

**REPUBLIC OF GHANA
MINISTRY OF COMMUNICATIONS & DIGITALISATION
eTRANSFORM GHANA PROJECTS (CR 6741-GH)**

**DEVELOPMENT OF REGULATIONS FOR THE NATIONAL
INFORMATION TECHNOLOGY AGENCY (NITA)**

Contract ID: eTP/RComp/1.6.3-GH-MOC-230670-CS-CQS

**NATIONAL INFORMATION TECHNOLOGY AGENCY (NITA)
SUBSIDIARY LEGISLATION**

Submitted by

Consult General

Contents

PART ONE: TECHNOLOGY POLICY IMPLEMENTATION OBLIGATIONS	- 6 -
1.0 Obligation of The Presidency and Public Services Institutions	- 6 -
2.0 NITA and PSIs Advertising Revenue.....	- 7 -
3.0 NITA NOTIFIED DEEV	- 8 -
4.0 NITA REGISTERED DEEV	- 9 -
5.0 Scope of Local DEEV Activities.....	- 10 -
6.0 NITA CERTIFIED DEEV	- 13 -
7.0 NITA AfCFTA Scope of Works.....	- 13 -
8.0 Multiple use Resident selection base Procurement.....	- 14 -
9.0 Public Services Institutions Providing Utility Services	- 15 -
10.0 Entities of the Presidency and Public Services Institutions Revenue Sharing and Advertising Bids	- 16 -
11.0 NITA Procurement Support and Collaboration Responsibilities	- 16 -
12.0 NITA, PPA and Multiple Local DEEV bids.....	- 17 -
13. BENEFITS OF NOTIFICATION, REGISTRATION AND CERTIFICATION ..	- 17 -
14.0 Inter-Regulatory Cooperation	- 17 -
15.0 ENTITIES OF THE PRESIDENCY AND PUBLIC SERVICES INSTITUTIONS INTERSECTORIAL COMMITTEE	- 18 -
16.0 Consumer Protection Complaints	- 18 -
17.0 Registration of eCommerce Providers & Entities.....	- 19 -
18(1) Benefit of Consumer Association Registration.....	- 19 -
19(1) Prohibition of exclusion of Ghana law	- 19 -
20(1) Bilateral Agreements under AfCFTA & Dispute Resolutions	- 20 -
21(1) Consumer Rights Publication	- 20 -
22(1) Foreign DEEV entities and Ghanaian Resident Consumers	- 20 -
23(1) Consumer Complaints Technology Platform	- 21 -
24.0 Arbitration in Digital Disputes	- 21 -
25.0 Business Sector Ecosystem	- 22 -
26.0 Consumer/ Users of Technology Ecosystem	- 22 -
27.0 Universal Service and Universal Access	- 23 -
28.0 Public Digital Records and Archiving.....	- 25 -

29.0	DATA BASE AND BIG DATA	- 25 -
30.0	INTER-REGULATORY COOPERATION.....	- 26 -
31.0	NON-INFRASTRUCTURE BASED DIGITAL ENABLED	
	ENTREPRENEURIAL VEHICLES –	- 27 -
31.0	Forms.	- 27 -
32.0	Fees.....	- 27 -
	PART TWO NOTIFICATION, REGISTRATION & CERTIFICATION REGIME	- 28 -
33.0	DEEV and NITA Status.	- 28 -
34.0	Continuing Obligation under Notification, Registration and Certification status.-	
30 -		
36.0	Suitable guarantee.	- 31 -
37.0	Application for recognition of Foreign DEEV	- 31 -
38.0	Implied conditions.....	- 32 -
39.0	Replacement of NITA Status Document.....	- 33 -
40.0	Transfer or assignment of licence.....	- 33 -
41.0	Partnerships in NITA recognised Status.....	- 33 -
42.0	Register of NITA recognised Status.	- 34 -
43.0	NITA recognised Status.....	- 34 -
44.0	Obligations of Providers.....	- 34 -
45.0	Contents of Provider disclosure record.	- 34 -
	PROVISION RELATING TO COMPLIANCE AUDITS	- 35 -
46.	Qualification and registration of compliance auditors.	- 35 -
47.	Procedure for annual compliance audit.....	- 35 -
48.	Auditor's Technology report.....	- 36 -
49.	Additional compliance audits.....	- 36 -
50.	Consequence of failing annual compliance audit.	- 36 -
51.	Criteria for recognition of foreign DEEV.....	- 37 -
	NOTIFICATION, REGISTRATION & CERTIFICATION ENTITIES DIGITAL RECORDS	
	OBLIGATIONS.....	- 37 -
52.	Record-keeping.	- 37 -
53.	Books of account.	- 38 -
54.	Retention and custody of records.	- 38 -
	TECHNICAL COMPONENTS COMPLIANCE	- 38 -
55.	Technical components.	- 38 -
56.	Review of software, etc.	- 39 -
	DATA PROCESSING ADDITIONAL OBLIGATIONS	- 39 -

57.	Data protection.....	- 39 -
58.	Liquidation and Assignment of Statutory Records:	- 40 -
	ISSUE OF GUIDELINES, AUDITS, DIRECTIVES AND ORDERS	- 40 -
59	Directives and administrative orders.....	- 40 -
60.	Guidelines.	- 40 -
	PART THREE: OPEN DATA AND THE STATE	- 40 -
61.	Open Data	- 40 -
62.	NITA and Public Records and Archives Administration Department	- 41 -
63.	PRIVATE SECTOR OPEN DATA.....	- 41 -
64.	Information Communications Technology Gazette -Open Data	- 41 -
65.	Private Sector Open Data Operators	- 42 -
	PART FOUR: NETWORK SECURITY	- 42 -
66.	Network and Security	- 42 -
67.	Compliance Audit	- 43 -
	PART FIVE: CYBER SECURITY.....	- 43 -
68.	Cyber Security.....	- 43 -
69.	Chief Information Officer	- 44 -
70.	Inspection and investigation.....	- 44 -
	PART SIX : DIGITAL RECORDS CLASSIFICATIONS REGIMES	- 45 -
71.	Classification levels	- 45 -
72.	Hosting of GoG Entity Data	- 45 -
73.	Top Secret Level.....	- 46 -
74.	Secret Level	- 46 -
75.	Restricted and Protected Level.....	- 46 -
76.	Sector Specific Level.....	- 46 -
77.	Interoperable and Multiple Level.....	- 46 -
78.	Open Data Level.....	- 46 -
79.	Institutions Further classification Obligations.....	- 47 -
80.	Chief Information Officer Duties	- 49 -
81.	Access Control User Obligations	- 49 -
	PART SEVEN:	- 50 -
82.	AFRICAN CONTINENTAL FREE TRADE AGREEMENT	- 50 -
	PART EIGHT	- 51 -
	Regulation and Competition	- 51 -
83.	Regulatory Market	- 51 -
84.	Scope of Law	- 52 -

86.	Competition Manipulation	- 52 -
87.	Market Dominance	- 53 -
88.	Abuse of Market Dominance	- 53 -
89.	Prevention of Market dislocation.....	- 54 -
	Local Business Protection.....	- 54 -
90.	Prohibited Conduct	- 54 -
91.	Investigative Powers	- 55 -
92.	Investigation Findings and Sanctions	- 57 -
93.	Foreign Entities & National Interest	- 58 -
94.	Public Service Institutions (PSI)Applications	- 58 -
95.	PSI Service Levels Agreement Minimum Standards.....	- 58 -
96.	PSI Service Levels Agreement Minimum Content.....	- 58 -
97.	NITA Notification, Registered and/ or Certification Local DEEV Service Levels Agreement Minimum Standards	- 59 -
98.	NITA notification Local DEEV Service Levels Agreement Minimum Content	- 59 -
99.	NITA recognised Foreign Incorporated DEEV Service Levels Agreement Minimum Standards	- 60 -
100.	NITA recognised Foreign Incorporated DEEV Service Levels Agreement Minimum Content	- 60 -
101	Forms.	- 61 -
102.	Fees.	- 61 -
232.	Interpretation.....	- 61 -
233.	Commencement	- 68 -
	FIRST SCHEDULE	- 68 -
	i. FIRST SCHEDULE PART ONE FORM 1	- 68 -
	ii. FIRST SCHEDULE PART ONE FORM 1A	- 72 -
	iii. FIRST SCHEDULE FEES	- 74 -
	SECOND SCHEDULE TO PART THREE – OPEN DATA CONTRIBUTORS FORMS	- 75 -
	iv. SECOND SCHEDULE FEES	- 78 -
	THIRD SCHEDULE TO PART FOUR - DIGITAL FORENSIC AND INTERCEPTION	Error!
	Bookmark not defined.	
	v. THIRD SCHEDULE FEES	Error! Bookmark not defined.
	FOURTH SCHEDULE PART FIVE FORM 1	- 79 -
	FIFTH SCHEDULE TO PART SIX – CYBER SECURITY	- 81 -
	SIXTH SCHEDULE – PART SEVENTH TECHNICAL COMPONENTS	- 84 -
	SEVENTH SCHEDULE TO PART EIGHT– CLASSIFICATION RETURNS FORMS	Error!
	Bookmark not defined.	

**NATIONAL INFORMATION TECHNOLOGY AGENCY REGULATIONS 2023,
(LI.....)**

IN EXERCISE of the powers conferred on the Minister for Communications by section 3(1)(b) and 28 of the National Information Technology Act, 2008 Act 771 these Regulations are made thisday of2023

PART ONE: TECHNOLOGY POLICY IMPLEMENTATION OBLIGATIONS

1.0 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 Institutions (PSIs) 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 of 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.

(7) 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.

(8) Except for National Security classified contracts all entities of the Presidency and 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.

(9) 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.

2.0 NITA and PSIs Advertising Revenue

(1) 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 advertising 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.

(2) 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.

(3) NITA shall be responsible for managing all advertising revenue attributable to the Governments of other participating Africa Continental Free Trade Agreement (AfCFTA) countries arising from NITA hosted Data Centre platforms and activities managed by NITA pursuant to contract and/or bilateral agreements.

(4) 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.

(5) 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.

(6) 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.

(7) 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.

3.0 NITA NOTIFIED DEEV

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

(1) Entities which have provided NITA with notification as DEEV 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.

(2) To Entities of the Presidency and /or Public Services Institutions:

(3) 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 seeks to have NITA perform technical advisory services to such Regulators in technology related disputes between the entity and such Regulators.

(4) Every NITA approved DEEV 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) months after the annual notification period whichever shall last occur.

(5) 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 Regulatory Authority, Agency, Commission under the provisions of the 1992 Constitution and/or created by Statute.

(7) The Rights and Incentives of DEEV entities with NITA issued notification, registration and certification Certificates shall be prescribed by Gazette Publication and shall be consistent with:

- i. the National ICT Policy, Strategy and Action Plan
- ii. progressively deepening the growth of the Local DEEV sector and
- iii. facilitating Inter-Regulatory cooperation in areas engaged in by DEEV with approved NITA notification certificate holders.

(8) It is mandatory for every NITA Notified Certificate Local DEEV entity holder 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.

(9) It is mandatory for every NITA Notified Certificate Local DEEV entity holder 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 DEEV is a holder of a Notified NITA issued certificate or that same has not expired and/or has been renewed.

(10) Anyone who 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 shall be deemed to be making a dishonest representation without lawful excuse.

(11) No NITA Notified Certificate Local DEEV 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.

(12) No Foreign DEEV 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.

(13) 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.

4.0 NITA REGISTERED DEEV

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

(2) Entities Registered and approved by NITA as Registered DEEV 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.

- (3) Every NITA Registered DEEV 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.
- (4) On approval of an application for Registration, the applicant shall be required to pay the prescribed statutory fee for the prescribed area for Registration.
- (5) 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.
- (6) The Rights and Incentives of DEEV 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.
- (7) Every NITA Registered Certificate Local DEEV 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.
- (8) Any Local DEEV entity holding the status of a NITA Registered entity not in good standing that 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 DEEV is a NITA Registered entity shall be deemed to be making a dishonest representation without lawful excuse..

