Form I
(Regulation 6(1))

THE ZAMBIA INFORMATION AND COMMUNICATIONS TECHNOLOGY AUTHORITY

The Cyber Security and Cyber Crimes Act, 2021
(Act No. 2 of 2021)

The Cyber Security and Cyber Crimes (Critical Information Infrastructure) Regulations, 2021

Notes for Applicants

1. In line with Section 19(1) of the Cyber Security and Cyber Crimes Act 2021 (Act), Critical Information Infrastructure (CII) shall be registered with the Authority, and the information shall be maintained by the Authority in line with Section 21 of the Act. Note:
   (a) One form is required for each Critical Infrastructure Asset;
   (b) If a CII owner wishes to change ownership of a Critical Information Infrastructure, they shall apply to the Authority in line with Section 20(1) of the Act.
2. Instruction on completing the form:

   (a) 'Section 4: Asset Operator' Form can be duplicated if multiple asset operators exist, the Asset Operators number must be indicated in the text box at the top of the form.

   (b) All attachments must:
      (i) be certified; and
      (ii) prove and/or relate to the information placed in the form(s). For example, 'Section 1: Critical Infrastructure Asset details' would require attachments such as; National Identity Card (National Registered Card), National Passport (Page 2 and 3), proof of incorporation or registration (in case of legal person).

   (c) arrangement of interconnected:

      (i) IT (Information Technology) refers to arrangement of interconnected computers that is used in the storing, accessing, processing, analysing and sending of information.
      (ii) OT (Operational Technology) refers to an arrangement of interconnected computers that is used in the monitoring and/or control of physical processes, that includes:
         (1) Supervisory control and data acquisition systems, distributed control systems, and other control system configuration such as programmable logic controllers;
         (2) A combination of control components, for example electrical, mechanical, hydraulic, pneumatic, that act together to achieve an

industrial objective (e.g. manufacturing, transportation of matter or energy).

(d) the asterisk * represents a mandatory requirement and must be completed.

3. An incomplete application shall NOT be processed and shall require resubmission.

APPLICATION AS CRITICAL INFORMATION INFRASTRUCTURE		
Section 1: Critical Infrastructure Asset details		
1.1.	In what sector is the critical infrastructure asset you are registering?*: *Select one (1) Option*	
	☐Aviation ☐Banking & Finance ☐Energy ☐Government ☐Healthcare ☐Information and Communication ☐Land Transport ☐Manufacturing ☐Media ☐Security & Emergency ☐ Water ☐Food ☐ Other (Specify):	
1.2.	Name of the Critical Infrastructure Asset*:	
1.3.	Location of the Asset*	
1.4.	Legal description of location, if available:	
1.5.	Describe the area that the Asset services. This information may be described in terms of the geographic locations in which services are provided. If the serviced area is in more than one State or Territory select all that apply. Documents can be attached to clarify or give further detail.*:	
	(a) Number of Provinces Serviced*:	
	(b) Province serviced*: *Select all that apply*	☐ Central ☐ Copperbelt ☐ Eastern ☐ Luapula ☐ Lusaka ☐ Muchinga ☐ North-Western ☐ Northern ☐ Southern ☐ Western ☐ Other (Specify):
1.6	Reason for Registration*: *Select one (1) Option*	☐ Existing holding - now captured within reporting threshold ☐ New Acquisition ☐ Other (Specify):
Asset Details – Attachments		
You can submit a maximum of 10 documents supporting your registration. Allowed file types are PDF, JPG, JPEG, PNG and XLSX. Each of these documents can be up to 5 mb (Excel and PDF files can be 10 mb) in size.		
Section 2: My Details		
2.2	In what capacity are you submitting this registration*: *Select one (1) Option*	☐ Existing holding - now captured within reporting threshold ☐ New Acquisition ☐ Other (Specify):
2.3	Details of primary contact	
	(a) Your legal name	
	Title:	
	First Name *:	
	Middle Name:	
	Surname or Family Name *:	
	Employer's Name*:	
	(b) Employer's Address	

	Street Address *: *PO Boxes are not acceptable*	
	City Or Town *:	
	Country *:	
	Province, State or Territory *:	
	Postcode or Zip code *:	
	Your job title / position *:	
	(c) Your preferred contact method: *Select one (1) Option*	☐ Email ☐ Primary telephone number ☐ Alternative telephone number
	(d) Your contact details	
	Your email address*:	
	Primary telephone number*: *Include country code*	
	Alternative telephone number*: *Include country code*	
2.4.	Details of secondary contact	
	(a)Their legal name	
	Title:	
	First Name *:	
	Middle Name:	
	Surname or Family Name *:	
	Employer's Name*:	
	(b)Employer's Address Street Address *: *PO Boxes are not acceptable*	
	City Or Town *:	
	Country *:	
	Province, State or Territory *:	
	Postcode or Zip code *:	
	(c) Your job title / position *:	
	(d) Your preferred contact method: *Select one (1) Option*	☐ Email ☐ Primary telephone number ☐ Alternative telephone number
	(e) Your contact details	
	Your email address*:	
	Primary telephone number*: *Include country code*	
	Alternative telephone number*: *Include country code*	
My Details – Attachments		
You can submit a maximum of 10 documents supporting your registration. Allowed file types are PDF, JPG, JPEG, PNG and XLSX. Each of these documents can be up to 5 mb(Excel and PDF files can be 10 mb) in size.		

Section 3: Responsible Entity

A Responsible Entity for an asset refers to:

- A controller of CII as interpreted in Section 2; or
- the entity that holds the licence, approval or authorisation (however described) to operate the asset and provide the service to be delivered by the asset;
- for an asset declared under section 17 to be a critical infrastructure asset—the entity specified in the declaration as the responsible entity for the asset (see subsection 17(1))

An entity can be an individual, a body corporate, a body politic, a partnership, a trust, a superannuation fund, or an unincorporated foreign company

3.1	Details Of Responsible Entity	
	(a) Legal name of Responsible Entity*:	
	(b) Type of entity*: *Select one (1) Option*	☐An individual Person ☐Body Corporate ☐Body Politic ☐ Superannuation Fund ☐Trust ☐Partnership ☐Unincorporated Foreign Company ☐ Other (Specify):
	(c) Country of incorporation or creation*:	
	(d) Business registration number *: *Company Registration Number or however described*	
	(e) Address of head office or principal place of business Street Address *: *PO Boxes are not acceptable*	
	City Or Town *:	
	Country *:	
	Province, State or Territory *:	
	Postcode or Zip code *:	
	(f) Original commencement date as Responsible Entity of this Asset*: *The month and year are mandatory, however, the day is optional*	
3.2	Operational information - Chief Executive Officer (or however described) of the Responsible Entity	
	(a)Legal name	
	Title:	
	First Name *:	
	Middle Name:	
	Surname or Family Name*:	
	Country of citizenship*:	
	Country of dual citizenship: *If applicable*	
3.3	Operational information – Data Arrangements	

	(a) Provide a description of the arrangements under which data prescribed by the rules relating to the asset is maintained. You can attach documents to provide further details.*:
3.4	Operational information – Other Operators of this Asset
	(a) Are there any other entities that are Operators for this Critical Infrastructure asset?*: *IF No - proceed to Section 5 'Additional information and Declaration', IF Yes - proceed to Section 4 'Asset Operators'*

Note: an operator is an entity that is authorised (however described) to operate the asset or part of the asset.

