authority outside Ghana by a warrant, the intercepted material and communication data and copies of the material or data shall be surrendered to an authority of

a country or territory outside Ghana only if the requirements of these Regulations are complied with.

(5) The Rules of Court Committee shall within six months of the coming into force of these regulations provide the rules regulating applications under these Regulations.

Persons entitled to request Interception warrants

An application for an interception warrant may be made by :

(a) the Co-ordinator of the National Security Council;

(b) a law enforcement agent of the rank of superintendent of Police or above

(c) the Director of the Immigration Service;

(d) the Director of an Intelligence Agency

(e) the Director of Narcotic Control Board

(f) the Director of the Economic and Organised Crime Office

Particulars of person, premises and computer

An interception warrant shall give detailed particulars of:

(a) the name and address of the person who is the subject of interception;

(b) the premises to which the interception warrant relates; or

(c) the location of the computer or the network to which a private or public communication network is or may be attached whether temporal or permanent; or

(d) data that may be stored whether known or unknown, private, public or backup

(2) The particulars shall where appropriate, identify the communication by reference to:

(a) any sender, or intended recipient or any person named or described in the warrant or

(b) communication originating from or intended for transmission to the premises named or described.

(3) Sub regulations (1) and (2) do not apply to an interception warrant if the relevant description of communication confines the conduct authorised or required to conduct falling within sub regulation (4)

(4) Interception falls within these Regulation if it consists of

(a) the interception of external communication in the course of transmission by means of a communication system; and

(b) any conduct authorised in relation to the interception.

Duration of an interception warrant

9(1) Unless otherwise determined by the Judge, an interception warrant shall be for a duration of 14 days.

(2) An interception warrant may be renewed by application to the Court.

(3) An application for the cancellation an interception warrant may be made to any High Court Judge.

Modification of an interception warrant

10. (1) An interception warrant may be modified at any time by any High Court Judge.

(2) A warrant shall not be renewed, modified or cancelled except by order of the Court.

Execution of interception warrant

11. (1) An interception warrant issued under these Regulations shall be executed

(a) by the person to whom it is addressed, or

(b) by a person acting through, or together with other persons as authorised by the warrant.

(2) A person who requires the assistance of any other person to execute an interception warrant

(a) may serve a copy of the warrant on a person who may be able to provide the assistance; or

(b) may make arrangements for the copy of the warrant to be served.

(3) An interception warrant shall be served by the authorised person on:

(a) a person who provides a postal service,

(b) a person who provides a public communication service, or

(c) a person not falling within paragraph (b) who has control of the whole or any part of a communication system located wholly or partly in Ghana

(4) A person served with an interception warrant who fails to comply with the warrant commits an offence and is liable upon summary trial and conviction to imprisonment for a term not exceeding two years or to a fine not exceeding five hundred penalty units or to both.

Governmental Obligations

Destruction of intercepted data

12. An intercepted material or communication data shall not be destroyed where:

(a) it is likely to become necessary during any subsequent investigations;

(b) it is necessary to facilitate the performance of the functions under these

Regulations;

(c) it is necessary to facilitate the conduct of a criminal investigation or prosecution;

(d) it is necessary for the performance of a duty imposed on under the Public Records and Archives Administration Department Act, 1997, (Act 535)

(e) it is considered by National Security to be in the national interest to be kept for classified purposes

Intercepted material

Use of intercepted material

13. (1) An intercepted material obtained under an interception warrant may be used in criminal proceedings.

(2) The contents of an intercepted material may be shared between law enforcement agencies and these Regulations shall not prohibit the disclosure of any of the contents of a communication if the interception of that communication is lawful.

Disclosure related issues

Duty of non-disclosure

14. (1) Where an interception warrant is issued or renewed, a person to whom it is addressed or who assists in its execution shall keep confidential the matters mentioned in sub regulation (2).

(2) The following matters shall be kept confidential:

(a) the existence and contents of the warrant;

(b) the fact of an application

(c) the details of the issue of the warrant and renewal or modification of the warrant;

(d) the existence and contents of any requirement to provide assistance to give effect to the warrant;

(e) the steps taken to give effect to the warrant or; and

(f) the particulars in the intercepted material, together with any related communication data.

(3) A person who makes a disclosure to another person of anything that is required to be kept confidential under these Regulations commits an offence and is liable upon summary trial and conviction to a term of imprisonment not exceeding five years or to a fine not exceeding two thousand penalty units or to both.

(4) In proceedings against a person for an offence under these Regulations in respect of a disclosure, it is a defence for that person to prove that

(a) reasonable steps were taken after first becoming aware of the matter to prevent any further disclosures

(b) the disclosure was made by or to a legal practitioner in circumstances of Solicitor/client relationship

(c) the disclosure was authorised.

(5) A disclosure shall not be justified where it is made with a view to furthering a criminal purpose.

Acquisition and disclosure of communications data

15. (1) These Regulations apply to any conduct in relation to a postal service or communication system to obtain communication data, but does not apply to

(a) conduct consisting of the interception of communications in the course of transmission by means of this service or system; and

(b) the disclosure to a person of communication data.

(2) Conduct to which these Regulations apply is lawful if

(a) it is conduct in which a person is authorised or required to engage in under these Regulations; and

(b) the conduct is in accordance with, or by virtue of, the authorisation or requirement.

(3) A person is not subject to civil liability in respect of conduct

(a) which is incidental to conduct which is lawful under these Regulations; and

(b) which might reasonably have been expected to have been implied.

(4) For purposes of this regulation

(a) references, in relation to traffic data comprising signals for the actuation of apparatus, to a communication system by means of which a communication is being or may be transmitted include references to any communication system in which that apparatus is comprised; and

(b) references to traffic data being attached to a communication include references to the data and the communication being logically associated with each other.

Notices and Issue

Authorisation notice

16. (1) An interception notice to an operator shall be in writing and accompanied by the order of the Court.

(2) A notice to an operator requiring communication data to be disclosed or to be obtained shall be in writing and shall describe the nature and scope of interception given, the communication data to be disclosed or obtained, particulars of the person giving the interception and the manner in which disclosure shall be made.

(3) A notice shall not require the disclosure of data to any person other than the person giving the notice or any other person whose name and particulars are specifically mentioned in the notice.

(4) An interception notice issued to an operator may be renewed at any time before the expiry of the interception warrant.

(5) An interception notice may be cancelled at any time.

Requirement for disclosure of protected information

Power to require disclosure in relation to encrypted product

17. (1) Where a Law Enforcement Agent is satisfied that

(a) a key or the means of decryption of information is in the possession of a person, or

(b) an imposition of a disclosure requirement in respect of the information

is

(i) necessary on grounds falling within sub regulation (3), or

(ii) necessary to secure the effective exercise or proper performance by any public authority of a statutory power or statutory duty, or

(c) that the imposition of such a requirement is proportionate to what is sought to be achieved by its imposition, and

(d) that it is not reasonably practicable for the person with the appropriate permission to obtain possession of the protected information in an intelligible form without giving notice under this regulation,

the person with that permission may, by disclosure notice to the person in possession of the key, impose a disclosure requirement in respect of the protected information.