5.0 Scope of Local DEEV Activities

(1) No Local DEEV 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 DEEV and be issued with a NITA Registered Entity Certificate and is not in default of renewal.

(2) No Local DEEV 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 DEEV and be issued with a NITA Certified Entity Certificate and is not in default of renewal.

(3) No Foreign DEEV shall provide services or solutions on any PSI 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 PSI 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 approved.
- 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 DEEV 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 its national and sovereign interests.

(4) No Local DEEV 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 DEEV and be issued with a NITA Registered Entity Certificate and is not in default of renewal.

(5) No Foreign DEEV 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 DEEV:

- 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 DEEV 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 its national and sovereign interests

(6) No Foreign DEEV 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 DEEV:

- 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 DEEV 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 its national and sovereign interests

6.0 NITA CERTIFIED DEEV

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

(2) Entities approved by NITA as Certified DEEV 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.

(3) Every NITA Certified DEEV 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.

(4) On approval of an application for Certification, the applicant shall be required to pay the prescribed statutory fee for the prescribed 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.

(5) The Rights and Incentives of DEEV entities with NITA issued Certified Certificate holders shall be prescribed by Gazette Publication and shall incorporate all Policy prescribed NITA Certified activities under the National ICT Policy, Strategy and Action Plan.

(6) Gazette Publications shall progressively deepen the growth of Local DEEV NITA Certified certificate holders and promote Inter-Regulatory cooperation.

(7) It is mandatory for every NITA Certified Certificate Local DEEV entity holder in good standing to display on its digital information accessed by the public and in its Trade Circulars the status of its NITA Certified holding certificate and the date of expiration of same.

(8) It is mandatory for every NITA Certified Local DEEV entities holders not in good standing to remove every display its digital information accessed by the public and in its Trade Circulars any status which may represent or cause any reasonable 3rd Parties to believe that such Local DEEV is a holder of Certified type of NITA issued certificate or that same has not expired and/or has been renewed.

7.0 NITA & AfCFTA Scope of Works

(1) NITA shall be responsible for the issue of NITA certified status to Local Digital Enabled Entrepreneurial entities which register with NITA and which demonstrate to NITA that such Applications and Competence in technology related implementation solutions within the AfCFTA.

- (2) NITA certificate of recognition shall not be mandatory for any Local Digital Enabled Entrepreneurial Entity to conduct any technology related implementation solutions within the AfCFTA.
- (3) NITA shall be responsible for the issue of NITA registered status to Local Digital Enabled Entrepreneurial entities which register with NITA and which demonstrate to NITA that such Applications and Competence in technology related implementation solutions within the AfCFTA.
- (4) NITA certificate of registration shall not be mandatory for any Local Digital Enabled Entrepreneurial Entity to conduct any technology related implementation solutions within the AfCFTA.
- (5) NITA shall be responsible for the issue of NITA notification status to Local Digital Enabled Entrepreneurial entities which register with NITA and which demonstrate to NITA that such Applications and Competence in technology related implementation solutions within the AfCFTA.
- (6) NITA certificate of notification shall not be mandatory for any Local Digital Enabled Entrepreneurial Entity to conduct any technology related implementation solutions within the AfCFTA.
- (7) NITA shall in consultation with other countries within the AfCFTA determine modalities for the creation and development of an AfCFTA Applications Hosting Store and the terms and conditions of Applications hosting and downloading.

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

- (1) The Procurement Process for inviting multiple Local DEEV 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.
- (2) No MMDA shall process any application received from any Local DEEV entity under the Multiple use Resident selection-based procurement programme unless proof is provided that the Local DEEV:
- i. is registered with the Data Protection Commission
 - ii. has a Notification Certificate issued by NITA and valid at the time of response to the issuer bid request.
 - iii. Product has been evaluated and confirmed by NITA that the product meets the PSI platform security and other requirements.
 - iv. product is limited in use to access user information and related payments.
 - v. Product displays District and Municipal related By-laws and notices,
 - vi. product makes exclusive use of Open Data intended for public use and/or digital entrepreneurial growth.
 - vii. has no MMDA related data input features, data retention feature held on the systems of such multiple Local DEEV entity product, resident users may have the option to download such permitted records of the MMDAs on such user enable devices.
 - viii. product and/or service does not perform any functions which is reserved for NITA Registered and NITA Certified status holders.
 - ix. Product does not require payment for use by MMDAs or Users inconsistent with the provisions of these Regulations advertising revenue sharing and payment revenue percentage sharing.
 - x. products shall not have access monopoly rights to MMDA record interface inconsistent with the provisions of these Regulations.

(3) Multiple Local DEEV 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) meet 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 and
- (d) 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 used 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. enabling 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.

(4) Local DEEV 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 DEEV 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.

9.0 Public Services Institutions Providing Utility Services

(1) The Procurement Process for inviting multiple Local DEEV 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.

(2) Any Local DEEV entity applying to participate with multiple Local DEEV entity bid products shall provide evidence to the receiving Utility provider that:

- i. The Local DEEV is registered with the Data Protection Commission
- ii. The Local DEEV has a NITA Certified status issued by NITA and valid at the time of response to the issuer bid requested,

- iii. The Local DEEV 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

(3) Local NITA Certified DEEV 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 DEEV 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.

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

(1) 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.

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

11.0 NITA Procurement Support and Collaboration Responsibilities

(1) 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.

(2) 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 been provided with evidence by such entity of the Presidency and/or Public Services Institutions that it has 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 PSI 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.

12.0 NITA, PPA and Multiple Local DEEV bids

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

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

13. BENEFITS OF NOTIFICATION, REGISTRATION AND CERTIFICATION

(1) NITA shall in respect of DEEV which have their notification, registration and certifications approved by NITA:

- i. Compile a credible register for networking between Local DEEV 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 DEEV entities.

14.0 Inter-Regulatory Cooperation

(1) 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.

(2) 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.

(3) 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.

(4) 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.

(5) 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:

- (a) Particulars of each Inter-Regulatory Committee composition
- (b) Scope of Inter-Regulatory Committee discussions
- (c) Heading of Inter-Regulatory Committee discussions relating to Local DEEV Notification entities

- (d) Heading of Inter-Regulatory Committee discussions relating to Local DEEV Registration entities
- (e) Heading of Inter-Regulatory Committee discussions relating to Local DEEV Certification entities
- (f) Heading of Inter-Regulatory Committee discussions relating to NCA Industry Forum entities
- (g) 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
- (h) Conclusions of Inter-Regulatory Committee discussions
- (i) In-conclusive matters under of Inter-Regulatory Committee discussions
- (j) Deferred matters under the Inter-Regulatory Committee discussion
- (k) Matters which reasonably require Ministerial Directive

15.0 ENTITIES OF THE PRESIDENCY AND PUBLIC SERVICES INSTITUTIONS INTERSECTORIAL COMMITTEE

- (1) Entities of the Presidency and Public Services Institutions 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.
- (2) The Standing Committee shall be composed of four persons to be nominated as follows:
 - (a) one persons nominated by the Director-General of
 - i. NITA,
 - ii. NCA and
 - iii. GIFEC
 - (b) one person nominated by the Minister who shall preside over the meetings of the Standing Committee.
- (3) 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.
- (4) 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.
- (5) 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.

16.0 Consumer Protection Complaints

- (1) 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.

(2) 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.

17.0 Registration of eCommerce Providers & Entities

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

(2) Notwithstanding the non-compulsory requirement of Local, AfCFTA and Foreign eCommerce providing entities to register with any Consumer Protection Complaint Association, NITA shall have the right to receive complaints of consumers whose consumer protection rights have been violated and to investigate same

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

(4) NITA shall register eCommerce related Consumer Protection Complaint Associations

(5) Consumer Protection Complaints Associations shall give a digital Register of all registered members and shall make same publicly and digitally available at no cost to members of the Public on its digital interface accessible to members of the Public

18(1) Benefit of Consumer Association Registration

(a) 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.

(b) 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.

19(1) Prohibition of exclusion of Ghana law

(a) 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 effect where any aggrieved party commences any legal proceeding in the High Court in Ghana.

(b) 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 effect 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.

20(1) 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.

21(1) Consumer Rights Publication

- (a) The consumer rights of persons receiving digital services shall be published by the Minister in the ICT Gazette in consultation with NITA registered Technology focused Consumer Associations.
- (b) Without prejudice to the afore regulations both registered and unregistered Consumer Associations and the general public shall be entitled to respond to a publication by the Minister solicitating for views, suggestions and consumer right protection matters.
- (c) 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.
- (d) 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.
- (e) Entities engaged in eCommerce relating trading incorporated in Ghana or registered as External companies in Ghana shall be entitled to be registered as DEEV 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.

22(1) Foreign DEEV entities and Ghanaian Resident Consumers

- (a) Foreign DEEV entities which carry on a business in Ghana by leveraging on technology within the scope of section 335 of the Companies Act, xxxx shall ensure compliance with the provisions of the Companies Act and file a copy of their Registered status in Ghana with NITA.
- (b) Where any Foreign DEEV entity whose services are carried out by leveraging on technology incorporates as a Ghanaian company it shall register with the Ghana Investment Promotion Centre and file a copy of the registered status in Ghana with NITA and be exempt from any requirement to register as an external company under the Companies Act.
- (c) A Foreign DEEV entity shall be deemed to carry on a business in Ghana where it provides services to any resident in Ghana leveraging on technology in consideration

for any amount and the nature of such activities is consistent with that of similar entities operating business in Ghana.

- (d) The Minister may from time to time and for the avoidance of doubt, publish in the electronic Gazette the name of Foreign DEEV entities which are deemed to be providing services to residents in Ghana and such Foreign DEEV entities shall ensure that within a period of 180 days, they comply with the provisions of the Companies Code, relevant laws relating to investment in Ghana and provide evidence of their compliance with NITA.
- (e) Foreign DEEV entities shall include without limitation entities engaged in social media related activities in which data subjects resident in Ghana is processed

23(1) Consumer Complaints Technology Platform

- (a) The Consumer Protection Complaints Associations under which NITA provides Regulatory oversight shall register their Consumer Complaints conflict resolution procedures with NITA.
- (b) 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.
- (c) Consumer Protection Complaint Association conflict resolution procedures shall be binding between eCommerce which associate with such Registered Associations and consumers of such eCommerce transactions.
- (d) Consumer Protection Complaint Associations shall as part of the registration with NITA provide details of Local, AfCFTA and Foreign eCommerce registered providers.

24.0 Arbitration in Digital Disputes

- (1) 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 DEEV with NITA approved Notification, Registration and/or Certification.
- (2) The Rules 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 DEEV with NITA approved Notification, Registration and/or Certification.
- (3) The Rules of Arbitration shall be published in the Ghana ICT Gazette and shall be incorporated by all NITA approved DEEV 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.

25.0 Business Sector Ecosystem

(1) 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 in respect of activities not related to Entities of the Presidency and Public Services Institutions 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

(2) In all interfaces with Entities of the Presidency and Public Services Institutions, Private Sector Business and users of technology shall adhere to NITA prescribed Government of Ghana prevailing and amended Ecosystem

1. standards,
2. protocols,
3. access control rights and
4. prohibitions of Entities of the Presidency and Public Services Institutions
5. all Cyber Security Protocols and
6. the use of approved authentication service provider

(3) 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 and shall adhere to all Government of Ghana Ecosystems rules, prohibitions, reporting standards, access control and all other relevant technology relating matters.

26.0 Consumer/ Users of Technology Ecosystem

(1) 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.

(2) In all digital platform interface with Entities of the Presidency and Public Services Institutions, consumers and users of technology shall adhere to

1. standards,

2. protocols,
3. access control rights and prohibits of Entities of the Presidency and
4. Public Services Institutions
5. all Cyber Security Protocols and
6. the use of approved authentication service providers of Entities of the Presidency and Public Services Institution

(3) 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.