Responsible Entity – Attachments

You can submit a maximum of 10 documents supporting your registration.
Allowed file types are PDF, JPG, JPEG, PNG and XLSX.
Each of these documents can be up to 5 mb (Excel and PDF files can be 10 mb) in size.

Section 4: Asset Operator NO.

Record details of entity that is defined as an operator of any parts of this critical asset. *If applicable*
Once all operators have been recorded, continue to the Declaration section.

4.1.	Operator Details	
	(a) Legal name of entity*:	
	(b) Type of entity*: *Select one (1) Option*	☐An individual Person ☐Body Corporate ☐Body Politic ☐ Superannuation Fund ☐Trust ☐Partnership ☐Unincorporated Foreign Company ☐ Other (Specify):
	(c) Country of incorporation or creation*:	
	(d) Business registration number *: *Company Registration Number or however described*	
	(e) Address of head office or principal place of business Street Address *: *PO Boxes are not acceptable* City Or Town *: Country *: Province, State or Territory *: Postcode or Zip code*:	
	(f) Original date the Operator commenced operating this asset*: *The month and year are mandatory, however, the day is optional*	
4.2	Operator arrangements	
	(a)Provide details of the arrangements (such as outsourcing or offshoring) under which this entity operates the Asset or part of the Asset. This would include a description of the arrangements if the control system of the asset is managed by a separate body. Documents can be attached to provide further information.*	

Asset Operators – Attachments

You can submit a maximum of 10 documents supporting your registration.
Allowed file types are PDF, JPG, JPEG, PNG and XLSX.
Each of these documents can be up to 5 mb (Excel and PDF files can be 10 mb) in size.

Asset Registry Requirements

CII ASSET INVENTORY

Instruction:
Enter a list of components/assets that make up the CII. Information relating to the identity, hardware, network, software and logging of each component/asset should be included.

LOGICAL NETWORK DIAGRAM REQUIREMENTS

Instruction:

FOR IT ENVIRONMENT

1. Depict logical connections of components within CII system.
2. Indicate IP address range of clusters/components within CII system (e.g. IP: 192.168.X.X/16)
3. Indicate all external connections (both internet facing and non-internet facing) from CII system:

FOR OT ENVIRONMENT

1. Depict logical connections of components within CII system:
2. Indicate IP address range of clusters/components within CII system (e.g. IP: 192.168.X.X/16)
3. Indicate all external connections (both internet facing and non-internet facing) from CII system:

INFORMATION ON INTERCONNECTED COMPUTER(S) OR COMPUTER SYSTEM(S)

Instruction:
Enter the list of computers/computer systems that are connected to the CII. Information relating to the identity, connections to CII, software and operator of the computers/computer systems should be included.

INTERNET LINKS SUPPORTING CII

Instruction:

Enter the list of internet links supporting the CII system and the DDoS mitigation in place for these links.

OUTSOURCED SERVICES SUPPORTING CII SYSTEM

Instruction:
Enter the list of services outsourced to third-party vendors for supporting CII system. Vendors providing Managed Security Services (MSS) for CII System should also be included.

CLOUD SOLUTIONS

Instruction:

Enter the list of cloud services used to support CII system.

Section 5: Declaration

5.1 Further Information

(a) Provide any further information here that you believe is relevant and may assist the Authority:

5.2	Declaration
	I/we declare that all the particulars and information provided in this application are complete, correct and true and I/we agree that in the event that any of the said particulars and information provided is found to be untrue or fraudulent, the licence will be revoked. I/we agree that in the event of the revocation of the licence, any fee paid to the authority for licence shall be forfeited. I/we declare that in the event that the nature of my/our business changes, or I/we no longer carry out operations in terms of the registration, I/we will notify the Authority in which case my/our registration may be revoked or revised. Declared at …… this …… days of …… 20…… by the following persons who are duly authorised to sign for and on behalf of the applicant under the authority of the Power of Attorney or Board resolution which is hereby attached.
	Name: *Name of individual filling in this form*
	Date: *Completion Date*
	Signature:

Declaration – Attachments
You can submit a maximum of 10 documents supporting your registration. Allowed file types are PDF, JPG, JPEG, PNG and XLSX. Each of these documents can be up to 5 mb (Excel and PDF files can be 10 mb) in size.

My Details – Attachments
_____ _____ Applicant Date _____ _____ Officer Date

FOR OFFICIAL USE ONLY
Received by _____ _____ Officer Date Received Amount Received: _____ Serial No. of application: _____

Section 6: Attachments	
6.1	Asset Details – Attachments

6.2	My Details – Attachments
6.3	Responsible Entity – Attachments
6.4	Asset Operators – Attachments
6.5	Asset Registry Requirements – Attachments
6.6	Declaration – Attachments

Form II
(Regulation 7)

THE ZAMBIA INFORMATION AND COMMUNICATIONS TECHNOLOGY AUTHORITY

The Cyber Security and Cyber Crimes Act, 2021
(Act No. 2 of 2021)

The Cyber Security and Cyber Crimes (Critical Information Infrastructure) Regulations, 2021

REQUEST FOR FURTHER PARTICULARS

To **[Insert Applicant/ Certificate Holder Name]**

In relation to your application for a(n) **[Insert Certificate Category]** with reference number **[Insert ZICTA Reference Number]** address of **[Insert Applicant/ Certificate Holder's Current Address].**

[Insert details of further particulars being requested]

The failure to submit the requested information within [Insert Period] from the date hereof shall lead to your application being treated as invalid and shall be rejected.

Dated this **[Insert day]** day of **[Insert Month]** **[Insert Year]**

.....

Director-General

Form III
(Regulation 8)

THE ZAMBIA INFORMATION AND COMMUNICATIONS TECHNOLOGY AUTHORITY

The Cyber Security and Cyber Crimes Act, 2021
(Act No. 2 of 2021)

The Cyber Security and Cyber Crimes (Critical Information Infrastructure) Regulations, 2021

Certificate No.: .....

In accordance with Section 19 of the Cyber Security and Cyber Crimes Act No. 2 of 2021, this

INSERT CERTIFICATE TYPE

is granted by the Director-General of the Zambia Information and Communications Technology Authority to:-

INSERT HOLDERS NAME

INSERT HOLDERS ADDRESS

for

establishment and operation of a ***INSERT STATION/SYSTEM TYPE*** for the purpose of carrying on

INSERT SERVICE

as specified in the **Terms and Conditions** as shown in the Annexures attached hereto.