(2) A notice under this regulation to impose a disclosure requirement in respect of any information

(a) shall be in writing ;

(b) shall describe the information to which the notice relates;

(c) shall specify the purpose for which the notice is given;

(d) shall specify the office, rank or position held by the person giving the notice ;

(e) shall specify a reasonable time within which the notice is to be complied with; and

(f) shall set out the disclosure that is required by the notice and the form and manner in which it is to be made.

(g) indicate whether or not access to the information is authorised by an interception warrant

(3) Where it appears to a person issuing the disclosure notice that

(a) more than one person is in possession of the key to a protected information,

(b) any of those persons is in possession of that key in the capacity as an agent, officer or employee of a body corporate or natural person is in possession of the key, a notice under this regulation shall be given to an officer or employee of the body corporate who appears to be an appropriate person to receive the notice.

(4) A notice under this regulation shall not require the making of a disclosure to a person other than

(a) the person giving the notice; or

(b) the person specified in or identified by the notice.

(5) A notice under this regulation shall not require the disclosure of a key which

(a) is used solely to generate electronic signatures; and

(b) has not been used for any other purpose.

Disclosure notice in relation to protected information

18. (1) The effect of a disclosure notice imposing a disclosure requirement in respect of an encrypted information on a person who is in possession of information is that he:

(a) shall be required to use any key that the person possesses to grant access to the information or to put the information into an intelligible form; and
(b) may be required, in accordance with the notice imposing the requirement, to make a disclosure of the information in an intelligible form.

(2) A person who is subject to a requirement under sub regulation (1) (b) to make a disclosure of any information in an intelligible form complies with that requirement if

(a) that person makes, a disclosure of any key to the information that is in the person's possession; and
(b) the disclosure is made to the person to whom it was required to be provided in accordance with the notice imposing the requirement.

(3) Where, in a case in which a disclosure requirement in respect of an information is imposed on a person by these Regulations and

(a) that person is not in possession of the information,
(b) that person is incapable, without the use of a key to obtain access to the information and to disclose it in an intelligible form, or
(c) the notice states that it can be complied with only by the disclosure of a key to the information,

(4) The effect of imposing the disclosure requirement on that person is to require that person to make a disclosure of any key to the protected information at a relevant time in accordance with the notice imposing the requirement.

(5) Sub regulations (6) to (9) apply where a person
(a) is entitled or obliged to disclose a key to information for the purpose of complying with any disclosure requirement imposed under these Regulations; and
(b) is in possession of more than one key to that information.

(6) A person need not give notice to make a disclosure of any key which by itself, is sufficient to enable the person to whom they are disclosed to obtain access to the information and to put it into an intelligible form.

(7) Where

(a) a person is given notice to comply with a requirement without disclosing the keys in the person's possession, and
(b) there are different keys, or combinations of key, in the possession

of that person, the disclosure of which would constitute compliance,
the person given notice may select which of the keys, or combination of keys, to disclose for the purpose of complying with the requirements in accordance with these Regulations.

(8) A person who has notice shall not be taken to have complied with the disclosure requirement unless the key to the protected information has been disclosed to give access to the protected information in an intelligible form to the person providing the notice. .

(9) Where, a disclosure requirement in respect of any information is imposed on a person under these Regulations and

(a) that person has been in possession of the key to that information but is no longer in possession of it, or

(b) if the person had continued to have possession of the key, the person would have been required by virtue of the giving of the notice to disclose it, or

(c) that person is in possession of information which would facilitate the obtaining or discovery of the key or the putting of the protected information into intelligible form,

the person shall be required to disclose the facilitating information in accordance with the notice.

Conditions relating to disclosure notice

19. (1) A disclosure notice imposing a disclosure requirement in respect of any information shall:

a. Require the disclosure of the information to be made in intelligible form or by reference to the requisite decryption method which would make the entire information intelligible
b. specify the matters falling within subsection 2 to which the notice is given
c. specify the time by which the notice is to be complied with and
d. set out the disclosure that is required by the notice and the form and manner in which it is to be made

(2) A person shall not give a direction under sub regulation (1) unless that person is satisfied that:

(a) there are special circumstances of the case which mean that the purposes for which it was believed necessary to impose the requirement in question would be defeated, in whole or in part, if the direction were not given; and

(b) the direction given is proportionate to what is sought to be achieved by prohibiting compliance with the requirement in question otherwise than by the disclosure of the key itself.

(3) The matters to be taken into consideration in evaluating whether the requirement under this regulation has been complied with include without limitation:

(a) the extent and nature of any protected information, in addition to the protected information in respect of which the disclosure requirement is imposed; and

(b) any adverse effect which the direction might have on a business carried on by the person on whom the disclosure requirement is imposed.

Non-compliance with disclosure notice

20. (1) A person, other than a person under investigation or charged with any offence who is entitled to the right not to incriminate himself, to whom a relevant disclosure notice is given commits an offence if that person fails to comply with the disclosure notice without lawful excuse and is liable upon summary trial and conviction to a term of imprisonment not exceeding three years or a fine not exceeding two thousand penalty units or both.

(2) In proceedings against a person for an offence under this regulation, if it is shown that that person was in possession of key to an information at any time before the time of the disclosure notice, that person have the burden of proving that he did not have the key at the time of the service of the disclosure notice.

(3) In proceedings against a person for an offence under these Regulations it is a defence for that person to show

(a) that it was not reasonably practicable to make the disclosure required by virtue of the disclosure notice before the time required under the notice, or

(b) that disclosure was made as soon as it was reasonably practical to do so.

Disclosure notice and duty to keep secret

21. (1) For the purposes of these Regulations the contents of a disclosure notice relating to an investigation, monitoring and prevention of any criminal offence shall be confidential and shall not be disclosed except in accordance with law.

(2) Where the subject matter of a disclosure notice does not relate to any matter in respect of which a duty to keep anything confidential is required, the notice may impose a duty to keep confidential the contents of such notice. ~~court order~~.

(3) A person who makes a disclosure to any other person of anything that is required by a disclosure notice to be kept confidential commits an offence and is liable upon summary trial and conviction to a term of imprisonment not exceeding two years or a fine not exceeding five hundred .penalty units or to both.

(4) In proceedings against a person for an offence in respect of any disclosure, it is a defence for that person to prove that

(a) the disclosure was effected entirely by the operation of software or an independent third party's equipment designed to indicate when a key to protected information has ceased to be secure and over which the person had no knowledge or control; or

(b) the person could not reasonably have been expected to take steps, after being given the notice or becoming aware of it or of its contents, to prevent the disclosure; or

(c) the disclosure was made to a legal practitioner in circumstances of client lawyer privilege and for purposes otherwise than for furthering criminal purposes.