27.0 Universal Service and Universal Access

(1) Universal Access scope and definitions shall be reviewed annually by NITA in consultation with the NCA and GIFEC and shall be published in the Gazette.

(2) Except in situations of force majeure, Universal Access shall include without limitation the undermentioned categories:

- i. Minimum download speeds that all infrastructure service providers shall ensure are always prevalent on the infrastructure network.
- ii. Minimum upload speeds that all infrastructure service providers shall ensure are prevalent on the infrastructure network at all times
- iii. Minimum downtimes that all infrastructure service providers shall ensure are prevalent on the infrastructure network at all times
- iv. Minimum resolution of technical and escalation of complaints affecting universal access standard breaches

(3) Universal Service scope and definition shall be reviewed annually by NITA in consultation with NCA and GIFEC and shall be published in the Gazette

(4) Except in situations of force majeure, Universal Service shall include without limitation the undermentioned services:

- i. The right to have working free Wi-Fi hotspots within a radius of at least one kilometre of every District and Metropolitan Assembly for log in by persons holding valid Ghana Cards who register for use of Free Wi-Fi Hotspots with such Districts and Metropolitan systems.
- ii. The right to have working technical support for persons with disability in the use of digital devices to access forms of Public Service Institutions and complete payments upon their production of a valid Ghana Card
- iii. The rights of at least one Digital Library in every District and/or Metropolitan Area to serve communities and accredited Junior High Secondary Schools and Senior High Secondary Schools
- iv. 3G broadband services at last mile where the ratio of the average monthly income of rural and last mile areas to the average monthly income of the monthly minimum wage is equal to or worse than 1:5 such rate shall apply to 5GB data of monthly usage in Districts and Metropolitan communities designated as deprived and/or marginalised communities as published in the Gazette.
- v. 3G broadband services in urban poor communities where the ratio of the average urban poor of more than sixty (60%) such community to the average monthly income of the monthly minimum wage is 1:2 for 5GB data of monthly usage on GIFEC provided Hotspots.

- vi. All Public Service Institutions shall have publicly advertised 1-800 Hot lines to which residents shall be entitled to make inquiries and follow up on application submitted to such Public Service Institutions during normal working hours
- (5) No Last Mile community in any District and/or Metropolitan area shall be designated as deprived and/or marginalised unless more than sixty (60%) such District and/or Metropolitan area created under the provisions of the 1992 Constitution is below the minimum wage.
- (6) 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
- (7) 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.
- (8) 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.
- (9) 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.
- (10) NITA and GIFEC shall provide technical support to Digital Libraries in Educational Institutions and MMDAs in rural communities, marginalised, deprived, and urban poor communities to progressively expand universal access and universal service availability to PSI digital services nationwide.
- (11) (1) 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
- (2) 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
- (12)** (1) 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

(2) 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.

28.0 Public Digital Records and Archiving

(1) 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.

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

(3) 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. do not suffer any degradation of data quality,
- ii. do not suffer any reliability or loss of content,
- iii. are capable of being accessed by always authorised users along the PSI ecosystem notwithstanding their encryption.
- iv. are incapable of being the subject matter of alteration and the integrity of the data remains unchanged.
- v. retains underlining software in which always assures data access by the PSI and data integrity.
- vi. retains source codes access relevant to access and use of legacy data without compromise to data integrity.

29.0 DATA BASE AND BIG DATA

(1) 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.

(2) 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

(3) 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) progressive development of the distributed ledger technology database for the Presidency and all other Public Services Institutions
- (d) prescription of standards, protocols, directives together with their corresponding data classification levels to maximise security of data, authentication of data, deepening of digital forensic ecosystem, minimisation of risk of wholesale data loss and/or compromise

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

(5) 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.

30.0 INTER-REGULATORY COOPERATION

(1) 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 DEEV sector competing with existing industry players regardless of such services and products being capable of single or multiple Regulatory areas services delivery.

(2) NITA shall be the facilitator of meetings between recognised Industry Fora groups under the ETA and ECA which seek publication of ICT Policy Guidelines, Regulatory Guidelines, Gazette Publication and/or the Regulatory engagement for the development of

- (a) Technical standards,
- (b) New Generation technology Regulatory practices, standards, license applications, prudential requirements

(3) NITA shall be the facilitator of meetings between recognised Industry Fora groups under the ETA and ECA for the settlement of initial complaints and facilitating discussions for the attainment of the goal of the National ICT Policy received from Local DEEV registered and/or certified entities:

- (a) in connection with Regulatory Bodies in the Financial, Insurance, Securities, Pension, Aviation, Shipping & Logistics and Utilities services
- (b) in respect of complaints of Regulatory Bodies unfair practices which deepen monopolistic and uncompetitive behaviour of existing industry players regardless of such services and products
- (c) challenges arising from single of multiple Regulatory Bodies requirements in respect products and services which have cut across multiple Regulatory Bodies and which Local DEEV challenge as inimical to the growth of the Local DEEV entities ecosystem.

31.0 NON-INFRASTRUCTURE BASED DIGITAL ENABLED ENTREPRENEURIAL VEHICLES –

(1) Local DEEV may engage in all such Digital Enabled Entrepreneurial Vehicles as is technologically feasible except:

- i. as prohibited by Law
- ii. the subject matter of Regulatory activity and the Local DEEV refuses to comply with Regulatory Guidance and Instructions
- iii. is a product for use on the Public Service Institutions infrastructure and such Local DEEV has the appropriate NITA Certification into relation to its application as a Registered, Certified or Notification providing entity and has a valid renewal certification

(2) No non-Ghana DEEV shall provide Digital Enabled Entrepreneurial Vehicles to any Public Service Institutions except same have been Registered, Certified, or provided Notification to NITA prior to such product entry or use and been issued with Certification from NITA and its annual renewal remaining valid at the time of the provision of such Digital Enabled Entrepreneurial Vehicles.

(3) For the purposes of these regulations Digital Enabled Entrepreneurial Vehicles include without limitation, technology related products and/or services, inclusive of designs, solutions, and all other technological feasible based products but exclusive of virtual infrastructure which is a regulatory matter for the NCA.

32.0 Forms.

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

33.0 Fees.

(1) The fees in the Schedule of these Regulations are prescribed for the purposes of these Regulations.

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

(3) The fees in respect of Notification, Registration, Certification by DEEV shall be classified into Startups, Entities in Business for less than 5 years, entities with less than 10 employees, entities with more than 10 employees but less than 50 employees, entities with more than 50 employees and the fees shall be graduated.

(4) The fees in respect of Critical Infrastructure operators shall be classified into Startups, Entities in Business for less than 5 years, entities with less than 10 employees, entities with more than 10 employees but less than 50 employees, entities with more than 50 employees and the fees shall be graduated.

(5) The fees in respect of Industry Forum shall be as prescribed under part One of these Regulations.

(6) The Fees shall be such as to promote the development of digitalisation within the Governmental and Private Sector ecosystem and shall not be prohibitive to sector growth,

prevention of the development of Startup, inimical to the promotion and development of competition within the technology ecosystem or inimical to the DEEV abilities to compete with foreign technology sector products, solutions, entities and research and development

PART TWO NOTIFICATION, REGISTRATION & CERTIFICATION REGIME

34.0 DEEV and NITA Status.

- (1) There shall be three types of NITA status for DEEV in respect of
 - (i) The categories of services and place of DEEV within the Government Digital Ecosystem and/or
 - (ii) the support that a DEEV may be entitled to receive from NITA

- (2) The DEEV types of NITA status are as follows:
 - (i) notification of operations within the private sector technology ecosystem
 - (ii) application for registration of operations within the private and public sector technology ecosystem
 - (iii) application for certification within the private and public sector technology ecosystem

The notification of operation shall be renewed bi-annually where a DEEV seek to benefit from NITA registered notification entities permitted operations and presence within the Government of Ghana digital ecosystem.

The application for Registration shall be renewed once every five years where a DEEV seeks to benefit from NITA registered entities permitted operations and presence within the Government of Ghana digital ecosystem.

The application for Certification shall be renewed once every ten years where a DEEV seeks to benefit from NITA certified entities permitted operations and presence within the Government of Ghana digital ecosystem and support by NITA in the African Continental Free Zone and under the African Continental Free Trade Agreement.

- (3) Every Notification of operations by a DEEV shall upon payment of the prescribed fee attract an annual NITA notification status certificate and digital badge and unless renewed shall expire.

Every Application for Registration by a DEEV shall upon payment of the prescribed fee attract an annual NITA Registration status certificate and digital badge and unless renewed shall expire.

Every Application for Certification by a DEEV shall upon payment of the prescribed fee attract an annual NITA Registration status certificate and digital badge and unless renewed shall expire.

- (4) Every notification of operations by a DEEV shall be accompanied by the following documents

- (i) Copy of the incorporation documents under the companies Act, Private Partnership Act, Trustees Incorporation Act or Business Names Act
- (ii) Prescribed Notification Fee

- (iii) Prescribed Annual Renewal Fee for the annual period commencing the date of the filing of the Notification
- (iv) Particulars of the business objects
- (v) Particulars of the area of business operations
- (vi) Particular of the business operations in last mile communities
- (vii) Particulars of business operations in marginalised and deprived communities
- (viii) Particulars of business operations in districts and municipalities
- (ix) Particulars of business operation in rural and urban communities
- (x) Particulars of areas in Ghana Digital Economy Policy and Strategy pillars, mature areas, focused areas and new technologies
- (xi) Particulars of Regulatory bodies of notifying entities

(5) An application for Registration shall be accompanied by the following documents

- (i) Copy of the incorporation documents under the companies Act, Private Partnership Act, Trustees Incorporation Act or Business Names Act
- (ii) Prescribed Notification Fee
- (iii) Prescribed Annual Renewal Fee for the annual period commencing the date of the filing of the Notification
- (iv) Particulars of the business objects
- (v) Particulars of the area of business operations
- (vi) Particular of the business operations in last mile communities
- (vii) Particulars of business operations in marginalised and deprived communities
- (viii) Particulars of business operations in districts and municipalities
- (ix) Particulars of business operation in rural and urban communities
- (x) Particulars of areas in Ghana Digital Economy Policy and Strategy pillars, mature areas, focused areas and new technologies
- (xi) Particulars of the business plan inclusive of details of the qualifications of the personnel intended to be employed, the proposed operating procedure and the various services to be provided and applicable fees.
- (xii) Provision of a suitable guarantee
- (xiii) Particulars of Regulatory bodies of notifying entities
- (xiv) 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
- (xv) that the directors shall bring any future such occurrences to the attention of the Agency any such occurrences.

An application for Certification shall be accompanied by the following documents

- (i) Copy of the incorporation documents under the companies Act, Private Partnership Act, Trustees Incorporation Act or Business Names Act
- (ii) Prescribed Notification Fee
- (iii) Prescribed Annual Renewal Fee for the annual period commencing the date of the filing of the Notification
- (iv) Particulars of the business objects
- (v) Particulars of the area of business operations
- (vi) Particular of the business operations in last mile communities

- (vii) Particulars of business operations in marginalised and deprived communities
- (viii) Particulars of business operations in districts and municipalities
- (ix) Particulars of business operation in rural and urban communities
- (x) Particulars of areas in Ghana Digital Economy Policy and Strategy pillars, mature areas, focused areas and new technologies
- (xi) Particulars of the business plan inclusive of details of the qualifications of the personnel intended to be employed, the proposed operating procedure and the various services to be provided and applicable fees.
- (xii) Provision of a suitable guarantee.
- (xiii) Particulars of Regulatory bodies of notifying entities
- (xiv) 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
- (xv) 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.