Date of Issue: .....

Registration Fee.....

.....
Director-General

Form IV
(Regulation 9)

THE ZAMBIA INFORMATION AND COMMUNICATIONS TECHNOLOGY AUTHORITY

The Cyber Security and Cyber Crimes Act, 2021
(Act No. 2 of 2021)

The Cyber Security and Cyber Crimes (Critical Information Infrastructure) Regulations, 2021

APPLICATION FOR CHANGE OF OWNERSHIP				
		Shaded Fields for official use only	**Certificate code**	
			Date and Time	
Information Required		*Information Provided*		
1.	Certificate No.			
2.	Name of holder			
3.	Expiry date			
4.	Name of assignee			
	Nationality			
	Identity card (NRC) No. or Passport No.- (attach certified copies)			
5.	Holder's Address:			
	Tell:			
	Email:			
6.	Reasons for changes	(a)		
		(b)		
		(c)		
		(d)		
		(e)		
		(f)		
7.	Appendix			
	Appendix No. 1	Reasons for change of ownership		
	Appendix No. 2	any other relevant information as the Authority may require		
My Details - Attachments				

_____ _____
Applicant Date

_____ _____
Officer Date

FOR OFFICIAL USE ONLY

Received by _____
Officer

Amount Received: _____

Serial No. of application: _____

Form V
(Regulation (10)

THE ZAMBIA INFORMATION AND COMMUNICATIONS TECHNOLOGY AUTHORITY

The Cyber Security and Cyber Crimes Act, 2021
(Act No. 2 of 2021)

The Cyber Security and Cyber Crimes (Critical Information Infrastructure) Regulations, 2021

APPLICATION FOR TRANSFER OF CERTIFICATE OF REGISTRATION				
		Shaded Fields for official use only	**Certificate code**	
			Date and Time	
Information Required		*Information Provided*		
1.	Certificate No.			
2.	Current Holder			
3.	Name(s) of assignee(s)			
	Nationality of assignee(s)			
	Details of assignee	NRC No.		Passport No.
	Type of assignee	☐ Individual ☐ Partnership	☐ Company	
4.	Assignee's Address			
	Tell:			
	Email:			
5.	Appendices			
	Appendix No. 1	Reasons for transferring		
	Appendix No. 2	Any other relevant information as the Authority may require		
My Details – Attachments				

_____ _____
Applicant Date

_____ _____
Officer Date

FOR OFFICIAL USE ONLY

Received by _____
Officer

Amount Received: _____

Serial No. of application: _____

Form VI
(Regulation 10(6))

THE ZAMBIA INFORMATION AND COMMUNICATIONS TECHNOLOGY AUTHORITY

The Cyber Security and Cyber Crimes Act, 2021
(Act No. 2 of 2021)

The Cyber Security and Cyber Crimes (Critical Information Infrastructure) Regulations, 2021

NOTICE OF REJECTION OF TRANSFER OF CERTIFICATE

1. Here insert the full names and address of the applicant
2. Here insert ZICTA reference Number

TO (1) .....

.....

.....

IN THE MATTER OF (2) .....

You are notified that your application to transfer your certificate has been rejected.

The grounds for rejection of to the certificate are shown in the Annexures hereto.

Dated this ..... day of..... 20 .....

.....
Director-General

Form VII
(Regulation 11 (2))

THE ZAMBIA INFORMATION AND COMMUNICATIONS TECHNOLOGY AUTHORITY

The Cyber Security and Cyber Crimes Act, 2021
(Act No. 2 of 2021)

The Cyber Security and Cyber Crimes (Critical Information Infrastructure) Regulations, 2021

APPLICATION FOR CHANGES TO CRITICAL INFORMATION INFRASTRUCTURE				
		Shaded Fields for official use only	**Certificate code**	
			Date and Time	
My Details – Attachments				
Information Required		*Information Provided*		
1.	Certificate No.			
2.	Name of Holder			
3.	Name(s) of assignee(s)			
	Nationality of assignee(s)			
	Details of assignee	NRC No.	Passport No.	
	Type of assignee	☐ Individual ☐ Partnership	☐ Company	
4.	Assignee's Address			
	Tell:			
	Email:			
5.	Name of Critical Information Infrastructure			
6.	Appendices			
	Appendix No. 1	Reasons for change of Critical Information Infrastructure design, configuration, security or operation		
	Appendix No. 2	Details of change of Critical Information Infrastructure design, configuration, security or operation		
	Appendix No. 3	any other relevant information as the Authority may require		
My Details – Attachments				
_____ Applicant			_____ Date	

_____ _____ Officer Date
FOR OFFICIAL USE ONLY Received by _____ Officer Amount Received: _____ Serial No. of application: _____

Form VIII
(Regulation 11(3))

THE ZAMBIA INFORMATION AND COMMUNICATIONS TECHNOLOGY AUTHORITY

The Cyber Security and Cyber Crimes Act, 2021
(Act No. 2 of 2021)

The Cyber Security and Cyber Crimes (Critical Information Infrastructure) Regulations, 2021

NOTICE OF APPROVAL/REJECTION FOR CHANGES TO CRITICAL INFORMATION INFRASTRUCTURE

To **[Insert Applicant Name]** of **[Insert Applicant Address]**

IN THE MATTER OF [**Insert ZICTA Reference Number]** you are notified that your request to make changes to the critical information infrastructure has been approved/rejected.

The grounds for rejection to make changes to the critical information infrastructure are shown in the Annexures attached hereto.

Dated this **[Insert day]** day of **[Insert Month]** **[Insert Year]**

.....

Director-General

FOR OFFICIAL USE ONLY

This notice has, this **[Insert day]** day of **[Insert Month]** **[Insert Year]** been eneterd in the Register.

.....

Director-General

Form IX
(Regulation 14)

THE ZAMBIA INFORMATION AND COMMUNICATIONS TECHNOLOGY AUTHORITY

The Cyber Security and Cyber Crimes Act, 2021
(Act No. 2 of 2021)

The Cyber Security and Cyber Crimes (Critical Information Infrastructure) Regulations, 2021

Notes for Applicants

(a) In line with Section 19(1) of the Cyber Security and Cyber Crimes Act 2021 (Act), Critical Information Infrastructure (CII) shall be registered with the Authority, and the information shall be maintained by the Authority in line with Section 21 of the Act. Note:
   1. One form is required for each Critical Infrastructure Asset;
   2. If a CII owner wishes to change ownership of a Critical Information Infrastructure, they shall apply to the Authority in line with Section 20(1) of the Act.

(b) Instruction on completing the form:

(iii) 'Section 4: Asset Operator' Form can be duplicated if multiple asset operators exist, the Asset Operators number must be indicated in the text box at the top of the form.