(7) A disclosure is not lawful where such disclosure is made with the view to

furthering any criminal purpose.

Matters relating to disclosed keys

Protection of disclosed keys in relation to encrypted product

22. (1) The person who obtains a key under these regulations shall ensure that the key is protected and shall not use any key for any purpose incompatible with these regulations and the law.

Any persons who uses a key under these regulation for purposes incompatible with these regulations commits an offence and shall be liable upon summary trial and conviction on conviction to a sentence not less than six (6) months and not more than thirty six (36) month and a fine not less than five thousand penalty points and not more than ten thousand penalty points or both

Mandatory log compilation:
All entities of the Presidency and Public Service Institutions shall ensure that each respective computer system generates and keeps digital logs of every user-access activity on systems of the Presidency and Public Service Institutions.

All entities of the presidency and Public Service Institutions shall ensure that each respective computer system generate and keep or digital logs of every third party activities on systems of the Presidency and Public Service Institutions

All entities of the Presidency and Public Service Institutions shall ensure that each respective computer system generate and keep or digital logs of every generates backups and the backup are hosted on NITA designated servers.

All digital logs generated on computer systems of the Presidency and Public Service Institutions shall constitute classified information to which only persons with prescribes user controls can access same.

All digital logs shall be generated and held in a manner using technology which makes :
the deletion impossible based on the science of existing known technology at the time,
any attempt and/or alteration and any modification capable of being instantly detected

All digital logs shall be generated and designed in a manner which
a) detects every user violation or prohibited conduct,
b) generates user violation logs and
c) automatically notifies the Chief Information Officers and NITA designated Officers of user violations
howsoever arising or caused.

Offences
It is an offence under these Regulations to retain on engage in any conduct prohibited under these regulations in respect of digital logs and person and/or entity found guilty of this offence shall be liable upon summary trial and conviction be sentenced to a term of

imprisonment not exceeding Two (2) years or to an entity penalty not exceeding Ten Thousand Penalty Points or both.

Miscellaneous provisions

Application

23. (1) A provision of these Regulations in relation to a conduct of any description which is or may be authorised by a warrant, authorisation or notice, or in relation to which information may be obtained in any manner, shall not be construed

(a) to make it unlawful to engage in any conduct of that description, that is not otherwise unlawful under these Regulations and would not be unlawful apart from these Regulations;

(b) to require
  (i) the issue, grant or giving of a warrant, authorisation or notice, or
  (ii) taking any step for or towards obtaining the authority of such a warrant, authorisation or notice, before any such conduct of that description is engaged in; or

(c) to prejudice any power to obtain information by any means that do not involve conduct that may be authorised under these Regulations.

(2) References, in relation to traffic data that comprises signals for the actuation of apparatus, to a communication system by means of which any communication is being or may be transmitted to include references to a communication system in which that apparatus is comprised;

(3) References to traffic data being attached to a communication include references to the data and the communication being logically associated with each other.

Interpretation

24. In these regulations unless the context otherwise requires

"apparatus" includes any equipment, machinery or device and any wire or cable;

"body corporate" includes an incorporated entity under the Companies Code, a partnership under the Incorporated Partnership Act, A Trust under the Trustees Incorporation Act, a Co-operative under the Cooperatives Act, a business registered under the Registration of Business Names Act or any unincorporated body of persons.

"business" includes references to any activities of a government department, of any public authority or of any person or office holder on whom functions are conferred by or under any enactment.

"certified", in relation to a certificate, means a description certified by the

certificate as a description of material the examination of which the Minister considers necessary;

"communication" includes

(a) any electronic transmission by a communication or postal service;

(b) anything comprising speech, music, sounds, visual images or data of any description; and

(c) signals serving either for the impartation of anything between persons, between a person and a thing or between things or for the actuation or control of any apparatus;

"communications data" means any of the following

(a) any traffic data comprised in or attached to a communication (whether by the sender or otherwise) for the purposes of any postal service or communication system by means of which it is being or may be transmitted;

(b) any information which includes none of the contents of a communication (apart from any information falling within paragraph (a)) and is about the use made by any person

(i) of a postal service or communications service; or

(ii) in connection with the provision to or use by a person of a communications service, of a part of a communication system;

(c) any information not falling within paragraph (a) or (b) that is held or obtained, in relation to persons to whom he provides the service, by a person providing a postal service or communications service;

"communications operator" means a person who lawfully provides or communications service;

"communications service" means any service inclusive without exception to data, voice, video and all forms of multimedia features that consists in the provision of access to, and of facilities for making use of, any communication system (whether or not one provided by the person providing the service); and

"communication system" means any system (including the apparatus comprised in it) which exists (whether wholly or partly in Ghana or elsewhere) for the purpose of facilitating the transmission of communications by any

means inclusive of transmission by use of electronic, electrical or electro-magnetic energy.

"copy", in relation to intercepted material or related communications data, means any of the following whether in digital or tangible form

(a) any copy, extract or summary of the material or data which identifies itself as the product of an interception, and

(b) any record referring to an interception which is a record of the identities of the persons to or by whom the intercepted material was sent, or to whom the communications data relates and "copied" shall be construed accordingly;

"Court" means High Court .

"data", in relation to a postal item, means any information relating to such item held in electronic form.

"detecting crime" include

(a) establishing by whom, for what purpose, by what means and generally in what circumstances any crime was committed; and

(b) the apprehension of the person by whom any crime was committed; and any reference in this Act to preventing or detecting serious crime shall be construed accordingly;

"designated person" means person authorised under these regulations to issue appropriate notices or authorisation

"document" includes a map, plan, design, drawing, picture or other image;

"electronic signature" includes a digital signature and advanced electronic signature and refers to anything in electronic form which

(a) is incorporated into, or otherwise logically associated with, any electronic communication or other electronic data;

(b) is generated by the signatory or other source of the communication or data; and

(c) is used for the purpose of facilitating, by means of a link between the signatory or other source and the communication or data, the establishment of the authenticity of the communication or data, the establishment of its integrity, or both;

"external communication" means a communication sent or received outside the Republic of Ghana;

"government department" includes any Government of Ghana Ministry, Department or Agency;

"hospital" has the same meaning as in the Ghana Health Service and Teaching Hospitals Act, 1996, Act 525 and includes Private Hospital as defined in section 19 of the Private Hospitals and Maternity Homes Act, 1958, No 9;

"intercepted material", in relation to an interception warrant, means the contents of any communications intercepted by an interception to which the warrant relates;

"interception subject", in relation to an interception warrant, means the person about whose communications information is sought by the interception to which the warrant relates;