35.0 Continuing Obligation under Notification, Registration and Certification status.

(1) Every entity carrying a NITA Notification, Registration and/ or Certification status ensure that : -

- (a) all updates to information provided to NITA are updated within a period not exceeding 28 days of any changes of submitted information.
- (b) a report from a qualified compliance auditor certifying that the prescribed licensing, standards, and technical requirements have been satisfied during a period for which a renewal of the NITA status is required.
- (c) in the case of entities with Registration and/or Certification status, particulars of the compliance auditors and a copy of contract of engagement between the entity and the compliance auditor.
- (d) In the case of entities applying for Registration and/or Certification, Audited accounts for the periods for the date of incorporation to the year immediately preceding the application for Registration, Certification and/ or status renewal.

(2) The Agency may, on an application for Registration and/or Certification status 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.

(3) The Agency may on application for Registration and/or Certification status 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 have been withdrawn, without prejudice to a fresh application being made by the applicant.

36.0 Withdrawal of application for Registration and Certification status

(1) An application for Registration and/or Certification Status shall be deemed to be withdrawn and shall not be further proceeded with except by fresh application if -

- (a) the applicant fails to provide all particulars required for Registration and/or Certification Status within a period of three months from delivery of application; or
- (b) an application for the Registration and/or Certification Status is rejected.

37.0 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 Registration and/or Certification status category;
- (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 Status remains unless notification of withdrawal of guarantee is given to NITA, accepted by NITA upon provision of an acceptable alternative Guarantee in substitution therefor.

38.0 Application for recognition of Foreign DEEV

(1) The statutory Form prescribed in these regulations shall be used in an application for recognition by a Non-AfCFTA Foreign DEEV.

(2) Non-AfCFTA Foreign DEEV shall be entitled to apply for the Certification status with NITA and shall not engage in areas prescribed as Notification and Registration status areas..

(3) No application for Non-AfCFTA Foreign DEEV shall be approved for operation in classified and areas determined by the National Security as restricted areas in the national and security interest

No Foreign DEEV shall

- 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 can 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

39.0 Implied conditions.

(1) Every Registration and Certification status granted under these regulations shall contain the following minimum conditions that the holder shall: -

- (a) keep and maintain working capital reasonably sufficient to carry on or operate as set out in the submitted documents;
- (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 status recognition 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.

40.0 Replacement of NITA Status Document.

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

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

(3) An application for a replacement NITA recognised Status shall be accompanied by a statutory declaration to the effect that the NITA recognised Status issued to the applicant 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 NITA recognised Status, an additional police report addressed to the Agency and released to the applicant of the loss and the stage of investigation or otherwise by the police.

(4) An applicant shall surrender to the Agency the discovery of a lost original NITA recognised Status or recovery of any part of the destroyed NITA recognised Status.

41.0 Transfer or assignment of licence.

(1) A NITA recognised Status from the Agency shall not be transferable.

(2) A NITA recognised Status holder may upon application for approval by the Agency make provision for the transfer of its contractual obligations to its customers to another same category NITA recognised Status holding 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 NITA recognised Status 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 NITA recognised Status third parties with similar objects upon terms that the Agency may deem fit

42.0 Partnerships in NITA recognised Status.

(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 NITA recognised Status accordingly and allow the NITA recognised Status 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.

43.0 Register of NITA recognised Status.

- (1) The Agency shall keep and maintain a physical and electronic Register of NITA recognised Status holders in such form as it thinks fit.
- (2) Any person upon the payment of the prescribed fee may inspect the Register of NITA recognised Status holders and make copies of or take extracts from the Register.
- (3) The Agency shall publish a list of NITA recognised Status entities under these regulations in such form and manner as it may determine.

44.0 NITA recognised Status

No person shall carry on or operate, or hold himself out as NITA recognised Status holder unless

- (i) in the case of NITA notification, no rejection of notification has been issued to the entity within 180 days of its delivery notification
- (ii) in the case of NITA Registration and/or Certification, there is a valid Status in operation and renewal thereof

45.0 Obligations of Providers.

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

- (a) Particulars of all NITA recognised Status, 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 NITA recognised Status;
- (e) the repository used by the provider;
- (f) the procedure of independent verification of any licensed Provider

46.0 Contents of Provider disclosure record.

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

- (a) the business name and registered address of the NITA status holders;
- (b) the landline, mobile numbers and help desk facilities of the NITA status holders,;
- (c) the electronic mail, social media handles or other acceptable formats by

which the NITA status holders 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 status issued to the NITA status holders;
- (f) any restrictions imposed on the status issued to the NITA status holders, if any;
- (g) if the revocation of a NITA status holders which has taken effect, the fact of the revocation and its effective date;
- (h) if a NITA status holders has been surrendered, the fact of the surrender and its effective date;
- (i) if the NITA status holders 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 NITA status holders 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 NITA status holders suitable guarantee;
- (m) the total amount of all claims filed with the Agency for payment from the suitable guarantee filed by the NITA status holders;
- (n) a brief description of any limit known to the Agency and applicable to the NITA status holders liability or legal capacity to pay damages in tort or for breach of a duty under the Act or these Regulations;

(2) The NITA status holders shall furnish the Agency with any particulars required to be published in the NITA status holders' disclosure record.

PROVISION RELATING TO COMPLIANCE AUDITS

47.0 Qualification and registration of compliance auditors.

(1) An auditor qualified with the Agency determined ISO information technology standards consistent with the National ICT Policy and these Regulations shall be appointed by a NITA recognised Registration and/ or Certification status holder to prepare compliance audits under these regulations.

(2) A NITA recognised Registration and/ or Certification status holder 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 NITA recognised Registration and/ or Certification status holders' business or profit sharing 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.

48.0 Procedure for annual compliance audit.

(1) The NITA recognised Registration and/ or Certification status holder 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 NITA recognised Registration and/ or Certification status holder 's compliance as one of the following:

- (a) full compliance, if the licensed entity appears to comply with all the requirements of the National Information Communication Technology Policy and these Regulations;
- (b) substantial compliance, if the licensed entity appears generally to comply with the requirements of the National Information Communication Technology 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 National Information Communication Technology 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 NITA recognised Registration and/ or Certification status holder 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.

49.0 Auditor's Technology 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 Electronic Transactions 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.

50.0 Additional compliance audits.

The Agency may conduct unscheduled audits of a NITA recognised Registration and/ or Certification status holder at any time.

51.0 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 NITA recognised Registration and/ or Certification status holder 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 NITA recognised Registration and/ or Certification status holder

(b) the revocation or suspension of a NITA recognised Registration and/ or Certification status issued under these regulations.

(3) The Agency may impose sanctions on a NITA recognised Registration and/ or Certification status holder where such entity fails to comply with recommendations made by a compliance auditor in respect of findings of partial or non-compliance.

52.0 Criteria for recognition of foreign DEEV.

(1) A foreign DEEV shall satisfy the following requirements to qualify for NITA status recognition by the Agency:

(a) it shall be authorised under the laws in the country of incorporation to carry on or operate as a DEEV in that country;

(b) the DEEV must demonstrate a level of security equal to or more stringent than the level of security of NITA recognised Registration and/ or Certification status holder in Ghana;

(c) it has registered as an external agency in Ghana in compliance with the provisions of the companies Act;

(d) in respect of any business conducted in Ghana it shall comply with the standards and technical requirements under relevant law and applicable Regulators; and

(e) it shall comply with such other requirements as the Agency thinks fit.

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

NOTIFICATION, REGISTRATION & CERTIFICATION ENTITIES DIGITAL RECORDS OBLIGATIONS

53.0 Record-keeping.

(1) A holder of NITA Notification, Registration and/ or Certification status shall keep and maintain detailed written records documenting -

(a) the security measures taken to comply with the National ICT Policy and Strategy goals and these Regulations;

(b) if the NITA status holder 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 relevant laws and these Regulations.

(2) The records required under sub regulation (1) shall include evidence demonstrating that the NITA status holder has -

(a) confirmed the identification of the person named in a certificate that the NITA status holder 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 NITA status holder has issued; and
- (d) complied with all relevant legislation in issuing, publishing, suspending, and revoking a certificate.

54.0 Books of account.

(1) A holder of an NITA Notification, Registration and/or Certification status 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.

55.0 Retention and custody of records.

(1) A holder of an NITA Notification, Registration and/or Certification status, 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 NITA Notification, Registration and/or Certification status holder generating the records unless the NITA status holder:

- (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 NITA Notification, Registration and/or Certification status holder.

(3) A holder of an NITA Notification, Registration and/or Certification status shall keep its records in a secure place and in a secure manner.

TECHNICAL COMPONENTS COMPLIANCE

56.0 Technical components.

(1) The technical components required for the purposes of the NITA Notification, Registration and/or Certification status shall be the technical components specified in the electronic Gazette published pursuant to these Regulations.

(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.

(6) The technical components used for the purposes of 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

57.0 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

58.0 Data protection.

(1) A holder of an NITA Notification, Registration and/or Certification status 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 carrying out the permitted functions under the National Information Communication Technology Policy 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 these Regulations shall only be used for the purposes stated in the documents submitted in obtaining the NITA Notification, Registration and/or Certification status 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

(c) it is permitted processes under the Data Protection Act whether as exempt processing or otherwise.

(4) If a subscriber uses a pseudonym with the approval of any licensed entity, such entity shall transmit data concerning the subscriber's 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.

(5) No NITA Notification, Registration and/or Certification status holder shall register a subscriber solely upon a pseudonym and the NITA Notification, Registration and/or Certification status holder shall require particulars of subscriber's identity prior to processing any application.

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

59.0 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 NITA Notification, Registration and/or Certification status holders 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 NITA Status holder to ensure transfer of such records to third parties NITA Notification, Registration and/or Certification status holders 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 NITA Notification, Registration and/or Certification status holders under these regulations.

(3) The Data Trustee shall not be liable to any third party for any claim it may have against the NITA Notification, Registration and/or Certification status entity in liquidation.

ISSUE OF GUIDELINES, AUDITS, DIRECTIVES AND ORDERS

60.0 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.

61.0 Guidelines.

(1) The Agency may issue guidelines to NITA Notification, Registration and/or Certification status holders and qualified auditors in respect of -

- (a) what constitutes or satisfies the requirements for a trustworthy system;
- (b) suitable security measures;
- (c) qualified auditors and audits required under the National Information Communications Policy and these Regulations; and
- (d) such other matters as the Agency thinks fit.

PART THREE: OPEN DATA AND THE STATE

62.0 Open Data

(1) NITA shall be responsible for the monitoring of all entities of the Presidency and/or Public Services Institutions 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.

63.0 NITA and Public Records and Archives Administration Department

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

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

(3) 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.

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

(5) NITA and PRAAD shall publish in the Information Communications Technology 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.

64.0 PRIVATE SECTOR OPEN DATA

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

(2) 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.

(3) No person or entity shall operate, establish, and 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.

65.0 Information Communications Technology Gazette -Open Data

(1) 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 DEEV 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 always.

66.0 Private Sector Open Data Operators

(1) 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: NETWORK SECURITY

67.0 Network and Security

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

(5) 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.

68.0 Compliance Audit

(1) Every Entity 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 Entity 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 FIVE: CYBER SECURITY

69.0 Cyber Security

(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 Regulations 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 Services 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 Services Institutions' disaster prevention and disaster recovery policy.

(4) 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

70.0 Chief Information Officer

(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.

71.0 Inspection and investigation

- (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 SIX : DIGITAL RECORDS CLASSIFICATIONS REGIMES

72.0 Classification levels

(1) 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

(2) NITA may provide additional classification levels for protected computers, protected systems, and critical databases.

(3) 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 Services Institution as to their location and hosting.

(4) 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.

73.0 Hosting of GoG Entity Data

(1) No GoG entity shall host any data on non GoG servers without prior application to and approval issued by NITA

(2) All private sector entities under Regulatory Authorities in Ghana shall provide details of the entity hosting any data of GoG Entities and authorisation to be issued by NITA to such hosting entities of all and any matter relating to GoG entity data issued under the laws of Ghana, required by the Ghana ICT Policy and directives issued by the Minister.