(iv) All attachments must:
   1. be certified; and
   2. prove and/or relate to the information placed in the form(s). For example, 'Section 1: Critical Infrastructure Asset details' would require attachments such as; National Identity Card (National Registered Card), National Passport (Page 2 and 3), proof of incorporation or registration (in case of legal person).

(c) arrangement of interconnected:

   1. IT (Information Technology) refers to arrangement of interconnected computers that is used in the storing, accessing, processing, analysing and sending of information.
   2. OT (Operational Technology) refers to an arrangement of interconnected computers that is used in the monitoring and/or control of physical processes, that includes:
      (1) Supervisory control and data acquisition systems, distributed control systems, and other control system configuration such as programmable logic controllers;
      (2) A combination of control components, for example electrical, mechanical, hydraulic, pneumatic, that act together to achieve an

industrial objective (e.g. manufacturing, transportation of matter or energy).

(d) the asterisk * represents a mandatory requirement and must be completed.

(c) An incomplete application shall NOT be processed and shall require resubmission. This does not include sections with 'No' selected.

RENEWAL OF CERTIFICATE OF REGISTRATION

Current Certificate code	
Date - dd/mm/yyyy	

Section 1: Critical Infrastructure Asset details

Have any changes not already reported to the Authority been made in regard to this Section?

If Yes Complete this Section, If No, proceed to section 2.

☐Yes ☐No

1.1.	In what sector is the critical infrastructure asset you are registering?*: *Select one (1) Option*	
	☐Aviation ☐Banking & Finance ☐Energy ☐Government ☐Healthcare ☐Information and Communication ☐Land Transport ☐Manufacturing ☐Media ☐Security & Emergency ☐Water ☐Food ☐ Other (Specify):	
1.2.	Name of the Critical Infrastructure Asset*:	
1.3.	Location of the Asset*	
1.4.	Legal description of location, if available:	
1.5.	Describe the area that the Asset services. This information may be described in terms of the geographic locations in which services are provided. If the serviced area is in more than one State or Territory select all that apply. Documents can be attached to clarify or give further detail.*:	
	(a) Number of Provinces Serviced*:	
	(b) Province serviced*: *Select all that apply*	☐ Central ☐ Copperbelt ☐ Eastern ☐ Luapula ☐ Lusaka ☐ Muchinga ☐ North-Western ☐ Northern ☐ Southern ☐ Western ☐ Other (Specify):
1.6	Reason for Registration*: *Select one (1) Option*	☐ Existing holding - now captured within reporting threshold ☐ New Acquisition ☐ Other (Specify):

Asset Details – Attachments

You can submit a maximum of 10 documents supporting your registration.
Allowed file types are PDF, JPG, JPEG, PNG and XLSX.
Each of these documents can be up to 5 mb (Excel and PDF files can be 10 mb) in size.

Section 2: My Details

Have any changes not already reported to the Authority been made in regard to this Section?

If Yes Complete this Section, If No, proceed to section 3.

☐Yes ☐No

2.2	In what capacity are you submitting this registration*: *Select one (1) Option*	☐ Existing holding - now captured within reporting threshold ☐ New Acquisition ☐ Other (Specify):
2.3	Details of primary contact	
	(a) Your legal name	
	Title:	
	First Name *:	
	Middle Name:	

	Surname or Family Name *:	
	Employer's Name*:	
	(b) Employer's Address Street Address *: *PO Boxes are not acceptable*	
	City Or Town *:	
	Country *:	
	Province, State or Territory *:	
	Postcode or Zip code *:	
	Your job title / position *:	
	(c) Your preferred contact method: *Select one (1) Option*	☐ Email ☐ Primary telephone number ☐ Alternative telephone number
	(d) Your contact details	
	Your email address*:	
	Primary telephone number*: *Include country code*	
	Alternative telephone number*: *Include country code*	
2.4.	Details of secondary contact	
	(a)Their legal name	
	Title:	
	First Name *:	
	Middle Name:	
	Surname or Family Name *:	
	Employer's Name*:	
	(b)Employer's Address Street Address *: *PO Boxes are not acceptable*	
	City Or Town *:	
	Country *:	
	Province, State or Territory *:	
	Postcode or Zip code *:	
	(c) Your job title / position *:	
	(d) Your preferred contact method: *Select one (1) Option*	☐ Email ☐ Primary telephone number ☐ Alternative telephone number
	(e) Your contact details	
	Your email address*:	

	Primary telephone number*: *Include country code*	
	Alternative telephone number*: *Include country code*	

My Details – Attachments

You can submit a maximum of 10 documents supporting your registration. Allowed file types are PDF, JPG, JPEG, PNG and XLSX. Each of these documents can be up to 5 mb(Excel and PDF files can be 10 mb) in size.

Section 3: Responsible Entity

Have any changes not already reported to the Authority been made in regard to this Section?

If Yes Complete this Section, If No, proceed to section 4.

☐Yes ☐No

A Responsible Entity for an asset refers to:

- A controller of CII as interpreted in Section 2; or
- the entity that holds the certificate of registration , approval or authorisation (however described) to operate the asset and provide the service to be delivered by the asset;
- for an asset declared under section 17 to be a critical infrastructure asset—the entity specified in the declaration as the responsible entity for the asset (see subsection 17(1))

An entity can be an individual, a body corporate, a body politic, a partnership, a trust, a superannuation fund, or an unincorporated foreign company

3.1	Details Of Responsible Entity	
	(a) Legal name of Responsible Entity*:	
	(b) Type of entity*: *Select one (1) Option*	☐An individual Person ☐Body Corporate ☐Body Politic ☐ Superannuation Fund ☐Trust ☐Partnership ☐Unincorporated Foreign Company ☐ Other (Specify):
	(c) Country of incorporation or creation*:	
	(d) Business registration number *: *Company Registration Number or however described*	
	(e) Address of head office or principal place of business Street Address *: *PO Boxes are not acceptable*	
	City Or Town *:	
	Country *:	
	Province, State or Territory *:	
	Postcode or Zip code *:	
	(f) Original commencement date as Responsible Entity of this Asset*: *The month and year are mandatory, however, the day is optional*	

3.2 Operational information - Chief Executive Officer (or however described) of the Responsible Entity

	(a)Legal name	
	Title:	

	First Name *:	
	Middle Name:	
	Surname or Family Name*:	
	Country of citizenship*:	
	Country of dual citizenship: *If applicable*	
3.3	Operational information – Data Arrangements	
	(a) Provide a description of the arrangements under which data prescribed by the rules relating to the asset is maintained. You can attach documents to provide further details.*:	
3.4	Operational information – Other Operators of this Asset	
	(a) Are there any other entities that are Operators for this Critical Infrastructure asset?*: *IF No - proceed to Section 5 'Additional information and Declaration', IF Yes - proceed to Section 4 'Asset Operators'*	

Note: an operator is an entity that is authorised (however described) to operate the asset or part of the asset.

