STATUTORY INSTRUMENT NO. OF 2021

The Cyber Security and Cyber Crimes Act, 2022
(Act No. 2 of 2022)

The Cyber Security and Cyber Crimes (Critical Information Infrastructure) Regulations, 2022

ARRANGEMENT OF REGULATIONS

IN EXERCISE of the powers contained in section 90 of the Cyber Security and Cyber Crimes Act, the following Regulations are made:

PART I
PRELIMINARY

Title

1. These Regulations may be cited as the Cyber Security and Cyber Crimes (Critical Information Infrastructure) Regulations 2022

Interpretation

2. In these Regulations, unless the context otherwise requires -

"cyber audit" includes vulnerability assessment, penetration testing and risk assessment;

"cyber dependence" means a relationship among vital or essential services where one vital or essential service can influence the state of other vital or essential services;

"cyber security maturity assessment" means a tool that is used to examine an institution's security posture including, the examination of security capabilities for prevention, detection, response, governance, security foundations and threat intelligence, and provides the current and target maturity scores;

Act No. 3 of 2021

"processing" has the meaning assigned to the word in the Data Protection Act, 2021;

Act No. 3 of 2021

"sensitive personal data" has the meaning assigned to the words in the Data Protection Act, 2021;

"time criticality" means the point at which the disruption of the vital or essential service is likely have grave impact on society.

Prohibition against use of unlicenced person

3. (1) A controller shall not engage an unlicensed person to provide cyber security services.

(2) A controller who contravenes sub-regulation (1) commits an offence.

Declaration of critical information and critical information infrastructure

4. (1) The following information is declared critical information for the purposes of these Regulations:

(a) information processed by a public body;

(b) information processed by operators of electronic communications networks and the providers of electronic communications services;

(c) information relating to the following sectors:

(i) banking and financial services;

(ii) health;

(iii) transport and communication;

(iv) defence and national security;

(v) energy;

(vi) insurance;

(vii) education;

(viii) taxation; or

(ix) mining;

(d) location based or mapping data;

(e) sensitive personal data;

(f) information processed by sector computer incident response teams; and

(g) configuration settings of critical information infrastructure.

(2) An infrastructure on which the critical information in sub-regulation (1) is contained and any other infrastructure connected thereto is declared critical information infrastructure.

(3) Infrastructure that is essential to the provision of the following vital services is declared critical information infrastructure:

(a) generation, supply or distribution of electricity;

(b) medical or hospital;

(c) water supply and sewerage;

(d) education;

(e) agriculture;

(f) digital financial services;

(g) internet banking;

(h) automatic teller machines;

(i) payment gateway;

(j) aviation operation;

(k) data center;

(l) broadcasting;

(m) fire and police;

(n) emergency services;

(o) metrological services;

(p) transportation services;

(q) tax collection;

(r) payment switch services;

(s) mineral mining and operation; or

(t) any other services that the Authority may by declaration determine as vital services.

Identification of critical information infrastructure

5. The Authority shall in identifying critical information infrastructure consider-

(a) the impact of the loss of the services referred to in regulation 4(3) on -

(i) the economy;

(ii) public health and safety;

(iii) social wellbeing of the public;

(iv) governance of the nation; and

(v) cyber dependence.

(b) the following factors relating to the impact referred to in paragraph (a):

(i) scale of distribution of the impact;

(ii) time criticality; and

(iii) the effects of the loss of vital or essential services on the public.

PART II

REGISTRATION OF CRITICAL INFORMATION INFRASTRUCTURE

Application for registration of critical information infrastructure

6. A controller shall apply to the Authority for registration of a critical information infrastructure in Form I set out in the First Schedule.

Request for further particulars

7. The Authority may, request the controller to submit further particulars, within a specified period in relation to an application in Form II set out in the First Schedule.

Issue certificate of registration

8. The Authority shall where the controller meets the requirements of the Act, issue a certificate of registration in Form III set out in the First Schedule.

Rejection of application

9. The Authority shall, where the Authority rejects the application, inform the applicant within fourteen days from the date of the decision of the rejection in Form IV set in the First Schedule.

Application for change in ownership of critical information infrastructure

10. A controller who intends to change ownership of the critical information infrastructure, shall apply to the Authority in Form V set ut in the First Schedule.

Transfer of certificate of registration

11. (1) A controller who intends to transfer a certificate of registration shall apply to the Authority in Form VI set out in the First Schedule.

(3) An application to transfer a certificate of registration shall be accompanied by an application for registration made by a prospective transferee.

(4) The Authority shall, within thirty days of receipt of an application for the transfer of a certificate of registration -

(a) approve the transfer of the certificate of registration; and

(b) endorse on the certificate of registration the details of the new holder of the certificate of registration.