(3) No data of any GoG entity shall be owned by any hosting entity, application developer, enterprise solution provider or any third party howsoever described or arising and any contract to the contrary shall be null and void.

(4) GoG entity shall host any data on non GoG servers outside the jurisdictions which sole or in combination with other level contain any data in the following classification levels:

- i. Top Secret
- ii. Secret
- iii. Confidential
- iv. Restricted
- v. Protect

74.0 Top Secret Level

(1) 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.

75.0 Secret Level

(1) 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.

76.0 Restricted and Protected Level

(1) 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 during its routine business operations and services and would have damaging consequences if lost, stolen but are not subject to a heightened threat profile.

77.0 Sector Specific Level

(1) 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.

78.0 Interoperable and Multiple Level

(1) 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.

79.0 Open Data Level

(1) 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.

80.0. Institutions Further classification Obligations

(1) 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 PL Y
- vii. Information areas suffix marking shall be IFM

(2) 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.

(3) 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.

(4) 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

(5) 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.

(6) 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

(7) 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

(8) 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

(9) 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.

(10) 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

81.0 Chief Information Officer Duties

(1) 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.

(2) 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.

(3) Every Chief Information Officer shall be responsible for monitoring compliance with:

- i. these Regulations,
- ii. Electronics Transactions Act,
- iii. National Information Technology Act,
- iv. Ghana Technology related Policies and Directives,
- v. Directives, Standards, Information Reporting and
- vi. Requests from NITA, the Minister with responsibility for Communications

and such additional duties which may be imposed on same during the discharge of their duties.

82.0 Access Control User Obligations

(1) 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.

PART SEVEN:

83.0 AFRICAN CONTINENTAL FREE TRADE AGREEMENT

(1) 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.

(2) 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.

(3) 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.

(4) 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.

(5) 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 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.

(6) 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.

(7) No entity shall be appointed to manage any Data Centre on which Government of Ghana data is held unless such entity demonstrates 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

(8) 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.

PART EIGHT

Regulation and Competition

84.0 Regulatory Market

(1) Market for purposes of these Regulations means without limitation non-telecommunications infrastructure and equipment which is technology-based products and services capable of being the subject matter of intellectual property rights intended for commercial sale and consumer use

- (a) which targets digital users of product and services consumers within and/or outside the territory Ghana
- (b) whose product and/or services are the same or similar to other competing products of other persons or entities
- (c) Innovative and not prohibited with potential market share impact locally and/or globally
- (d) Capable of being used for the same or similar purposes of other products available to consumers
- (e) Users to consumer is free, paid or, subscribed or any combination or permutation thereof combined in a manner with potential to impact market share locally and/or globally

(2) NITA shall as part of the performance of its Regulatory activities in discharging its role of monitoring and implementing the National ICT policy shall:

- a) receive complaints on monopolistic and anti-competitive conduct and practices
- b) investigate all complaints received in respect of monopolistic and anti-competitive conduct and practises
- c) conduct hearings into complaints in respect of monopolistic and anticompetitive conduct and practices
- d) impose pursuant to the outcome of such hearings, fines, and penalties for any monopolistic and/or anticompetitive practice(s) and/or conduct(s)
- e) recommend for prosecution by such Law Enforcement Agencies any conduct determined in the cause of any investigation to have infringed any provision of the criminal code, the NITA Act, the ETA and any regulations made thereunder
- f) provide and issue by Gazette Publications Guidelines on Anti-monopoly and anticompetitive conduct and practices
- g) provide technical support to requesting Statutory Regulators conducting investigations on monopolistic and anticompetitive conduct and practises where technology forms a part of the conduct under investigation

85.0 Scope of Law

(1) NITA shall in furtherance of its statutory mandate to monitor and implement the provisions of the National ICT Policy:

- a) Promote fair competition in the National ICT ecosystem
- b) Enhance the penetration of the Digital Penetration Index in the promoting of fair competition
- c) Provide Gazette Published Consumer Protection rights consistent with the provisions of the National ICT Policy
- d) Monitor, investigate, sanctions monopolistic and anticompetitive conduct and practices and
- e) advise law enforcement agencies for the prosecution of persons and entities whose conduct infringes the criminal code and/or constitute offences under the ETA, NITA, CSA Act and any other applicable primary legislation

(2) No conduct shall be held as monopolistic and anti-competitive by virtue only of the fact of

- a) Improving on technology research and development of new technological products and innovative services
- b) Upgrading the quality of existing technology products
- c) Harmonising and unifying product specifications or standard with the exclusive purpose and impact on improving product and/or service of consumers and users
- d) Bonafide exercise of intellectual property rights which has no direct or indirect effect of preventing competitors to access of licensing rights on terms and conditions which cannot reasonably be construed as having a monopolistic or anticompetitive impact in any area under NITA Regulations

86.0 Monopoly defined.

(1) Monopolistic Conduct is conduct, agreement, business plan operations and implementation which is designed, intended or whose business operations has the potential to or consequence of :

- a) Directly or indirectly by the combination of both price and quality of any product or service to interfere with the freedom of the consumer to make other product alternative choices from different providers
- b) Directly or indirectly frustrate the ability of other similar product and/or service providers to market their similarly products in any segment within the territory of Ghana

87.0 Competition Manipulation

Any act of persons or entities howsoever arising whether from sale or purchase of shares, assets, interest, rights, acquisitions, mergers, joint ventures, profit sharing agreement, management practise which results in market domination and consolidation by any person, entity or group of persons and entities to control the entry and choice of consumers shall be deemed acts calculated at manipulating competition.

88.0 Market Dominance

(1) Any technology product and/or service which is not under the Regulatory Power of the National Communication Authority which has a national consumer market share equal to or exceeding 35% of the preceding eighteen months shall for the purposes of these regulations be deemed to be a situation of market dominance.

(2) Market dominance shall be presumed where the one or more of the undermentioned conditions are present

- (a) the market share of the Local DEEV in relevant market under the Digital Economy Policy, Strategy and Guideline in the national percentage of Consumer and Users share is more than 40% and where there are at least five Local DEEV offering similar technology-based products and services
- (b) the market share of the Local DEEV, its affiliates or entities in which it holds more than 25% equity share and/or in any joint venture business in relevant market under the Digital Economy Policy, Strategy and Guideline in the national percentage of Consumer and Users share is more than 60% and where there are at least five Local DEEV offering similar technology-based products and services
- (c) The Local DEEV has the capacity based on economies of scales in addition to other variables to offer prices below the breakeven cost of its competitors and gain dominance or increase share of the market
- (d) The Local DEEV has the capacity based on the synergies it has in its affiliates, entities in which it holds more than 25% equity share and/or in joint venture business or any business arrangement which it such Local DEEV economies of scales in addition to other variables to offer prices below the breakeven cost of its competitors and gain dominance or increase share of the market
- (e) The Local DEEV entity, , its affiliates or entities in which it holds more than 25% equity share and/or in any joint venture business, provides a service to its competitors which unless unbundled and priced at unbundled costs would make it difficult for its competitors to compete within the market in a manner which does not inhibit the growth of a competition technology ecosystem
- (f) No Local DEEV entity which holds a national market share of the product or services which less than 15% shall be construed as having a dominant market position even all other factors which a business holding 40% of the national market share shall be deemed to have market dominance.

(2) Where a business operator who has been presumed to have a dominant market position can otherwise prove that they no aspects of their activities, marketing strategies, pricing, promotions and service to related to competitors inhibit competition and that the market dominance is attributable to factors outside the control of the Local DEEV holding more than 40% of the national market share it the provisions of dominance impositions under these Regulation shall not be applied and the Local DEEV entity shall be subjected to 6 monthly reviews to confirm or otherwise if any market dominance ought to be attribute to the Local DEEV entity

89.0 Abuse of Market Dominance

(1) Any entity with a dominant market shall not knowingly engage in conduct which would constitute an abuse of its dominant market position.

(2) An entity shall be deemed to engage in abuse of market dominant position where it engages in any of the following prohibited conduct and/or practices

- (a) marketing of product and/or services at unfairly at unfairly low prices;
- (b) marketing of products and/or services at prices below normal unit operations costs bereft of entity direct or indirect subsidy without any justifiable cause;
- (c) refusing to engage in any commercial undertaking and agreement with the sole directly or indirect purpose of prevention of new entrants in the market or creating market penetrating challenges for competitors of similar products and/or services without any justifiable cause;
- (d) prohibiting competitors or consumers from trading or patronising the products of competing third party products without any justifiable cause;
- (e) tying products/and or services or imposing unreasonable terms and conditions in the use of the products and/or services without any justifiable cause;
- (f) applying dissimilar prices or other transaction terms to counterparties with equal standing;
- (g) other conducts determined as abuse of a dominant position in other jurisdictions considered as jurisdiction upholding best practices

90.0 Prevention of Market dislocation

(1) Market dominance regulation shall not be used to prevent the promotion competition and growth within the Local DEEV where the subject of market dominance demonstrates that notwithstanding its market dominance and it is not engaged in any activity

- 1. or taken advantage of its market dominance to engage in market dislocation
- 2. which is monopolistic in nature and impact
- 3. which takes unfair advantage of advances which it denies its competitors and which has the potential to impact on market share
- 4. complying with directives and amended and updated directives issued by NITA for the promotion and deepening of competition under the National ICT Policy.

(2) It is permitted for such dominant Local DEEV to demonstrate that it:

- 1. is engaged in Fair competition notwithstanding its market dominant advantage
- 2. is involved in Voluntary alliances which are open to its competitors on similar terms and conditions
- 3. has gained the market dominants because of improved product scope and relevance to consumers which its competitors have failed to reasonably invest in such research producing results
- 4. has enhanced its competitiveness without engaging in any conduct and the tools by which its competitiveness is enhanced are open to its competitors who have not leveraged efficiently on same.

Local Business Protection

91.0 Prohibited Conduct

(1) Local DEEV shall in respect of any market in which their products and services are providers to Users of Technology and/ Public Sector Institutions shall not

- a. Engage in any conduct which may be described as fixing prices in a manner which reduces competition in the market
- b. Engage in any conduct which is predatory on the market

- c. Engage in cartel behaviour in any manner which may limit the choices of product and/or service users
- d. Engage in conduct which direct or indirectly engages in the sharing of the market between themselves by arrangement rather than as a natural consequence of competition
- e. Manipulation of the market with intent to consolidate predatory pricing and/or blur predatory activities
- f. Manipulation of the market with intent to disguise prohibited cartel behaviour
- g. Economic Concentration Implementation Prior Approval Procedure

(2) No market concentration activity shall be embarked upon by any group of Local DEEV Operators without the prior approval of NITA where the impact of such merger or acquisition has the potential to result in a national share of 50% of the market.

(3) Any purchase other Local DEEV sector business entities which results in a capability of appointment of the majority control of the Board of any entity, the right to veto any decision of the Board, the exercise of decisive influence on the acquired entity

(4) The provisions merger and/or acquisition is applicable notwithstanding that such merger and/or acquisition is by Local DEEV entities or Foreign incorporated entities and/or legal persons.

(5) Where NITA approves such merger and/or acquisition, the entity the subject matter of the merger and/or acquisition shall provide a declaration that it would not engage in any monopoly and/or anticompetitive conduct in the territory and/or engage in transparent and fair conduct calculated to distort or disable competition other Local DEEV entities from entry into the AfCFTA market directly or indirectly.

(6) There shall be an annual Report to be lodged by market dominant players and market concentration approved entities which shall detail their activities and demonstrate the upholding of conduct from which monopolistic and anticompetitive conduct cannot be directly or indirectly inferred and/or rationalised.

92.0 Investigative Powers

(1) NITA shall have power to investigate complaints and report of monopolistic and anticompetitive conduct without prejudice to NITA's right to inquire into such matters based on its internal market analysis and research.

(2) Any entity or individual may file a report to NITA for investigation of any Local or Foreign DEEV which it reasonably suspects to be engaged in monopolistic conduct and anticompetitive behaviour.