Responsible Entity – Attachments

You can submit a maximum of 10 documents supporting your registration.
Allowed file types are PDF, JPG, JPEG, PNG and XLSX.
Each of these documents can be up to 5 mb (Excel and PDF files can be 10 mb) in size.

Section 4: Asset Operator NO.

Have any changes not already reported to the Authority been made in regard to this Section?

If Yes Complete this Section, If No, proceed to section 'Asset Registry Requirements'.

☐Yes ☐No

Record details of entity that is defined as an operator of any parts of this critical asset. *If applicable*
Once all operators have been recorded, continue to the Declaration section.

4.1.	Operator Details	
	(a) Legal name of entity*:	
	(b) Type of entity*: *Select one (1) Option*	☐An individual Person ☐Body Corporate ☐Body Politic ☐Superannuation Fund ☐Trust ☐Partnership ☐Unincorporated Foreign Company ☐ Other (Specify):
	(c) Country of incorporation or creation*:	
	(d) Business registration number *: *Company Registration Number or however described*	
	(e) Address of head office or principal place of business	
	Street Address *: *PO Boxes are not acceptable*	
	City Or Town *:	
	Country *:	
	Province, State or Territory *:	
	Postcode or Zip code*:	

	(f) Original date the Operator commenced operating this asset*: *The month and year are mandatory, however, the day is optional*	
4.2	Operator arrangements	
	(a)Provide details of the arrangements (such as outsourcing or offshoring) under which this entity operates the Asset or part of the Asset. This would include a description of the arrangements if the control system of the asset is managed by a separate body. Documents can be attached to provide further information.*	

Asset Operators – Attachments

You can submit a maximum of 10 documents supporting your registration.
Allowed file types are PDF, JPG, JPEG, PNG and XLSX.
Each of these documents can be up to 5 mb (Excel and PDF files can be 10 mb) in size.

Asset Registry Requirements

Have any changes not already reported to the Authority been made in regard to this Section?

If Yes Complete this Section, If No, proceed to section 5.

☐Yes ☐No

CII ASSET INVENTORY

Instruction:
Enter a list of components/assets that make up the CII. Information relating to the identity, hardware, network, software and logging of each component/asset should be included.

LOGICAL NETWORK DIAGRAM REQUIREMENTS

Instruction:

FOR IT ENVIRONMENT

1. Depict logical connections of components within CII system.
2. Indicate IP address range of clusters/components within CII system (e.g. IP: 192.168.X.X/16)
3. Indicate all external connections (both internet facing and non-internet facing) from CII system:

FOR OT ENVIRONMENT

1. Depict logical connections of components within CII system:
2. Indicate IP address range of clusters/components within CII system (e.g. IP: 192.168.X.X/16)
3. Indicate all external connections (both internet facing and non-internet facing) from CII system:

INFORMATION ON INTERCONNECTED COMPUTER(S) OR COMPUTER SYSTEM(S)

Instruction:
Enter the list of computers/computer systems that are connected to the CII. Information relating to the identity, connections to CII, software and operator of the computers/computer systems should be included.

INTERNET LINKS SUPPORTING CII

Instruction:
Enter the list of internet links supporting the CII system and the DDoS mitigation in place for these links.

OUTSOURCED SERVICES SUPPORTING CII SYSTEM

	Instruction: Enter the list of services outsourced to third-party vendors for supporting CII system. Vendors providing Managed Security Services (MSS) for CII System should also be included.
CLOUD SOLUTIONS	
	Instruction: Enter the list of cloud services used to support CII system.
Section 5: Declaration	
Complete this Section	
5.1	Further Information
	(a) Provide any further information here that you believe is relevant and may assist the Authority:
5.2	Declaration
	I/we declare that all the particulars and information provided in this application are complete, correct and true and I/we agree that in the event that any of the said particulars and information provided is found to be untrue or fraudulent, the certificate of registration will be revoked. I/we agree that in the event of the revocation of the certificate of registration, any fee paid to the authority for certificate of registration shall be forfeited. I/we declare that in the event that the nature of my/our business changes, or I/we no longer carry out operations in terms of the registration, I/we will notify the Authority in which case my/our registration may be revoked or revised. Declared at ..... this ..... days of ..... 20..... by the following persons who are duly authorised to sign for and on behalf of the applicant under the authority of the Power of Attorney or Board resolution which is hereby attached.
	Name: *Name of individual filling in this form*
	Date: *Completion Date*
	Signature:
Declaration – Attachments	
You can submit a maximum of 10 documents supporting your registration. Allowed file types are PDF, JPG, JPEG, PNG and XLSX. Each of these documents can be up to 5 mb (Excel and PDF files can be 10 mb) in size.	
My Details – Attachments	

_____ Applicant	_____ Date
_____ Officer	_____ Date

FOR OFFICIAL USE ONLY

Received by _____ Officer _____ Date Received

Amount Received: _____

Serial No. of application: _____

Section 6: Attachments	
Complete this Section where/if applicable.	
6.1	Asset Details – Attachments
6.2	My Details – Attachments
6.3	Responsible Entity – Attachments
6.4	Asset Operators – Attachments
6.5	Asset Registry Requirements – Attachments

6.6	Declaration – Attachments

Form X
(Regulation 12(2))

THE ZAMBIA INFORMATION AND COMMUNICATIONS TECHNOLOGY AUTHORITY

The Cyber Security and Cyber Crimes Act, 2021
(Act No. 2 of 2021)

The Cyber Security and Cyber Crimes (Critical Information Infrastructure) Regulations, 2021

APPLICATION TO EXTERNALISE CRITICAL INFORMATION				
		Shaded Fields for official use only	**Certificate code**	
			Date and Time	
My Details				
Information Required		*Information Provided*		
1.	Certificate No.			
2.	Name of Holder			
3.	Name(s) of assignee(s)			
	Nationality of assignee(s)			
	Details of assignee	NRC No.	Passport No.	
	Type of assignee	☐ Individual ☐ Partnership	☐ Company	
4.	Assignee's Address			
	Tell:			
	Email:			
Details of Critical Information				
Information Required		*Information Provided*		
5.	Name of Critical Information			
6.	Purpose of Critical Information			
7.	Service for which Critical Information is required			
8.	Current Location of Critical Information (Country, City, Intuition)			
Details of External Host				