"international mutual assistance agreement" means an international agreement designated for the purposes of regulation 6 ;

"key", in relation to any electronic data, means any decryption procedure, key, code, password, algorithm or other data the use of which (with or without other keys)

(a) allows access to the electronic data, or
(b) facilitates the putting of the data into an intelligible form;

"Law Enforcement Agencies" includes , The Ghana Police Services, Ghana Immigration Services, Ghana Fire Services, Ghana Armed Forces, Serious Fraud Office and such other agencies that the Minister for the Interior may from time to time by Legislative Instrument include in the definition;

"modification" includes alterations, additions and omissions, and cognate expressions shall be construed accordingly;

"National Revenue Collection Agencies " means the Internal Revenue Service, Value Added Tax Service, and Customs Excise & Preventive Services;

"person" includes any organisation and any association or combination of persons;

"postal service" means any service incidental to the identification of a sender or intended recipient of any electronic payment medium or data transmission and includes any log or data generated during any electronic payment, record inputting in respect of any courier or any delivery service for collection, sorting, conveyance, distribution, delivery, verification during the provision of any such service.;

"postal operator" means a person who lawfully provides a postal service;

"private communication system" means any lawfully established communication system which, without itself being a public communication system, is a system in relation to which the following conditions are satisfied

(a) it is attached, directly or indirectly and whether or not for the purposes of the communication in question, to a public communication system whether or not such public communication system owner is known or unknown; and

(b) there is apparatus comprised in the system which is both located in Ghana and used (with or without other apparatus) for making the attachment to the public communication system;

"private information", in relation to a person, includes any information relating to his private, family life and any information which is not made publicly available by such person;

"protected information" means any electronic data which, without the key or process for decryption to the data

(a) cannot, or cannot readily, be accessed, or

(b) cannot, or cannot readily, be put into an intelligible form;

"public postal service" means any postal service which is offered or provided to, or to a substantial section of, the public in any one or more parts of Ghana and includes the provision of certification of transmission or delivery of communication through the service provider;

"public communications service" means any communications service which is offered or provided to, or to a section of, the public in any one or more parts of Ghana;

"public communication system" means any such parts of a communication system irrespective of the ownership structure by means of which any public communications service is provided to any member of the public in Ghana.;

"psychiatric services" has the same meaning as in the Mental Health Decree, 1972, (NRCD 30) ;

"related communications data", in relation to a communication intercepted in the course of its transmission by means of a postal service or communication system, means so much of any communications data as is obtained by, or in connection with, the interception and relates to the communication or to the sender or recipient, or intended recipient, of the communication;

"relevant enactment" means any enactment applicable to a law enforcement agency in the course of investigations, monitoring or prosecuting any offence

in Ghana or fulfilling any international agreement or co-operation requirement for the purpose of crime prevention, investigation, monitoring or prosecution.

"relevant interception warrant" means

(a) in relation to a person providing a public postal service, means an interception warrant relating to the interception of communications in the course of their transmission by means of that service; and

(b) in relation to a person providing a public communications service, means an interception warrant relating to the interception of communications in the course of their transmission by means of a communication system used for the purposes of that service.

"relevant public authority" means any national security agency, law enforcement agency and national revenue collection service;

"section 8(4) certificate" means any certificate issued for the purposes of section 8(4);

"senior officer", in relation to a body corporate, means a director, manager, secretary or other similar officer of the body corporate; and for this purpose "director", in relation to a body corporate whose affairs are managed by its members, means a member of the body corporate;

"surveillance" includes

(a) monitoring, observing or listening to persons, their movements, their conversations, computer and related network traffic and information or their other activities or communications;
(b) recording anything monitored, observed or listened to in the course of surveillance;
(c) surveillance by or with the assistance of a surveillance device and
(d) interception of a communication in the course of its transmission by means of a postal service or communication system

"surveillance device" means any apparatus including software, hardware, wireless, wired electronic or manual, designed or adapted for use in surveillance;

"traffic data", in relation to any communication, means

(a) any data identifying, or purporting to identify, any person, apparatus or location to or from which the communication is or may be transmitted,
(b) any data identifying or selecting, or purporting to identify or select, apparatus through which, or by means of which, the

communication is or may be transmitted,

(c) any data comprising signals for the actuation of apparatus used for the purposes of a communication system for effecting (in whole or in part) the transmission of any communication, and

(d) any data identifying the data or other data as data comprised in or attached to a particular communication, but that expression includes data identifying a computer, computer file or computer program access to which is obtained, or which is run, by means of the communication to the extent only that the computer, file or program is identified by reference to the apparatus in which it is stored;

"warrant" includes any authorisation, notice or other instrument (however described) conferring a power of the same description as may, in other cases, be conferred by a warrant.

PART FIVE: NETWORK SECURITY

Network and Security

16(1) NITA shall be responsible for providing network security and protection directives, standards and guidelines for all Entities of the Presidency and Public Services Institutions.

(2) NITA shall be responsible for the monitoring and enforcement of compliance by all Entities of the Presidency and Public Services Institutions of all directives, standards and guidelines issued by NITA.

(3) NITA shall be responsible for the monitoring and enforcement of compliance by all Entities of the Presidency and Public Services Institutions of all directives issued by the Minister.

(4) NITA shall define qualification levels required for network training for personnel of Entities of the Presidency and Public Services Institutions on aspects of networks infrastructure and security to ensure competence and capacity to adhere to directives, standards and guidelines issued by NITA

NITA shall in respect of the Internet of Things provide operational and security directives on their use, reporting regimes, access and activity permitted controls and such other security features as may be required to monitor, detect, prevent, track, identify and generate forensic evidence relevant to the apprehension and prosecutions of offenders and access and/or use breaches.

Compliance Audit

20(1) Every Entities of the Presidency and Public Services Institutions shall be subject to compliance audits at intervals determined by NITA to ensure compliance with

(a) primary legislation
(b) subsidiary legislations,
(c) Gazette required publications
(d) Directives, standards, and guidelines issued by NITA
(e) Directives from the Minister of Communications and
(f) Ghana ICT4AD Policy time projected timelines and policy objectives.

(2) Every Entities of the Presidency and Public Services Institutions shall ensure compliance with the audit findings within the period prescribed in such audits and audit reports, copies of which shall be forwarded to the NITA Board and the Minister.

PART SIX: CYBER SECURITY

Cyber Security

17(1) NITA shall be responsible for monitoring for compliance by Entities of the Presidency and Public Services Institutions and the enforcement of the Cyber Security Policies approved by the Minister and the National Security Advisor.

(2) Every Entity of the Presidency and Public Services Institutions shall as part of its Reporting under this Act report on its compliance and deviations from the Cyber Security Policy and where there are any deviations, such entity of the Presidency and Public Services Institution shall provide details of steps being taken to remedy such deviations under the period.