(3) NITA shall ensure that the identity of the entity or individual making such report is held confidential at all times as a classified document

(4) All complaints shall be in writing and/or sent electronically and where the complaint is received electronically same shall be treated with the same degree of confidentiality as classified documents.

(5) All complaints shall provide relevant facts and the evidence which forms the basis for the complaint and suspicion and NITA shall take steps to investigate same.

(6) NITA shall in respect of any investigation take the undermentioned step as part of the process of investigation and shall in this regard receive a court warrant to

- a. conduct the inspection by entering the business premises of the Local and/or Foreign DEEV entity under investigation or by getting into any other relevant place,
- b. inquire into the Local and/or Foreign DEEV entity operations under investigation, interested parties, or other relevant entities or individuals, and requiring them to explain the relevant conditions,
- c. make duplicate of the relevant documents, agreements, account books, business correspondences and electronic data, etc. of the Local and/or Foreign DEEV entity under investigation, interested parties and other relevant entities or individuals,
- d. seize and detain relevant evidence for a period prescribed by the Court which may be reviewed by extension or otherwise from time to time, and
- e. inquire into the Local and/or Foreign DEEV entity operators' bank accounts under investigation.

(7) NITA shall in carrying out the Court Orders in relation to entry and inspection of records shall rely on Law Enforcement Authorities from the Ghana Police Service who shall be under the command of a Police Office not below the rank of Inspector.

(8) When inquiring about and investigating suspicious monopolistic conducts, NITA shall make investigative notes and any statement taken shall be in the form of an investigative caution statement in the first instance and shall be taken by an Officer of the Ghana Police Service and comply with the law relating to investigation caution statements

(9) NITA and its Officers shall always keep confidential the trade secrets accessed during the course of the law enforcement without prejudice to the right of a suspect to avoid self-incrimination.

(10) NITA shall independently verify all facts, reasons and evidence provided by the Local and Foreign DEEV entities and interested parties under investigation.

(11) Where NITA makes a finding of monopolistic and/or anti competition conduct at the conclusion of its investigations, NITA shall make a determination and publish its finding in addition to the Regulatory penalties, sanctions it may impose and recommendations it may make to law enforcement agencies to carrying out criminal investigations as the Law Enforcement Agencies may deem fit.

(12) Where a Local or Foreign DEEV during any investigations admits to the engaging in monopolistic and/or anticompetitive conduct and undertakes to eliminate the impact of the conduct by taking specific measures within the time limit prescribed by NITA, NITA may suspend the investigation and publish the specific measures as undertaken by the Local and/or Foreign DEEV under investigation.

(13) Where NITA suspends the investigation, NITA shall monitor for compliance the implementation of the undertaken and where the monitoring over a period not less than 18

months or more than 2 years confirms adherence to the undertaking, NITA terminate the investigation.

- (14) NITA shall resume the investigation, where
- (a) the Local and/or Foreign DEEV fails to implement the undertaking,
 - (b) significant changes have taken place to the facts based on which the decision on suspending the investigation was made; or
 - (c) the decision on suspending the investigation was made based on incomplete or inaccurate information provided by the business operators.

93.0 Investigation Findings and Sanctions

(1) Where NITA makes a finding of monopolistic and/or anti-competitive conduct, NITA shall be entitled to

- (a) confiscate the illegal gains attributable to such monopolistic and/or anti competition conduct and/or
- (b) impose a sanction on such entity of 1% up to 10% of the sales revenue in the previous year and/or
- (c) revoke its license to operate.

(2) Where NITA makes a finding of unacceptable business practices which have the potential to have crystallised into monopolistic and/or anticompetition conduct but for the timeliness of the investigation, NITA shall be entitled to impose sanctions up to the equivalent of ten thousand penalty points.

(3) Where NITA makes a finding that the monopolistic practice and/or anti-competition conduct was engaged in but stopped before the commencement of investigation, NITA shall be entitled to confiscate the illegal gains attributable to such monopolistic and/or anti competition conduct

(4) Where any Local or Foreign DEEV entity abuses its dominant market status NITA shall be entitled to

- (a) confiscate the illegal gains attributable to such dominant market abuse and/or
- (b) impose a sanction on such entity of 1% up to 10% of the sales revenue in the previous year and/or
- (c) revoke its license to operate.

(5) Where any Local or Foreign DEEV entity implements concentration without lawful authority or in breach of its obligations thereunder, NITA shall be entitled to

- (a) confiscate the illegal gains attributable to such concentration actions and conduct and/or
- (b) impose a sanction on such entity of 1% up to 10% of the sales revenue in the previous year and/or
- (c) revoke its license to operate.

(6) NITA shall in arriving on its decision take into consideration of such factors inclusive of the nature, extent and duration of the violations and shall not act in a capricious manner and/or in a manner which would inhibit the attainment of the goal of the National ICT Policy and the digitalisation goal within the territory and within the AfCFTA countries.

(8) Local DEEV entities, Users of Technology and Public Sector Institutions shall be entitled in respect of monopolistic conduct and/or anticompetitive conduct which causes general or special loss to take such civil based actions as they may deem fit.

(9) The findings of NITA shall be a public document and shall be published on the website of NITA and capable of download.

(10) All appeals against the decisions of NITA shall be to the Technology Tribunal set up under these Regulation in the first instance and further to the Court of Appeal in the final instance.

94. Foreign Entities & National Interest

(1) Where any Foreign DEEV seek to merge or acquire any interest in a Local DEEV or incorporate a Ghanaian Local DEEV it shall first seek confirmation through NITA that such merger or acquisition is in the national interest.

(2) Such Foreign DEEV shall be required to provide evidence that it shall

- (a) not engage in any conduct which may be deemed under the laws of Ghana to be monopolistic or anticompetitive to the Local DEEV entities within the territory
- (b) not engage in any conduct which may be deemed to place the Local DEEV entities at any commercial disadvantage in their bid under the National ICT Policy to expand Local DEEV entities business activities and operations in participating countries of AfCFTA.

(3) NITA shall not engage in any conduct which is discriminatory, unfair, lack transparency and inconsistent with investigative practices.

95.0 Public Service Institutions (PSI) Applications

(1) NITA shall prescribe minimum standards through the Information Technology Gazette publication which all Public Sector applications shall adhere to in the following categories:

- 1. between Public Service Institutions
- 2. non-public service sector users which access or use such applications of the Public Service Institutions
- 3. standard Service Level Agreement contents to be complied with by applications, services, and products Public Service Institutions
- 4. standard Complaint procedures to be complied with by all applications, services, and products Public Service Institutions

96.0 PSI Service Levels Agreement Minimum Standards

(1) There shall be no annual aggregate downtimes which is more than 3% on any public service institutions technology-based product and/or services

(2) Downtime resolutions related processes shall be provided and adhered to

(3) Users of technology of such Public Services Institutions shall be updated on the status of the downtime problem resolution

97.0 PSI Service Levels Agreement Minimum Content

(1) Service Levels Agreement for PSI shall be provided for access to and by all users on all interfaces of a PSI to which users may engage.

(2) The minimum content of PSI Service Levels Agreement shall include without limitation the undermentioned issues:

- (a) Services levels
- (b) Definitions
- (c) PSI rights and responsibilities
- (d) User rights and responsibilities
- (e) Web application cookies applicable and options available
- (f) Data collection and processing purposes
- (g) Data processing exemptions within the territory
- (h) Data Subject complaint procedures
- (i) Amendments and Notifications for changes in the Service Levels Agreement
- (j) Service levels, rankings, priority, and resolution
- (k) Service levels matrices
- (l) Exception to the conditions, scope, and application of Service Levels Agreement
- (m) Service Management, Support, and complaint procedures
- (n) That an electronic copy of the SLA is lodged with NITA as Regulator of the PSI and to which further complaints may be lodged
- (o) Mean-time to resolution
- (p) Registration with the DPA

98.0 NITA Notification, Registered and/ or Certification Local DEEV Service Levels Agreement Minimum Standards

- (1) There shall be no annual aggregate downtimes which is more than 3% on any public service institutions technology-based product and/or services
- (2) Downtime resolutions related processes shall be provided and adhered to
- (3) Users of technology of such NITA Notification, Registered and/ or Certification Local DEEV product and/or services shall be updated on the status of the downtime problem resolution

99.0 NITA notification Local DEEV Service Levels Agreement Minimum Content

(1) Service Levels Agreement for NITA Notification, Registered and/ or Certification Local DEEV shall be provided for access to and by all users on all interfaces of a PSI to which users may engage.

(2) The minimum content of NITA Notification, Registered and/ or Certification Local DEEV Service Levels Agreement shall include without limitation the undermentioned issues:

- (a) Services levels
- (b) Definitions
- (c) NITA notification Local DEEV rights and responsibilities
- (d) User rights and responsibilities
- (e) Web application cookies applicable and options available
- (f) Data collection and processing purposes
- (g) Data processing exemptions within the territory
- (h) Data Subject complaint procedures
- (i) Amendments and Notifications for changes in the Service Levels Agreement
- (j) Service levels, rankings, priority, and resolution
- (k) Service levels matrices
- (l) Exception to the conditions, scope, and application of Service Levels Agreement
- (m) Service Management, Support, and complaint procedures

- (n) That an electronic copy of the SLA is lodged with NITA as Regulator of the NITA Notification, Registered and/ or Certification Local DEEV and to which further complaints may be lodged
- (o) Mean-time to resolution
- (p) Registration with the DPA

100.0 NITA recognised Foreign Incorporated DEEV Service Levels Agreement Minimum Standards

- (1) There shall be no annual aggregate downtimes which is more than 3% on any
 - (a) Public Service Institutions
 - (b) NITA Local DEEV entity the subject matter of NITA Notification, Registration and/or Certification
 - (c) Users of public service institutions,
 - (d) Consumers/customers of NITA Local DEEV entity the subject matter of NITA Notification, Registration and/or Certification
 technology based product and/or services
- (2) Downtime resolutions related processes shall be provided and adhered to
- (3) Users of technology of such NITA recognised Foreign Incorporated DEEV product and/or services shall be updated on the status of the downtime problem resolution

101.0 NITA recognised Foreign Incorporated DEEV Service Levels Agreement Minimum Content

- (1) Service Levels Agreement for NITA recognised Foreign Incorporated DEEV shall be provided for access to and by all users on all interfaces of
 - (a) Public Service Institutions
 - (b) NITA Local DEEV entity the subject matter of NITA Notification, Registration and/or Certification
 - (c) Users of public service institutions,
 - (d) Consumers/customers of NITA Local DEEV entity the subject matter of NITA Notification, Registration and/or Certification
 to which users may engage.
- (2) The minimum content of NITA recognised Foreign Incorporated DEEV Service Levels Agreement shall include without limitation the undermentioned issues:
 - (a) Services levels
 - (b) Definitions
 - (c) NITA notification recognised Foreign Incorporated DEEV rights and responsibilities
 - (d) User rights and responsibilities
 - (e) Web application cookies applicable and options available
 - (f) Data collection and processing purposes
 - (g) Data processing exemptions within the territory
 - (h) Data Subject complaint procedures
 - (i) Amendments and Notifications for changes in the Service Levels Agreement
 - (j) Service levels, rankings, priority, and resolution
 - (k) Service levels matrices
 - (l) Exception to the conditions, scope, and application of Service Levels Agreement
 - (m) Service Management, Support, and complaint procedures

- (n) That an electronic copy of the SLA is lodged with NITA as Regulator of the recognised Foreign Incorporated DEEV and to which further complaints may be lodged
- (o) Mean-time to resolution
- (p) Registration with the DPA

102.0 Forms.

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

103.0 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.

104.0. Interpretation

(1) In this Regulations the following have the following meanings 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.

“Agency” means the National Information Technology Agency established under section 1(1) of the National Information Technology Agency, 2008, Act 771 and performing roles and functions under the provisions of the Electronic Transactions Act, 2008, Act xxx

“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.