Information Required		*Information Provided*
9.	Location (Country & City)	
10.	Name of Host (Institution)	
11.	Type of External Host	☐ Data Centre ☐ Other(If other specify)
12.	Type of Hosting	☐ Private Cloud ☐ Public Cloud ☐ On Premise ☐ Hybrid Cloud
13.	Tier Level (Data Centre only)	☐ Tier 1 ☐ Tier 2 ☐ Tier 3 ☐ Tier 4 ☐ Tier 5
14.	Server Room Security (If selected 'Other' in '2.')	☐ ISO 27001 or equivalent conformant ☐Not ISO 27001 or equivalent conformant
Accessibility and Auditability		
15.	Can 24/7 facilitation for external auditing be provided to the regulator by the host? Both remotely and on premise?	
16.	The Certificate Holder (Controller) is to facilitate access by the Authority to the Critical Information located outside the Republic, baring all costs of not less than six authority officers for; a pre inspection (prior to application decision) and not less than 4 visits/inspections in a calendar year. The cost will include; logistics, government rated allowances, lodging, processing of Visa/renewable Visa for the specific period and any other related costs. Does the Certificate Holder agree?	
	☐Yes ☐No **Note**: The granting and maintenance of an externalisation approval is subject to a pre-inspection, continuous inspections, audits, reports and conformity with this section. Pre-inspection does not guarantee approval. An approval is Valid only for the Host specified at the location inspected.	
17.	Will the Controller be able to access, monitor and audit the critical information remotely?	
18.	Who will have access to the Critical Information (Third Parties)? (Attach additional pages as necessary)	

	No.	**Name**	**Title**	**Institution**
	1			
	2			
	3			
	4			
	5			

Availability, Redundancy and Backup		
19.	Will the Critical information or service for which the critical information is relevant still be available or be able to operate within the Republic in the event of connection failure to the outside of the Republic?	
20.	Is there a backup for the Critical Information? If yes, specify where (country and city), and if it is hosted by the Controller or by a third party (Name and Location)?	
	☐Yes ☐No	
Critical Information and Reasons for Externalisation		
21.	Is the Critical the Critical Information currently hosted in country?	
	☐Yes ☐No	
22.	Why do you want to externalise the Critical Information?	
Additional Information		
23.	Period for which the Critical Information will be located outside the Republic? Specify period and period expiration date.	
Appendices		
23.	Appendices	
	Appendix No. 1	Reasons for externalisation of Critical Information
	Appendix No. 2	Details of Prospective Hosting Institution
	Appendix No. 3	Details of Backup
	Appendix No. 4	Any other relevant information as the Authority may require

My Details – Attachments

_____ _____

Applicant Date

_____ _____

Officer Date

FOR OFFICIAL USE ONLY

Received by _____

Officer

Amount Received: _____

Serial No. of application: _____

Form XI
(Regulation 12(3))

THE ZAMBIA INFORMATION AND COMMUNICATIONS TECHNOLOGY AUTHORITY

The Cyber Security and Cyber Crimes Act, 2021
(Act No. 2 of 2021)

The Cyber Security and Cyber Crimes (Critical Information Infrastructure) Regulations, 2021

NOTICE OF APPROVAL/REJECTION TO EXTERNALISE CRITICAL INFORMATION

To **[Insert Applicant Name]** ..... of **[Insert Applicant Address]** .....

IN THE MATTER OF [**Insert ZICTA Reference Number]** you are notified that your request to externalise Critical Information has been approved/rejected.

The grounds for rejection to externalise Critical Information shown in the Annexures attached hereto.

Dated this ..... **[Insert day]** ..... day of ..... **[Insert Month]** ..... **[Insert Year]**

.....

MINISTER

FOR OFFICIAL USE ONLY

This notice has, this ..... **[Insert day]** ..... day of ..... **[Insert Month]** **[Insert Year]** been eneterd in the Register.

.....

Form XII
(Regulation 21)

THE ZAMBIA INFORMATION AND COMMUNICATIONS TECHNOLOGY AUTHORITY

The Cyber Security and Cyber Crimes Act, 2021
(Act No. 2 of 2021)

The Cyber Security and Cyber Crimes (Critical Information Infrastructure) Regulations, 2021

REGISTER OF CONTROLLERS					
CII Owner	**CII Controller (If applicable)**	**Type of CII**	**Sector**	**Date of Registration**	**Address**

Form XIII
(Regulation 23(2))

THE ZAMBIA INFORMATION AND COMMUNICATIONS TECHNOLOGY AUTHORITY

The Cyber Security and Cyber Crimes Act, 2021
(Act No. 2 of 2021)

The Cyber Security and Cyber Crimes (Critical Information Infrastructure) Regulations, 2021

Notes for Applicants

1. In line with Section 23 of the Cyber Security and Cyber Crimes Act, 2021, Controllers of Critical Information Infrastructure (CII)shall report cyber security incidents to Authority on or after the occurrence of an incidents for the following events:
   (a) Category 1 -
   (i) A cyber security incident in respect of the CII.
   (b) Category 2 -
   (i) A cyber security incident in respect of any computer or computer system under the controller's control that is interconnected with or that communicates with the CII.
   (c) Category 3 -
   (i) Any other type of cyber security incident.
2. Controllers/Sectorial CIRTs should fill Part 1 (Incident Details) as necessary, within 2 hours of discovering the incident.

CYBER SECURITY INCIDENT REPORTING – DETAILS

PART 1

Section A: General Information

A1. Sectorial CIRT or Controller that is reporting this incident (Choose only one option)

☐ Sectorial CIRT

- ☐ Organisation
- ☐ Aviation
- ☐ Banking & Finance
- ☐ Energy
- ☐ Government
- ☐ Healthcare
- ☐ Information and Communication
- ☐ Land Transport
- ☐ Manufacturing
- ☐ Media
- ☐ Security & Emergency
- ☐ Water
- ☐ Food

If Controller:

☐ CII Owner (Specify Organisation Name):

☐ Other (Specify Organisation Name):

A2. Informer's Information

Name: Enter text here.
Designation: Enter text here.
Organisation: Enter text here.
Email Address: Enter text here.
Telephone Number: Enter text here.

A3. This is a/an

☐ New incident
☐ Update to a previously reported incident

Sectorial CIRT's or CII Owner's reference number for this incident (if any).

Enter text here.

A4. This incident is classified under (refer to 'Notes for Applicants')

☐ **Category 1** –	☐ **Category 2** –	☐ **Category 3** –

Section B: Incident Details

B1. When did the Controller become aware of the incident?
(Please specify in Zambia Local Time GMT+2)

Date: Enter text here.
Time: Enter text here.

B2. When was the incident reported to the AC?
(Please specify in Zambia Local Time GMT+2)

Date: Enter text here.
Time: Enter text here.

B3. Types of Threats/Incidents (You may choose more than one option)

☐ Denial of Service (DoS)
☐ Distributed Denial of Service (DDoS)
☐ Virus/Worm/Trojan
☐ Intrusion/Hack/Unauthorised access
☐ Website Defacement
☐ Misuse of Systems/Inappropriate usage
☐ Other (If Other Specify): Enter text here.

B4. Is this incident related to another incident previously reported? (Indicate Yes or No)

Choose an option.