(3) Every Entity of the Presidency and Public Service Institutions shall notify NITA of data and security breaches within a period not exceeding 24 hours from such detection of breach and shall provide :

(a) details to NITA of steps it has commenced to detail with such breaches,
(b) the digital forensic information and analysis which such entity of the Presidency and Public Services Institution has with respect to such breaches and
(c) particulars of its compliance with such entity of the Presidency and Public Service Institutions' disaster prevention and disaster recovery policy.

NITA shall be responsible for providing Policy framework and Directive to be complied with in all procurement related matters relating to cybersecurity and supply chain risk management principles and practices throughout the acquisition lifecycle when purchasing, deploying, operating, and maintaining Internet of Things (IoT)5 devices, systems, and services

Chief Information Officer

18(1) The Presidency and each Public Services Institution shall appoint a Chief Information Officer with responsibility for ensuring compliance of the entity of the Presidency and/or Public Services Institution with the provisions of these Regulations, Electronic Transactions Act and provisions of all information requested by NITA pursuant to implementation of the Information Communications Technology Policy, the NITA Act and regulations made thereunder and the Electronic Transactions Act and regulations made thereunder.

(2) Until a Chief Information Officer is appointed by such MDA the Chief Director shall be deemed to be the Chief Information Officer and shall perform the responsibilities of the Chief Information Office prescribed under these Regulations.

(3) Until a Chief Information Officer is appointed by such entity of the Presidency and/or Public Services Institution the person holding the highest office in such entity of the Presidency and/or Public Services Institution shall be deemed to be the Chief Information Officer and shall perform the responsibilities of the Chief Information Office prescribed under these Regulations.

(4) The Chief Information Officer shall be responsible for ensuring that all information provided to NITA and relevant Entities of the Presidency and Public Services Institutions' are accurate and timely.

Inspection and investigation

19(1) An inspector being an officer of NITA may

(a) enter the premises of an Entity of the Presidency and Public Services Institution to determine whether the provisions of the ETA, NITA, and Directives of the Minister in respect of matters required for reporting under this Legislation are being complied with;

(b) inspect and make copies of or extracts from books, records or other documents;

(c) demand the production of and inspect the relevant documents required for such compliance monitoring;

and

(d) inspect third party facilities and premises associated with or engaged by any Entity of the Presidency and Public Services Institution to provide services in respect of which compliance monitoring requests have been made by NITA or which provisions of this legislation requires reporting from such entities of the Presidency and Public Services Institutions to NITA

(2) The inspector may enter the premises at any reasonable time without notice and shall show identification of authorization in writing from NITA setting out the purpose of such entry to be pursuant to inspection under sub regulation 19(1) and the Chief Information Officer shall be obligated to provide such inspector with access and support to ensure that the inspectors carry out the inspection .

(3) A person shall not

(a) hinder or obstruct an inspector in the discharge of official duty; or

(b) impersonate an inspector

PART SEVEN : DIGITAL RECORDS CLASSIFICATIONS REGIMES

Classification levels

Data and Electronic Records by MDAs and each Arm of Government shall be classified and marked with one or more of the following security levels categories

i. Top Secret
ii. Secret
iii. Confidential
iv. Restricted
v. Protect
vi. Open Data

vii. Sector Specific
viii. Interoperable
ix. Multiple

Top Secret Level
Data and Electronic Records shall not be given the security level of Top Secret unless it is most sensitive information requiring the highest levels of protection from the most serious threats and relates to national security, national health, public health and protection or would significantly undermine diplomatic relations with International Institutions, Regional Organisation or bilateral relations.

Secret Level
Data and Electronic Records shall not be given the security level of Secret unless it is very sensitive information that justifies heightened protective measures to defend against determined and highly capable threat actors inclusive of cyber and digital threats, protection of critical infrastructure, protected computers, protected records or capable of impairing the capabilities of law enforcement agents in the discharge of the protection of the sovereignty of the Republic, the monitoring of offences against the state and the defence and protection of the Republic in its defence against hostile action of third countries or their agents.

Restricted and Protected Level
Data and Electronic Records shall not be given the security level of Restricted or Protected unless it is general information that is created or processed by the public sector in the course of its routine business operations and services and would have damaging consequences if lost, stolen but are not subject to a heightened threat profile.

Sector Specific Level
Data and Electronic Records shall be given Sector Specific classification where it constitutes the statutory core and preserved object and functions of that Institution or MDA for which it reports directly to specific Arms of Government and to no other institution except in matters relating to compliance and investigations by relevant law enforcement agencies of any breaches of law.

Interoperable and Multiple Level
Data and Electronic Records shall be given Interoperable and or Multiple classification where such data and electronic records may be relevant to any MDA and Arm of Government as a digital policy identified or potential convergent technology related information generated by such institutions howsoever originally generated.

Open Data Level
Data and Electronic Records shall be given Open Data classification where such data and electronic record does not constitute prohibited disclosure under the provisions of the Data Protection Act, does not have any of the classifications other than the Open Data Classification and promotes the attainment of objects of the Digital Policy of Ghana.

Institutions Further classification Obligations
Every MDA and Arm of Government shall in addition identify and determine records which related to any of the undermentioned categories and further apply the suffixes which relate to

their corresponding areas of National Interest codes in addition to their security levels categories

i. Defence& Security national interest area suffix marking shall be DAS
ii. Diplomacy national interest area suffix marking shall be DIP
iii. Economy & Finances national interest area suffix marking shall be EAF
iv. Life & Liberty national interest area suffix marking shall be LAL
v. Crime national interest area suffix marking shall be CRM
vi. Policy national interest area suffix marking shall be PLY
vii. Information areas suffix marking shall be IFM

No data and electronic Record by MDAs and Arms of Government generated after the passage of this Regulations shall be generated without assigning a classification and accompanying suffix for such data and electronic record.

Each entity of the Presidency and Public Services Institution shall assign access control codes to positions in the Organogram of such Institutions and each access control code shall determine the level of classified document holders of such position can generate and holders of such position can access.