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

"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;

"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 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.

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

“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 .

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

“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;

“Digital signature ” means an advanced electronic signature which satisfies the criteria of regulation 29;

“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;

“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

"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;

“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;

“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;

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

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.

MMDAs means Metropolitan, Municipal and District Assemblies which form part of the local government service.

“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 part 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) ;

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

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

“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-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;

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.

“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;

"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;

"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;

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

"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 provided that the certification-service-provider shall not exercise the rights stemming from the permission requested until it has received the decision of the National Information Technology Agency.

“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.

"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.

105.0 Commencement

This Regulation shall come into force effective XXXXX 2023 or such other date that the Minister may by Gazette notification give notice of its coming into force.

106.0 xx SCHEDULE

xx SCHEDULE xx ONE FORM 1

Forms for NITA Notification/Registration/Certification by technology-based product, design and solution providing entities. [Vendor Implementing technology design, products and services]

	FORM xx Regulations]		
	NATIONAL INFORMATION TECHNOLOGY ACT, 2008, ACT XXX NATIONAL INFORMATION TECHNOLOGY REGULATIONS, 2023, LI XXX		
<i>Tick (✓) whichever is relevant.</i>	NITA NOTIFICATION/REGISTRATION/CERTIFICATION * [TECHNOLOGY BASED PRODUCTS, DESIGNS & SOLUTIONS]		
PARTICULARS OF APPLICANT 1. Name of applicant and correspondence address		Fixed Line no.	
Contact persons & Designation	Contact persons Identification Document & Particulars.	Mobile No.	

Email:		Social Media Identification details			
2. Brand name of applicant where applicable		3. Date of incorporation.		4. Place of incorporation.	
5. Location Address of registered office		Registered Office email address		6. Address of other offices (if any)	
		Registered Office Digital address			
Areas of National ICT Policy impacted by Form content					
Universal Access & Connectivity ... YES/NO	Digital Government ... YES/NO	Data and Emerging technologies ... YES/NO	Digital Skills ... YES/NO	Digital Entrepreneurship ... YES/NO	Digital Security ... YES/NO
7. Particular of directors/partners					
Name and residential address	Nationality	Particulars of Registration with the Data Protection Commission	% of share held in company/ % of partnership		
	Particulars of Identification				
B. OPERATIONAL COSTS Total.....			Cedis Total.....		
1. Fixed assets (please specify) (a)..... (b)..... (c).....(d) PLEASE ADD SHEET FOR FIXED ASSETSValue of Fixed Asset Note: If the land, building, or equipment is rented/leased, specify the annual cost of rental/ lease.			Total fixed assets Cedis		
2. Pre-operational costs					

3. Working capital	
4. Insurance coverage	
Detailed description of business product and services, the subject matter of NITA Notification	Particulars of Security feature of products and services
Does not entity set aside a percentage of profits into Research and Development? YES* NO* [please circle relevant answer]	If YES please provide the percentage and attached the Audited Statement of Accounts which captures the amounts invested from previous years profit into Research & Development
Detailed description of business product and services, the subject matter of NITA Registration	Particulars of Security feature of products and services
Detailed description of business product and services, the subject matter of NITA Certification	Particulars of Security feature of products and services
Is your application to be relied upon in the provision of services and sale of products exclusively within the territory of Ghana	Brief Description of products and services
Is your application to be relied upon in the provision of services and sale of products for use within the territory of Ghana and in other signing countries to African Continental Free Trade Agreement? YES* NO* [please circle relevant answer]	Brief Description of products and services
Are any products and services provided by your entity activity the subject matter of any Regulatory Body? YES* NO* [please circle relevant answer]	If Yes, please provide details of the Regulatory Body
Can any products and services provided by your entity activity be construed by any Regulatory Body as a product or service in respect of which Regulation is required? YES* NO* [please circle relevant answer]	If Yes, please provide details of the Regulatory Body
Are any products and services provided by your entity activity the similar to products and services of entities under existing Regulatory Authority? YES* NO* [please circle relevant answer]	If Yes, please provide details of the Regulatory Body
Are any products and services of your entities used by your entity or other entities on any Critical Infrastructure in Ghana? YES* NO* [please circle relevant answer]	If Yes please provide details of such products and service and entities which use them on any critical infrastructure

Do your products or service hold data from any Arms of Government, Public Service Institution, Civil Service or State-Owned Organisation held by your entity on your entity hardware, cloud or Third Party Private Sector or Third Country? YES* NO* <i>[please circle relevant answer]</i>	If yes please provide description of the data which is held by your entity
What classification of data under the NITA Regulations do products and services of your entity capture	Please list the areas of classification of data
Does your entity contribute to the development of Open Data ecosystem? YES* NO* <i>[please circle relevant answer]</i>	If so, please provide area of Open data that your entity contributes to the development
Does your entity engage in any Industry Forum activities under the ETA? YES* NO* <i>[please circle relevant answer]</i>	If Yes please provide details of the Industry Forum related advocacy which would impact positively on your entity's business
Are any products and services of your entity subject to the laws of any Third Country ? YES* NO* <i>[please circle relevant answer]</i>	If Yes please provide the list of such Third Countries
Are any intellectual property rights of any of your products and services solutions owned by Non-Ghanaian entities? YES* NO* <i>[please circle relevant answer]</i>	If yes please provide a brief description of such products and service solutions in respect of which IPR are held by Non-Ghanaian entities
Is your entity sale of products and service solution owned by non-Ghanaian entities governed by contract agreement between your entity and such third-party holders? YES* NO* <i>[please circle relevant answer]</i>	If yes, are the contents of such Agreement confidentiality agreement for which disclosure is prohibited?
Has a receiver, or a receiver and manager, been appointed in respect of any of the applicant's asset at any time in the 3 years preceding this application? YES* NO* <i>[please circle relevant answer]</i>	
Has the applicant entered into a compromise or arrangement with creditors at any time in the 3 years preceding this application? YES* NO* <i>[please circle relevant answer]</i>	
Has a petition been presented in a court for the winding up of your entity at any time in the 3 years preceding this application? YES* NO* <i>[please circle relevant answer]</i>	

Declaration

xxxx SCHEDULE PART xxx FORM 1A

Forms for Registration of entities providing exclusive ICT Services and not Vendor Implementing technology design, products, and services.

FORM X Regulations]			
NATIONAL INFORMATION TECHNOLOGY ACT, 2008, ACT XXX NATIONAL INFORMATION TECHNOLOGY REGULATIONS, 2023, LI XXX			
Tick (✓/) whichever is relevant.	NITA NOTIFICATION/REGISTRATION/CERTIFICATION * ICT CONSULTANCY SERVICES		
PARTICULARS OF APPLICANT 1. Name of applicant and correspondence address		Fixed Line no.	
Contact persons & Designation	Contact persons Identification Document & Particulars.	Mobile No.	
Email:		Social Media Identification details	
2. Brand name of applicant where applicable	3. Date of incorporation.		4. Place of incorporation.
5. Location Address of registered office	Registered Office email address	6. Address of other offices (if any)	
	Registered Office Digital address		
7. Particular of directors/partners/proprietorship/joint venture undertaking			
Name and residential address	Nationality		% of share held in company/ % of partnership

.....	 Particulars of Identification	Particulars of Registration with the Data Protection Commission	
Areas of National ICT Policy impacted by Form content			
Universal Access & Connectivity ... YES/NO	Digital Government ... YES/NO	Data and Emerging technologies ... YES/NO	Digital Skills ... YES/NO
			Digital Entrepreneurship ... YES/NO
			Digital Security ... YES/NO
Detailed description of ICT Consulting services, the subject matter of NITA Registration			
Is your application to be relied upon in the provision of ICT Consulting services, the subject matter of NITA Registration exclusively within the territory of Ghana			
Is your application to be relied upon in the provision of ICT Consulting services, the subject matter of NITA Registration for use within the territory of Ghana and in other signing countries to African Continental Free Trade Agreement? YES* NO* [please circle relevant answer]			
Is your entity owned by non-Ghanaian entities? YES* NO* [please circle relevant answer]			
Has a receiver, or a receiver and manager, been appointed in respect of any of the applicant's asset at any time in the 3 years preceding this application? YES* NO* [please circle relevant answer]			
Has the applicant entered into a compromise or arrangement with creditors at any time in the 3 years preceding this application? YES* NO* [please circle relevant answer]			
Has a petition been presented in a court for the winding up of your entity at any time in the 3 years preceding this application? YES* NO* [please circle relevant answer]			
Has your entity provided any ICT Consulting services, to Arms of Government, Public Service Institution, Civil Service or State-Owned Organisation? YES* NO* [please circle relevant answer]			If yes please provide particulars of any such recipients

What classification of data under the NITA Regulations do does the range of your ICT Consulting Services cover	Please list the areas of classification of data
Does your entity engage in any Industry Forum activities under the ETA? YES* NO* [please circle relevant answer]	If Yes please provide details of the Industry Forum related advocacy which would impact positively on your entity's business
Are any aspects of your entity ICT Consulting Service under the control of laws of any Third Country ? YES* NO* [please circle relevant answer]	If Yes please provide the list of such Third Countries
Declaration	

xxxxx SCHEDULE FEES

Particulars	Fees (cedi)
Initial Notification, by DEEV	
(i) Startups,	
(ii) Entities in Business for less than 5 years,	
(iii) entities with less than 10 employees,	
(iv) entities with more than 10 employees but less than 50 employees,	
(v) entities with more than 50 employees	
Renewal Notification, by DEEV	
(i) Startups,	
(ii) Entities in Business for less than 5 years,	
(iii) entities with less than 10 employees,	
(iv) entities with more than 10 employees but less than 50 employees,	
(v) entities with more than 50 employees	
Initial Registration by DEEV	
(i) Startups,	
(ii) Entities in Business for less than 5 years,	
(iii) entities with less than 10 employees,	

(iv) entities with more than 10 employees but less than 50 employees,

(v) entities with more than 50 employees

Renewal Registration by DEEV

(i) Startups,

(ii) Entities in Business for less than 5 years,

(iii) entities with less than 10 employees,

(iv) entities with more than 10 employees but less than 50 employees,

(v) entities with more than 50 employees

Initial Certification by DEEV

(i) Startups,

(ii) Entities in Business for less than 5 years,

(iii) entities with less than 10 employees,

(iv) entities with more than 10 employees but less than 50 employees,

(v) entities with more than 50 employees

Renewal Certification by DEEV

(i) Startups,

(ii) Entities in Business for less than 5 years,

(iii) entities with less than 10 employees,

(iv) entities with more than 10 employees but less than 50 employees,

(v) entities with more than 50 employees

African Free Continental Free Trade Agreement

(i) Initial Registration

(ii) Renewal of Registration

107.0 xxxxx SCHEDULE TO PART xxxxx – OPEN DATA CONTRIBUTORS FORMS

	FORM X Regulations]	
--	------------------------------	--

	NATIONAL INFORMATION TECHNOLOGY ACT, 2008, ACT XXX NATIONAL INFORMATION TECHNOLOGY REGULATIONS, 2023, LI XXX			
Tick (✓) whichever is relevant.	OPEN DATA CONTRIBUTION APPLICATION FORMS Private Sector Applications *			
PARTICULARS OF APPLYING ENTITY		Fixed Line no.		
1. Name of Applying Entity and correspondence address				
Contact persons & Designation.	Contact persons Identification Document & Particulars.	Mobile No.		
Email:		Social Media Identification details		
2. Brand name of applicant where applicable	3. Date of incorporation.		4. Place of incorporation.	
5. Location Address of registered office	Registered Office email address		6. Address of other offices (if any)	
	Registered Office Digital address			
7. Particular of directors/partners/proprietorship/joint venture undertaking				
Name and residential address	Nationality	Particulars of Registration with the Data Protection Commission	% of share held in company/ % of partnership	
	Particulars of Identification			
Detailed description of Classification level related data				
Areas of National ICT Policy impacted by Form content				