If "Yes", please provide more details.

Enter text here.

B5. Please provide, to the best of your knowledge, the following details in respect of CII affected by the Cyber security incident:

The number of CII affected by the incident:

Enter text here.

Name(s) of the CII: Enter text here.
Name(s) of CII Owner(s): Enter text here.
Email Address: Enter text here.
Telephone Number: Enter text here.

B6. Please provide further details of the CII that is/are affected by this incident. Details should minimally include:

Location, purpose of the CII, hardware and software affected (please list details of hardware manufacturer, software developer, make/model, etc.).

Enter text here.

Where relevant, please indicate the Operating System (OS) of the affected CII:

☐ Microsoft Windows
☐ Linux/Unix
☐ Mac OS
☐ Other (If Other Specify): Enter text here.

If "other", please indicate the OS here: Enter text here.

B7. Please provide the following details relating to the Cyber security incident:

To the best of your knowledge, when did the incident occur? (Please specify in Zambia Local Time GMT+2)

Date: Enter text here. Unknown: ☐
Time: Enter text here.

If "Unknown", when was the incident first observed?
(Please specify in Zambia Local Time GMT+2)

Date: Enter text here.
Time: Enter text here.

To the best of your knowledge, how did the incident occur?
Enter text here.

How was the incident first observed/sighted/detected?

Enter text here.

B8. What are the effects that have been observed to result from the Cyber security incident? This includes any effect on the CII and interconnected computers or computer systems, and any effect on the CII Owner(s), licensee(s) and/or users of the essential service supported by the affected CII (e.g. service performance degradation, disruption to service availability, loss of personal data, loss of business data, loss of log information, etc.).

Enter text here.

B9. Where the CII mentioned above has/have been adversely affected, is there any potential effect on other critical asset(s) owned or controlled by the CII Owner(s)/licensee(s)? (e.g., where a domain controller has been compromised, other systems using domain credentials from the domain controller may be affected)

Enter text here.

If "Yes", please provide more details.

Enter text here.

B10. To the best of your knowledge, where the CII mentioned above has/have been adversely affected, is there any potential effect on asset(s) belonging to other CII Controller(s) (not necessarily from the same sector)? (Indicate Yes or No)

Enter text here.

If "Yes", please provide more details.

Enter text here.

Form XIV
(Regulation 23(4))

THE ZAMBIA INFORMATION AND COMMUNICATIONS TECHNOLOGY AUTHORITY

The Cyber Security and Cyber Crimes Act, 2021
(Act No. 2 of 2021)

The Cyber Security and Cyber Crimes
(Critical Information Infrastructure) Regulations, 2021

Notes for Applicants

3. In line with Section 23 of the Cyber Security and Cyber Crimes Act, 2021, Controllers of Critical Information Infrastructure (CII)shall report cyber security incidents to Authority on or after the occurrence of an incidents for the following events:
   (a) Category 1 -
   (i) A cyber security incident in respect of the CII.
   (b) Category 2 -
   (i) A cyber security incident in respect of any computer or computer system under the Controller's control that is interconnected with or that communicates with the CII.
   (c) Category 3 -
   (i) Any other type of cyber security incident.
4. Controllers should complete Part 2 (Incident Handling Status) and fill in/amend and Part 1 (Incident Details) if applicable, within 5 days after making the report.

CYBER SECURITY INCIDENT REPORTING - INCIDENT HANDLING STATUS

(If Applicable)

ZICTA Reference Number (to be filled in by the individual completing the Form):

Enter text here

Section A: General Information

A1. Sectorial CIRT or Controller that is reporting this incident (Choose only one option)

☐ Sectorial CIRT

- ☐ Organisation
- ☐ Aviation
- ☐ Banking & Finance
- ☐ Energy
- ☐ Government
- ☐ Healthcare
- ☐ Information and Communication
- ☐ Land Transport
- ☐ Manufacturing
- ☐ Media
- ☐ Security & Emergency
- ☐ Water
- ☐ Food

If Controller:

☐ CII Owner (Specify Organisation Name):

☐ Other (Specify Organisation Name):

A2. Informer's Information

Name: Enter text here.
Designation: Enter text here.
Organisation: Enter text here.
Email Address: Enter text here.
Telephone Number: Enter text here.

A3. This is a/an

☐ New incident
☐ Update to a previously reported incident

Sectorial CIRT's or CII Owner's reference number for this incident (if any).

Enter text here.

A4. This incident is classified under (refer to 'Notes for Applicants')

☐ **Category 1** –	☐ **Category 2** –	☐ **Category 3** –

Section B: Incident Details

B1. When did the Controller become aware of the incident?
(Please specify in Zambia Local Time GMT+2)

Date: Enter text here.
Time: Enter text here.

B2. When was the incident reported to the AC?
(Please specify in Zambia Local Time GMT+2)

Date: Enter text here.
Time: Enter text here.

B3. Types of Threats/Incidents (You may choose more than one option)

☐ Denial of Service (DoS)
☐ Distributed Denial of Service (DDoS)
☐ Virus/Worm/Trojan

☐ Intrusion/Hack/Unauthorised access
☐ Website Defacement
☐ Misuse of Systems/Inappropriate usage
☐ Other (If Other Specify): Enter text here.

B4. Is this incident related to another incident previously reported? (Indicate Yes or No)

Choose an option.

If "Yes", please provide more details.

Enter text here.

B5. Please provide, to the best of your knowledge, the following details in respect of CII affected by the Cyber security incident:

The number of CII affected by the incident:

Enter text here.

Name(s) of the CII:	Enter text here.
Name(s) of CII Owner(s):	Enter text here.
Email Address:	Enter text here.
Telephone Number:	Enter text here.

B6. Please provide further details of the CII that is/are affected by this incident. Details should minimally include:

Location, purpose of the CII, hardware and software affected (please list details of hardware manufacturer, software developer, make/model, etc.).

Enter text here.

Where relevant, please indicate the Operating System (OS) of the affected CII:

☐ Microsoft Windows
☐ Linux/Unix
☐ Mac OS
☐ Other (If Other Specify): Enter text here.

If "other", please indicate the OS here: Enter text here.

B7. Please provide the following details relating to the Cyber security incident:

To the best of your knowledge, when did the incident occur? (Please specify in Zambia Local Time GMT+2)

Date: Enter text here. Unknown: ☐
Time: Enter text here.

If "Unknown", when was the incident first observed?
(Please specify in Zambia Local Time GMT+2)

Date: Enter text here.
Time: Enter text here.

To the best of your knowledge, how did the incident occur?
Enter text here.

How was the incident first observed/sighted/detected?

Enter text here.

B8. What are the effects that have been observed to result from the Cyber security incident? This includes any effect on the CII and interconnected computers or computer systems, and any effect on the CII Owner(s), licensee(s) and/or users of the essential service supported by the affected CII (e.g. service performance degradation, disruption to service availability, loss of personal data, loss of business data, loss of log information, etc.).