Defence and Security refers to all data and electronic content which contain information which may or has the potential whether in any material particular or not to

i. Cause exceptionally grave damage to the effectiveness or security of law enforcement agents or to the continuing effectiveness of extremely valuable security or intelligence operations
ii. Cause serious damage to the operational effectiveness or security of law enforcement agents or the continuing effectiveness of highly valuable security or intelligence operations
iii. Cause damage to the operational effectiveness or security of law enforcement agents or the effectiveness of valuable security or intelligence operations
iv. Make it more difficult to maintain the operational effectiveness or security of Republic of Ghana or allied forces

Diplomacy refers to all data and electronic content which contain information which may or has the potential whether in any material particular or not to

i. Directly threaten the internal stability of the Republic of Ghana;
ii. Cause exceptionally grave damage to relations with Organisation and Unions including the United Nations and its affiliates, African Union and its affiliates, ECOWAS and its affiliates and Countries with the Republic of Ghana has diplomatic relations and ties
iii. Raise international tension in respect of matters accessed without authorisation from data and electronic records marked Top Secret, Secret, Confidential, Restricted or protected;
iv. seriously damage relations with Countries with which the Republic of Ghana has diplomatic relations and ties and are in respect of matters accessed without authorisation from data and electronic records marked Top Secret, Secret, Confidential, Restricted or Protected
v. Materially damage diplomatic relations and are in respect of matters accessed without authorisation from data and electronic records marked Top Secret, Secret,

Confidential, Restricted or protected resulting in the release from such countries of formal protest or other sanctions or rebuke.

vi. Affect diplomatic relations adversely and are in respect of matters accessed without authorisation from data and electronic records marked Top Secret, Secret, Confidential, Restricted or protected resulting in the release from such countries of formal protest or other sanctions or rebuke.

Economy and Finances refers to all data and electronic content which contain information which may or has the potential whether in any material particular or not to

i. Cause severe long-term damage to the economy of the Republic of Ghana
ii. Cause substantial material damage to national finances or economic and commercial interests
iii. Work substantially against national finances or economic and commercial interests;
iv. Substantially undermine the financial viability of major State Enterprises, businesses which benefit from or financed in any manner from any proceeds of the Consolidated Fund at any time regardless of the amount of period of such funding, business in which the Republic has any investments, businesses which information and operation constitutes part of the critical infrastructure
v. Cause financial loss or loss of earning potential or to facilitate improper gain or advantage for individuals or companies in any manner that would constitute the basis of inquiry on legal matters impacting on insider trading or information or abuse of office
vi. Cause financial loss or loss of earning potential, or to facilitate improper gain for individuals or companies in any manner that would constitute the basis of inquiry on legal matters impacting on insider trading or information or abuse of office
vii. Give an unfair advantage for individuals or companies in any manner that would constitute the basis of inquiry on legal matters impacting on insider trading or information or abuse of office

Life and Liberty refers to all data and electronic content which contain information which may or has the potential whether in any material particular or not to

i. Lead directly to widespread loss of life
ii. Threaten life directly, or seriously prejudice public order, or individual security or liberty
iii. Prejudice individual security or liberty
iv. Cause substantial distress to individuals
v. Cause distress to individuals

Crime refers to all data and electronic content which contain information which may or has the potential whether in any material particular or not to

i. Impede the investigation or
ii. facilitate the commission of serious crime
iii. Prejudice the detection or monitoring of crime
iv. Prejudice the investigation or facilitate the commission of crime

Policy refers to all data and electronic content which contain information which may or has the potential whether in any material particular or not to

i. Undermine, or otherwise disrupt in any manner national security, national interest, public health and safety related operations;

ii. Seriously impede the development or operation of major government policies and policy initiatives without limitations of policies relating to technology and digital policies and implementation
iii. Undermine the proper management of the public sector and its operations;
iv. Impede the effective development or operation of government policies;
v. Disadvantage government in policy or commercial negotiations with International and Regional organisations, Donor countries, countries with such Ghana has bilateral relations with and entities whether private, public or third country owned.
vi. Disadvantage government in the development and constructive approach in commercial or policy negotiations with International and Regional organisations, Donor countries, countries with such Ghana has bilateral relations with and entities whether private, public or third country owned.

Information refers to all data and electronic content which contain information which may or has the potential whether in any material particular or not to

i. Breach proper undertakings to maintain the confidence of information provided by third parties;
ii. Breach statutory restrictions on disclosure of information
iii. Breach proper undertakings to maintain the confidence of information provided by third parties;
iv. Breach statutory restrictions on the disclosure of information

Chief Information Officer Duties

Every Chief Information Officer shall ensure that in respect of all documents marked as multiple, interoperable access control rights are enabled to persons holding officers in relevant and assigned MDAs and Arms of Government to be capable of accessing same in accordance with law.

Every Chief Information Officer shall ensure that in respect of all documents which are marked as Open Data category data and electronic records, same are content verified by the Chief Information Officer and thereafter placed on the Open Data content website in the appropriate category in consultation with the NITA Department responsible for Security.

Every Chief Information Officer shall be responsible for monitoring compliance with this Regulations, Electronics Transactions Acts, National Information Technology Act, Ghana Technology related Policies and Directives, Directives, Standards, Information Reporting and Requests from NITA, the Minister with responsibility for Communications and such additional duties which may be imposed on same in the course of the discharge of their duties.

Access Control User Obligations

It shall be the duty of every officer holding any position for which access control rights, duties and obligations are imposed under the provisions of these Regulations to seek clarification from the Chief Information Officer with responsibility for such MDA and Arm of Government where in doubt.

Offences

Any person who attempt to access or access data and electronic records beyond that authorised by such persons access control code commits an offence and is liable upon

conviction to a fine of not less than xxx or more than penalty points or not more than xxx years imprisonment or both.

Any person who without lawful authority the proof which shall lie on him, attempts or grants access or any person knowing that such person is not authorised by virtue of the access control level of such person or non-availability of any access control commits an offence and is liable on conviction a fine of not less than xxx or more than penalty points or not more than xxx years imprisonment or both.

Any persons who does not have an access control code who attempt to access, or accesses data and electronic records commits an offence and is liable upon conviction to a fine of not less than xxx or more than penalty points or not more than xxx years imprisonment or both.

Any person who without lawful authorisation attempts to access or access data and electronic records relating to

i. Defence& Security national interest area suffix marked DAS
ii. Diplomacy national interest area suffix marked DIP
iii. Economy & Finances national interest area suffix marked EAF
iv. Life & Liberty national interest area suffix marked LAL
v. Crime national interest area suffix marked CRM
vi. Policy national interest area suffix marked PLY
vii. Information areas suffix marked IFM

the proof of such access or attempt which shall lie on the Republic commits an office and shall be liable upon summary trial and conviction on conviction to a fine of not less than xxx or more than penalty points or not more than xxx years imprisonment or both.

Any person who access control rights, obligations and impositions are made under these Regulations and who fails to seek clarification on any matter which such officer is in doubt commits an offence and is liable on conviction of a fine of not less than xxx or more than penalty points or not more than xxx years imprisonment or both.
Any person who access control rights, obligations and impositions are made under these Regulations and who fails to so comply commits an offence and is liable on conviction to a fine of not less than xxx or more than penalty points or not more than xxx years imprisonment or both.

Any person who makes any unauthorized disclosure, alteration, or destruction of data and electronic record commits an offence and is liable on conviction to a fine of not less than xxx or more than penalty points or not more than xxx years imprisonment or both.

12(1) NITA may provide additional classification levels for protected computers, protected systems and critical databases.