Universal Access & Connectivity ... YES/NO	Digital Government ... YES/NO	Data and Emerging technologies ... YES/NO	Digital Skills ... YES/NO	Digital Entrepreneurship ... YES/NO	Digital Security ... YES/NO
OPEN DATA SECTOR	DOES ENTITY PROCESS ANY OF THESE CLASSIFIED COMMUNICATION [Answer Yes or No]	HAS THERE BEEN ANY POTENTIAL OR ACTUAL BREACH IN THE CLASSIFICATION AREA [Answer Yes or No]	ARE THERE ANY OUTSTANDING CYBER SECURITY RELATED MATTERS BEING RESOLVED [Answer Yes or No]		
Logistic Sector					
Agriculture Sector					
Industrial Sector					
Technology Sector					
Financial Sector					
Trade – In Country					
Trade – Export Sector					
Financial Sector					
Aviation Sector					
Maritime Sector					
Rail, Road & Transport sector					
Digital Entrepreneurial Enable Vehicles sector					
Digital Inclusion Sector					
Digital Penetration Sector					
Disability Sector					
Marginalised & Rural Sector					
Qualifications of Officer of Open Data Returning Entity:					
Attach photocopy of qualification of Open Data Returning Entity Date of certificate:..... Awarding Body/Institution..... Awarding Institutions Contact details.					
Is your entity owned by non-Ghanaian entities? YES* NO* [please circle relevant answer]					

Has the Open Data Returning Entity entered into a compromise or arrangement with creditors at any time in the 3 years preceding this application? YES* NO* <i>[please circle relevant answer]</i>	
Has a petition been presented in a court for the winding up of your entity at any time in the 3 years preceding this application? YES* NO* <i>[please circle relevant answer]</i>	
Is the Open Data Returning Entity gathering data from any Arms of Government, Public Service Institution, Civil Service or State-Owned Organisation? YES* NO* <i>[please circle relevant answer]</i>	If yes please provide particulars of any such Arms of Government, Public Service Institution, Civil Service or State-Owned Organisation
Has compliance audit in respect of the filed its' ICT Compliance Audit for the Returning Annual Period? YES* NO* <i>[please circle relevant answer]</i>	If Yes please provide details of the filing dates of the last compliance audit
Does the Open Data Returning entity engage in any Industry Forum activities under the ETA? YES* NO* <i>[please circle relevant answer]</i>	If Yes please provide details of the Industry Forum related advocacy group associated with the entity
Are any aspects of your entity Data Protection compliance requirement under the control of laws of any Third Country ? YES* NO* <i>[please circle relevant answer]</i>	If Yes please provide the list of such Third Countries
Declaration	

xxxxxxx SCHEDULE FEES

<i>Particulars</i>	<i>Fees (cedi)</i>
Open Data Application for contribution to National Open Data platform	

109.0 xxxx SCHEDULE PART xxxx FORM 1

	FORM X Regulations]			
	NATIONAL INFORMATION TECHNOLOGY ACT, 2008, ACT XXX NATIONAL INFORMATION TECHNOLOGY REGULATIONS, 2023, LI XXX			
Tick (✓/) whichever is relevant.	FORMS ACCOMPANYING SUBMISSION OF COMPLIANCE AUDIT*			
PARTICULARS OF COMPLIANCE AUDITOR 1. Name of Compliance Auditor and correspondence address		Fixed Line no.		
Contact persons & Designation.	Contact persons Identification Document & Particulars.	Mobile No.		
Email:		Social Media Identification details		
2. Brand name of applicant where applicable	3. Date of incorporation.		4. Place of incorporation.	
5. Location Address of registered office	Registered Office email address		6. Address of other offices (if any)	
	Registered Office Digital address			
7. Particular of directors/partners/proprietorship/joint venture undertaking				
Name and residential address	Nationality	Particulars of Registration with the Data Protection Commission	% of share held in company/ % of partnership	
	Particulars of Identification			

			
Areas of National ICT Policy impacted by Form content			
Universal Access & Connectivity ... YES/NO	Digital Government ... YES/NO	Data and Emerging technologies ... YES/NO	Digital Skills ... YES/NO
			Digital Entrepreneurshi p ... YES/NO
			Digital Security ... YES/NO
Detailed description of ICT Compliance Audit, the subject matter of NITA Filing of Returns			
1. Dates of last 5 submitted compliance audits: 			
2. Levels of compliance Compliance Audit No. 1 Full/Substantial/Partial/Non*- compliance Compliance Audit No. 2 Full/Substantial/Partial/Non*- compliance Compliance Audit No. 3 Full/Substantial/Partial/Non*- compliance Compliance Audit No. 4 Full/Substantial/Partial/Non*- compliance Compliance Audit No. 5 Full/Substantial/Partial/Non*- compliance *delete inapplicable findings of compliance audit			
Dates of re-audits in respect of each finding of partial or non-compliance audit finding 			
Qualifications of Compliance Auditor at the time of audit: 			
Attach photocopy of qualification of Compliance Auditor at time of audit Date of certificate:..... Awarding Body/Institution..... Awarding Institutions Contact details.			

Is your entity owned by non-Ghanaian entities? YES* NO* <i>[please circle relevant answer]</i>	
Has the Compliance Auditor entered into a compromise or arrangement with creditors at any time in the 3 years preceding this application? YES* NO* <i>[please circle relevant answer]</i>	
Has a petition been presented in a court for the winding up of your entity at any time in the 3 years preceding this application? YES* NO* <i>[please circle relevant answer]</i>	
Has your entity provided any ICT Compliance Auditing services, to Arms of Government, Public Service Institution, Civil Service or State-Owned Organisation? YES* NO* <i>[please circle relevant answer]</i>	If yes please provide particulars of any such recipients
What classification of data under the NITA Regulations do does the range of your ICT Compliant Auditing Services cover	Please list the areas of classification of data
Does your ICT Compliance Audit entity engage in any Industry Forum activities under the ETA? YES* NO* <i>[please circle relevant answer]</i>	If Yes please provide details of the Industry Forum related advocacy which would impact positively on your entity's business
Are any aspects of your entity ICT Compliance Audit Service under the control of laws of any Third Country ? YES* NO* <i>[please circle relevant answer]</i>	If Yes please provide the list of such Third Countries
Declaration	

110.0 xxxxxxx SCHEDULE TO PART xxxxxx – CYBER SECURITY
 CYBER SECURITY COMPLIANCE RETURN FORMS

	FORM X Regulations]	
	NATIONAL INFORMATION TECHNOLOGY ACT, 2008, ACT XXX NATIONAL INFORMATION TECHNOLOGY REGULATIONS, 2023, LI XXX	
Tick (✓) whichever is	CYBER SECURITY RETURN FORMS *	

.....	Particulars of Identification		
Areas of National ICT Policy impacted by Form content			
Universal Access & Connectivity ... YES/NO	Digital Government ... YES/NO	Data and Emerging technologies ... YES/NO	Digital Skills ... YES/NO
			Digital Entrepreneurship ... YES/NO
			Digital Security ... YES/NO
Detailed description of Classification level related data			
NITA REGULATIONS CLASSIFICATION LEVELS	DOES ENTITY PROCESS ANY OF THESE CLASSIFIED COMMUNICATION [Answer Yes or No]	HAS THERE BEEN ANY POTENTIAL OR ACTUAL BREACH IN THE CLASSIFICATION AREA [Answer Yes or No]	ARE THERE ANY OUTSTANDING CYBER SECURITY RELATED MATTERS BEING RESOLVED [Answer Yes or No]
Top Secret			
Secret			
Confidential			
Restricted			
Protect			
Open Data			
Sector Specific Interoperable			
Multiple			
Qualifications of Officer of Cyber Security Returning Entity:			
Attach photocopy of qualification of Cyber Security Returning Entity			
Date of certificate:..... Awarding Body/Institution.....			
Awarding Institutions Contact details.			
Is your entity owned by non-Ghanaian entities? YES* NO* [please circle relevant answer]			

Has the Cyber Security Returning Entity entered into a compromise or arrangement with creditors at any time in the 3 years preceding this application? YES* NO* <i>[please circle relevant answer]</i>	
Has a petition been presented in a court for the winding up of your entity at any time in the 3 years preceding this application? YES* NO* <i>[please circle relevant answer]</i>	
Is the Cyber Security Returning Entity services a part of any Arms of Government, Public Service Institution, Civil Service or State Owned Organisation? YES* NO* <i>[please circle relevant answer]</i>	If yes please provide particulars of any such Returning Entity
Has compliance audit in respect of the Cyber Security Returning entity filed its' ICT Compliance Audit for the Returning Annual Period? YES* NO* <i>[please circle relevant answer]</i>	If Yes please provide details of the filing dates of the last compliance audit
Does the Cyber Security Returning entity engage in any Industry Forum activities under the ETA? YES* NO* <i>[please circle relevant answer]</i>	If Yes please provide details of the Industry Forum related advocacy group associated with the entity
Are any aspects of your entity ICT Cyber Security compliance requirement under the control of laws of any Third Country ? YES* NO* <i>[please circle relevant answer]</i>	If Yes please provide the list of such Third Countries
Declaration	

xxxxxx SCHEDULE – PART xxxxxx TECHNICAL COMPONENTS
CYBER SECURITY IMPACTING TECHNICAL STANDARD

<i>Item No.</i>	<i>Matter</i>	<i>Technical components to be used</i>
1.	For the generation of advanced electronic signatures	Technical components that make it nearly certain that - (a) any given security feature is not capable of unauthorised duplication or creation; (b) is authentic, reliable, verifiable and cannot be created by any software, method, third party in any manner which would compromise the reliability of the advanced electronic signature.; and (c) security features is not capable of duplication.
2.	During - (a) the generation and storage of security feature; and	Technical components that have security features that - (a) allow the use of the user only after due identification of the user through a personal identification number or other data used for identification in conjunction with the data storage

- | | |
|--|---|
| <p>(b) the verification of advanced electronic signatures</p> | <p>medium for the security feature of the user;</p> <p>(b) do not disclose any information which would compromise any security feature during its use;</p> <p>(c) function in such a manner that unauthorised access to security feature cannot be derived from the advanced electronic signature; and</p> <p>(d) make forgery of advanced electronic signatures and falsification of signed data reliably noticeable and protect against the unauthorised use of the security feature.</p> |
| <p>3. For collecting identification data</p> | <p>Technical components that function in such a manner that -</p> <p>(a) they do not reveal the identification data; and</p> <p>(b) they ensure that the identification data is stored only on the data storage medium consistent with the security feature of the advanced electronic signature.</p> |
| <p>4. For the representation of data that is to be signed</p> | <p>Technical components that have security features that-</p> <p>(a) show unmistakably and in advance the creation of an advanced electronic signature; and</p> <p>(b) allow a determination of the data to which the advanced electronic signature refers.</p> |
| <p>5. For the checking of signed data</p> | <p>Technical components that have security features that allow it to be determined -</p> <p>(a) whether the signed data are unchanged;</p> <p>(b) to which data the advanced electronic signature refers; and</p> <p>(c) to which the originator of the advanced electronic signature is to be attributed.</p> |
| <p>6. For verifying certificates</p> | <p>Technical components that allow clear and reliable determination of whether verified certificates were present, without having been invalidated, in the Register of Certificates kept and maintained by a licensed authentication service provider.</p> |
| <p>7. For -</p> <p>(a) the authentication service provider disclosure record; and</p> <p>(b) any other record maintained in a verifiable or verifiable or accessible manner under the Act or the Regulations</p> | <p>Technical components that protect -</p> <p>(a) the data storage mediums in which the records are stored; and</p> <p>(b) the repositories in which the records are published, from unauthorised access and unauthorised modification.</p> |

8. For the generation of time-stamps Technical components that function in such a manner that the valid official time, without distortion, is added to the time-stamp when it is generated.