Enter text here.

B9. Where the CII mentioned above has/have been adversely affected, is there any potential effect on other critical asset(s) owned or controlled by the CII Owner(s)/licensee(s)? (e.g., where a domain controller has been compromised, other systems using domain credentials from the domain controller may be affected)

Enter text here.

If "Yes", please provide more details.

Enter text here.

B10. To the best of your knowledge, where the CII mentioned above has/have been adversely affected, is there any potential effect on asset(s) belonging to other CII Controller(s) (not necessarily from the same sector)? (Indicate Yes or No)

Enter text here.

If "Yes", please provide more details.

Enter text here.

PART 2

ZICTA Reference Number (to be filled in by the individual completing the Form):

Section C: Incident Handling Status

C1. What is/are the type(s) of follow-up action(s) that has/have been taken at this time?

Enter text here.

C2. What is the current status or resolution of this incident?

Enter text here.

C3. If it has not been resolved, what is the next course of action?

Enter text here.

C4. What is the earliest known date of attack or compromise? If earliest known date is unknown, please indicate accordingly. (Please specify in Zambia Local Time GMT+2)

Date: Enter text here. Unknown: ☐
Time: Enter text here.

C5. What is the source/cause of the incident? (Indicate 'NIL' if unknown)

Enter text here.

C6. Has the incident been reported to any law enforcement agency?

☐ Yes
☐ No
☐ Unknown

If "Yes", please specify which agency has the incident been reported to.

Enter text here.

Section D: Other Information

D1. IP Addresses (Required if surfaced from the incident)

Please provide the list of IP addresses surfaced from the incident. Please state the involvement of the IP addresses in the incident (e.g. Victim, Malware Command & Control Servers, etc.). If IP addresses were resolved from domain names, please specify the domain names and the date/time of resolution of IP addresses from the domain names.

IP Address	Involvement	Domain name from which IP address was resolved	Date/Time of Resolution of IP address from Domain name
Enter text here.	Enter text here.	Enter text here.	Enter text here.
Enter text here.	Enter text here.	Enter text here.	Enter text here.
Enter text here.	Enter text here.	Enter text here.	Enter text here.
Enter text here.	Enter text here.	Enter text here.	Enter text here.
Enter text here.	Enter text here.	Enter text here.	Enter text here.

D2. Domain Names (Required if surfaced from the incident)

Please provide the list of domains surfaced from the incident. Please state the involvement of the domain names in the incident. (e.g. Drive-by-download Servers, Malware Control & Command Servers, defaced website)

Domain Name	Involvement of Domain name
Enter text here.	Enter text here.
Enter text here.	Enter text here.
Enter text here.	Enter text here.
Enter text here.	Enter text here.
Enter text here.	Enter text here.

D3. Email Addresses (Required if surfaced from the incident)

Please provide the list of email addresses surfaced from the incident. Please state the involvement of the email addresses in the incident. For example, an email address from which a phishing email appears to have be sent from, etc.

Email Address	**Involvement of Email Address**
Enter text here.	Enter text here.
Enter text here.	Enter text here.
Enter text here.	Enter text here.
Enter text here.	Enter text here.
Enter text here.	Enter text here.

D4. Malicious Files (Required if surfaced from the incident)

Please provide information on the malicious files surfaced from the incident in the box below.

Filename	**Size**	**MD5 hash**	**Technical Analysis (Yes/No)**
Enter text here.	Enter text here.	Enter text here.	Enter text here.
Enter text here.	Enter text here.	Enter text here.	Enter text here.
Enter text here.	Enter text here.	Enter text here.	Enter text here.
Enter text here.	Enter text here.	Enter text here.	Enter text here.
Enter text here.	Enter text here.	Enter text here.	Enter text here.

D5. Please provide an assessment of the sectoral situational awareness.
(This section is applicable to Sectorial CIRT(s) only)

Enter text here.

Form XV
(Regulation 25)

THE ZAMBIA INFORMATION AND COMMUNICATIONS TECHNOLOGY AUTHORITY

The Cyber Security and Cyber Crimes Act, 2021
(Act No. 2 of 2021)

The Cyber Security and Cyber Crimes (Critical Information Infrastructure) Regulations, 2021

REQUEST FOR INFORMATION AND/OR DOCUMENTS

To **[Insert Applicant Name]** ..... of **[Insert Applicant Address]** .....

IN THE MATTER OF [**Insert ZICTA Reference Number]** you are requested to submit information and/or documents in respect of your status as a Critical Information Infrastructure controller.

The information and/or documentation required are shown in the Annexures attached hereto.

Dated this ..... **[Insert day]** ..... day of ..... **[Insert Month]** ..... **[Insert Year]**

.....

Director-General

FOR OFFICIAL USE ONLY

This notice has, this ..... **[Insert day]** ..... day of ..... **[Insert Month]** ..... **[Insert Year]** been eneterd in the Register.

.....

Director-General

Form XVI
(Regulation .....)

THE ZAMBIA INFORMATION AND COMMUNICATIONS TECHNOLOGY AUTHORITY

The Cyber Security and Cyber Crimes Act, 2021
(Act No. 2 of 2021)

The Cyber Security and Cyber Crimes (Critical Information Infrastructure) Regulations, 2021

CERTIFICATE OF APPOINTMENT AS CYBER INSPECTOR PURSUANT TO SECTION 8 OF THE CYBER SECURITY AND CYBER CRIMES ACT NO. 2 OF 2021 (THE ACT).

THIS IS TO CERTIFY that the Authority, in exercise of its powers under section 8 of the Cyber Security and Cyber Crimes Act No. 2 of 2021 (the Act), hereby appoints (Insert Name)…….whose National Registration Card Number is (Insert NRC Number)……. as a **Cyber Inspector**.

By this certificate (Insert Name)…… is authorised to exercise the powers of a Cyber Inspector as provided for in the Act.

TAKE NOTICE that as a **Cyber Inspector**, the said (Insert Name)…….. shall carry out the functions of the cyber inspector within the confines of the law .

Dated this …… day of ……. **2021**

SIGNATURE: _____

NAME: _____

_____

POSITION: DIRECTOR GENERAL

_____

FOR AND ON BEHALF OF THE AUTHORITY

SECOND SCHEDULE
(Regulations 6, 10, 11 and 13)

	Fee Units
Registration of Critical Information Infrastructure	1667
Renewal of Certificate of Registration	1667
Change of ownership of Critical Information Infrastructure	1667
Transfer of Certificate of Registration	1667

	Annual Fee
Externalisation of Critical Information	0.5% of the previous annual turnover

	Percentage
Percentage of total revenue collected by the Authority and payable to the Treasury	20

,

Minister of Technology and Science

LUSAKA

, 2021

[ ]