(2) Depending on the classification levels of protected computers, protected systems and critical databases, the Minister may give directives to entity of the Presidency and/or Public Service Institution as to their location and hosting.

NITA shall in respect of the classification levels issue the technology framework standards, designs and procedures to ensure security compliance and clearance which each classified level and the reporting regime of any detections breaches, unauthorized intrusions,

assessment areas to reported in respect of any breaches, unauthorized instruction and such other matters which NITA may deem fit.

PART EIGHT: .gh DOMAIN NAME

All entities of the Presidency and Public Services Institution shall exclusively use the.gh country in combination with such .gov or public service institution abbreviation and ecosystem name and same shall be controlled, managed, allocated, distributed and renewed by NITA

No officers or employee of any entities of the Presidency and Public Services Institution shall use any email or register any URL address for the conduct of and in the performance of its statutory and constitutional functions any generic or country domain name other that the country domain name .gh

NITA shall be responsible for management of the email servers and mail box setting, filtering, security, backup and disaster controls of all issues relating to .gh domain matters of MDAs and Arms of Government.

No MDA and Arm of Government shall host any email content or server on any cloud or server which is not managed and operated by NITA and external to the geographic location of Ghana

All .gh domain name security issues and procedures relating to disaster recovery and management protocols and to geographical locations of such security related matters not designated for public use or access by unauthorised persons shall remain Top Secret issues and the provisions relating to data classification shall apply mutatis mutandis to same.

NITA shall ensure that ‘gh domain name shall be able to function and operate and survive actions of hostile local and foreign actions and actors howsoever arising and shall be responsible for developing security protocols and actions for compliance by all entities of the Presidency and Public Services Institutions in relation thereto.

All entities of the Presidency and Public Services Institutions shall through their Chief Information Officers notify NITA of all downtime and Service Level Agreement complaints received and unresolved, inconsistency and violations within 24 hours of receipt or events relating to the .gh hosting user experience

NITA shall in line with the SLA between entities of the Presidency and Public Services Institution take steps to resolve the matter failing which such entities of the Presidency and Public Services Institution shall through their Chief Information Officer escalate the complaint for the attention of the Minister of Communication and National and Cyber Security Committee.

The Minister of Communication & Digitalisation and the National and Cyber Security Authority shall within 24 hours of notification escalate the matter to the relevant first point of

National Security and thereafter the classified process for resolving such issues that assume responsibility for investigations, monitoring, resolution and related matters.

The notification regime shall be by electronic ticketing and electronic ticketing escalation in addition to such other additional technical processes designed by NITA in line with policy compliance and the discharge of its functions under the Act and Regulations thereunder.

NITA shall draw up the Service Level Agreement between NITA and Private Sector registered users wheresoever located whether legal, natural, sovereign entities or persons to which NITA provides any hosting services.

NITA shall until the incorporation of such Non-Profit Association and management of the .gh is transferred to same pursuant to the provisions of the Act draw up the application and registration and renewal process for use of third parties of the .gh domain name and the fees and applicable charges related thereon.

Upon the incorporation of the Non Profit Association and management of the .gh transfer to same, NITA shall continue be the registrar of the .gh for entities of the Presidency and Public Services Institution and in that regard such incorporated Association shall ensure compliance with these Regulations and in the management of the .gh domain name.

PART NINE: INDUSTRY FORUM

Every Inter-Regulatory cooperation group shall have a standing Committee which shall meet at such period set by the Group, or such period directed by the Minister pursuant to a request received by the Minister from NITA, any member of the Inter-Regulatory Cooperation group, any Petition from any Industry Forum under NCA, NITA or NITA recognised Industry Forum setting out good cause for the summoning of a meeting of any Standing Committee

NITA shall be the convenor of meetings between recognised Industry Fora groups under the ETA and ECA seeking implementation of the policy initiative of the Digital Innovation Fund for Underserved & Marginalised Communities and shall pursuant thereto be the convenor of meetings between NITA, GIFEC, NCA and such Industry Forum groups and advocates.

NITA shall be the convenor of meetings between recognised Industry Fora groups under the ETA and ECA seeking implementation of the policy initiative of in all matters relating to the setting up of Digital Educational Laboratories in educational Institutions and Underserved & Marginalised Communities and shall pursuant thereto be the convenor of meetings between NITA, GIFEC, NCA and such Industry Forum groups and advocates.

PART TEN: COMPLAINTS AND DISPUTE PROCEDURES

Consumer Complaints Unit

There is hereby established under these Regulations a Consumer Complaint Unit which shall be responsible for receiving all complaints from:

Parties to any ecommerce transaction in respect of services or products

a) originating from Ghana
b) :delivered to any resident in Ghana
c) Terminating and/or rendered in Ghana

d) Involving any digital based presentation made by any resident in Ghana intended to induce any party to enter into any financial transaction or financial commitment to such resident

Rules of the Technology Appeals Tribunal
NITA shall in consultation with the Ghana Arbitration Centre and the Judicial Service of Ghana develop the rules and procedure for receiving complaints and adjudicating on disputes on decisions of the Agency.

The terms and conditions of the Rules for receiving complaints and adjudicating on appeals against the decisions of the Agency shall be published in the Ghana ICT Gazette and constitute the binding Rules of Mediation and/or Arbitration.

Technology Appeals Tribunal
There is established an appeal tribunal to be called the Technology Appeals Tribunal which shall be convened on an ad-hoc basis to consider appeals against
(a) decisions or orders made by the NITA or
(b) to review a particular matter under a licence, the ETA Act or Regulations, and·
(c) decisions of the Consumer Complaints Unit set up under these Regulation.

Rules of the Technology Appeals Tribunal
Rules of The Technology Appeals Tribunal the Technology Appeals Tribunal shall be developed by a Five member Committee appointed by the Minister from nomination provided by the Ghana Arbitration Centre and the Judicial Service.

The Committee shall within a period not exceeding 90 days from the date of their appointment and composition submit to the Minister for approval, modification, amendment and other considerations, the proposed Rules of the Technology Appeals Tribunal.

The Minister shall upon consideration of the proposed Rule finalise in collaboration with the Board the Rules of the Technology Appeals Tribunal which shall be published in the Ghana ICT Gazette and shall constitute the Rules of the Tribunal.

The Rules of the Appeal Tribunal as published in the Ghana ICT Gazette shall be as part of the terms and conditions for the processing of issue of licenses and/or approval of notification, registration and certification processes be deemed to be incorporated by all NITA :

a) approved VAS with NITA approved Notification, Registration and/or Certification
b) licensed entities holders

as their dispute resolution process which shall be first accepted by users of their services as a precondition for access and use by their customer

The Board shall by Gazette publication after approval by Parliament, set out all rules and procedures inclusive of filing fees, service procedures, hearing procedures, reading of Rulings and enforcement of decision of the Tribunal.

Composition of the Tribunal
The members of the Tribunal shall be appointed by the chair- person of the Public Services Commission and shall consist of

(a) a chairperson who is either a retired Justice of the Superior Court or a lawyer of at least fifteen years standing who has experience in telecommunication law, policy, regulations or arbitration, and
(b) two other members with knowledge of and experience in the electronic communications industry, electronic engineering, law, economics or business or public administration.

The Public Services Commission shall appoint a registrar and other staff necessary for the smooth operations of the Tribunal.

The expenses of the Tribunal shall be paid out of income derived by the Agency and shall be part of the annual budget of the Agency. Rules of procedure of the Tribunal

Right of appeal
A person affected by a decision of the Agency or Consumer Complaints Unit may appeal against it by sending a notice of appeal to the Tribunal in accordance with the rules of procedure of the Tribunal.
The notice of appeal must be sent within twenty-eight days after the date the decision that is being appealed against is announced or received.
The appellant shall set out in the notice of appeal
(a) the decision appealed against,
(b) the provision under which the decision appealed against was taken, and
(c) the grounds of appeal.
Within one month after receipt of a notice of appeal the Tribunal shall be convened to consider the appeal.

Decisions of the Tribunal
The Tribunal, after hearing the appeal may
(a) quash the decision,
(b) allow the appeal in whole or in part, or
(c) dismiss the appeal and confirm the decision of the Agency.
If the Tribunal allows the appeal in part, it may vary the decision of the Agency in any manner and subject to any conditions or limitations that it considers appropriate to impose.
The Tribunal may take into consideration any submissions filed by a person acting as a friend of the Tribunal in reaching a decision on an appeal brought before it.
A decision of the Tribunal shall have the same effect as a judgement of the High Court.

Appeals against the decisions of the Tribunal
(1) A party dissatisfied with a decision of the Tribunal may appeal to the Court of Appeal
(2) An appeal under this section shall relate only to a point of law arising from the decision of the Tribunal.
(3) An appeal shall be made within ninety days after the decision of the Tribunal and there shall be no extension of time.

Technology Appeal Platform

All process for service under the Rules shall be by application of technology and there shall be no mandatory requirement for physical filing of document or physical presence by the parties in any Hearing Procedures under this part of the regulations.

All hearings under the Rules shall be along secured and encrypted processes

The Appeals Hearing List shall constitute Public Records and shall be published in the Ghana ICT Gazette and on the website of the Agency.

The Rulings of the Tribunal shall constitute Public Records and except for the parties who shall be entitled to free copies, same shall be available to any requesting party by the payment of prescribed fees as published in the Gazette

Rulings of the Tribunal and all processes shall be signed using such relevant and applicable technology which are secured, capable of authentication and detection of any alterations made thereafter by any unauthorised persons

Technology Applications Communication and related matters

All applications, submitted documents shall be signed using such relevant and applicable technology which are secured, capable of authentication and detection of any alterations made thereafter by any unauthorised persons

All attachments of records and documents relied upon by any applicant as part of the application or correspondence process shall be submitted in pdf format or such other prescribed format set out in the ICT Gazette publications of NITA

All attachments of pictures and/or images submitted as standalone records and documents relied upon by any applicant as part of the application or correspondence process shall be submitted in PNG, JPEG, GIF, TIFF, and BMP format or such other prescribed format set out in the ICT Gazette publications of NITA

PART TEN: AFRICAN CONTINENTAL FREE TRADE

NITA shall be responsible for monitoring and implementing the provisions of the Digital Economy Policy in all matters related to leveraging on technology within the context of the African Continental Free Trade Agreement between Sovereign African Countries.

NITA shall be responsible for monitoring and implementing the provisions of the Digital Economy Policy in promoting and facilitating the growth and development of a national technology ecosystem to enable the private sector leverage on technology within the context of the African Continental Free Trade Agreement.

NITA shall provide access and services relating to Data Centre activities for Sovereign African Countries seeking to leverage on Technology in any aspect of the African Continental Free Trade Agreement.

NITA shall be responsible for ownership of the Data Centre on which data of all MDAs and Arms of Government are store upon except that NITA shall be entitled to engage third parties meeting security and related standards.

No entity can be appointment, engaged or manage any Data Centre of NITA or any Data Centre on which information of any Arms of Government, MDA or Statutory Bodies is hosted or store of which such entity is :

(i) subject to disclosure requirements of any third country, is under the control, directions or regulatory authority of any 3rd Country or third entity
(ii) under any disclosure or reporting requirements/obligation to any 3rd country or third entity in respect of any matter, data or information of Data Centre contents in which Government of Ghana, MDAs and Statutory Bodies information is hosted or stored
(iii) under the direction or control of any third countries or laws of third countries giving such countries in respect of any activity which constitute part of works and services in managing Data Services in Ghana
(iv) under disclosure requirements howsoever arising of information and a duty to comply with sanctions of any country or entity hosting any data in the Data Centre

and any contract entered into with any such entity shall be deemed to be null, void and of no effect and the State shall not be liable or the determination any such agreement with any such 3rd Party.

Where after the commencement of this agreement any such Data Centre managing entity is not qualified to continue to manage the Data Centre, such Data Centre shall within a period not exceeding three (3) month provide evidence of steps taken enabling same to fulfil all the conditions of this agreement failing which the contract shall be deemed to be an unlawful contract and frustrated by the operation of force majeure being the passage by a Sovereign Country Parliament of a law forbid practices which managing entity is unable to secure a release from its third country or entity.

No entity shall be appointed to manage any Data Centre on which Government of Ghana data is held unless such entity demonstrate to NITA that it can comply with the provisions of this Law and the Laws of Ghana and meets the:

(i) security standards,
(ii) terms and conditions published in the Gazette relating to the Government of Ghana Centre, Rules, Terms and Conditions of Use, Management, Limitation on extent of liability and processing compliance requirements under the Data Protection Act, xxxx.
(iii) entities vetted standards and approved by National Security

Settlement of Disputes under this section shall be governed by the terms and conditions of the bilateral agreement signed between the Government of Ghana and the participating African Continental Free Trade Agreement country.

Commencement

22(1) This Regulation shall come into force effective …….. XXXXX 2022 or such other date that the Minister may by Gazette notification give notice of its coming into force.

SCHEDULE TO PART ONE

FORMS

SCHEDULE TO PART TWO
FORMS

SCHEDULE TO PART THREE
FORMS

SCHEDULE TO PART FOUR
FORMS

SCHEDULE TO PART FIVE
FORMS

SCHEDULE TO PART SIX
FORMS

SCHEDULE TO PART SEVEN
FORMS

SCHEDULE TO PART EIGHT
FORMS

SCHEDULE TO PART NINE
FORMS

SCHEDULE TO PART TEN
FORMS