(5) The Authority shall reject an application to transfer the certificate of registration if the applicant fails to comply with the conditions for the grant of the certificate of registration, and the provisions of the Act.

(6) The Authority shall, where it rejects an application to transfer a certificate of registration under sub-regulation (5), inform the applicant in Form VII set out in the First Schedule.

Changes to critical information infrastructure

12. (1) A controller shall not without the prior approval of the Authority make any change to the design, configuration, security or operation of a critical information infrastructure.

(2) A controller who intends to make any change in the design, configuration, security or operation of a critical information infrastructure shall apply to the Authority in Form VIII set out in the First Schedule.

(3) The Authority may approve or reject an application in sub-regulation (1) within thirty days after the receipt of such application.

PART III
LOCALISATION OF CRITICAL INFORMATION

Localisation of critical information

13. (1) A controller shall ensure that infrastructure on which critical information is contained is located in the Republic.

(2) A controller who intends to externalise critical information shall apply to the Minister in Form VI set out in the First Schedule.

(3) The Minister may approve or reject the application in sub-regulation (2), within thirty days of receipt of the application and inform the applicant in Form X set out in the First Schedule.

(4) The Minister may, in considering an application by a controller to externalise critical information, take into account-

(a) security measures being applied to the information and infrastructure on which the information is contained are adequate;

(b) whether it is necessary for the information to be stored outside the geographical jurisdiction of the Republic;

(c) national security;

(d) submissions by concerned data controller;

(e) consent by the data subject; and

(f) any other factors that the Ministers considers necessary.

(5) The Minister shall consult the Authority, the Council and relevant security agencies when considering an application in sub-regulation (4).

PART IV
GENERAL PROVISIONS

Mandatory measures for critical information infrastructure

14. (1) A controller of a critical information infrastructure shall implement effective measures for-

(a) the physical security of the hardware and other infrastructure

where the critical information infrastructure is located;

(b) limitation of access to the critical information infrastructure or information stored in the critical information infrastructure;

(c) periodic maintenance and security testing;

(d) timely and uninhibited access to the critical information Infrastructure by authorised persons;

(e) administrative control of personnel having access to various components of the critical information infrastructure;

(f) limitations on use of removable storage devices;

(g) security and disaster recovery; and

(h) any other measures that the Authority may determine.

(2) A controller of a critical information infrastructure shall incorporate the measures referred to in sub-regulation (1) into written institutional policies, procedures and codes of practice.

Integration of critical information

15. (1) A controller of critical information shall not integrate or permit the integration of the critical information infrastructure with any information

infrastructure belonging to a third party without notifying the Authority.

(2) A controller of a critical information infrastructure shall not integrate the critical information infrastructure third party that does not have in place measures to ensure that the security of the critical information infrastructure is not compromised.

(3) A controller shall ensure access to the critical information infrastructure is provided in accordance with standards issued by the Authority.

(4) A controller of a critical information infrastructure shall not, without lawful authority, transfer critical information through migration or replication from a critical information infrastructure to a third party.

Securing integrity and authenticity of critical information

16. (1) A controller of a critical information infrastructure shall implement measures to ensure that a building, room or other structure in which a critical information infrastructure is located has -

(a) sufficient cooling mechanism to prevent overheating of equipment;

(b) equipment to prevent or mitigate the effect of a fluctuation of an electric load; and

(c) any other measures necessary to maintain the integrity of the critical

information infrastructure.

(2) A person in control of a critical information infrastructure shall ensure that infrastructure is not used for general storage of any material that is not connected to the operation or maintenance of the database.

(3) A controller shall develop a system of security clearance levels for personnel and third parties who have access to a critical information infrastructure.

(4) A controller shall maintain a register of persons having access to a critical information specifying-

(a) the name and residential address of the person;

(b) the designation of the person within the institution;

(c) the nationality of the person accessing the critical information;

(d) the extent of the authorisation and restrictions applicable to the person in relation to utilisation of the critical information infrastructure;

(e) the details of the third party and extent to which that third party has access to the critical information;

(f) the general level of security

clearance a person enjoys in relation to a critical information infrastructure.

(5) A controller shall ensure that a person in charge of critical information is a fit and proper.

Procedures and technological methods for use in storage or archive of critical information infrastructure

17. (1) A controller may, where critical information is stored in a critical information infrastructure is no longer immediately required for use, place the information in an archive for storage.

(2) Where critical information has been stored in an archive, the same security requirements, policies, procedures and codes of practice that apply to critical information infrastructure shall apply to archived critical information.

(3) A controller shall keep a register of all critical information that has been archived stating the date on which the information was archived and the persons authorised to access the archived information.

Disaster recovery and backup site

18. (1) A controller shall have a disaster recovery and backup site which may be independent of each other and shall be independent from the location of the critical information infrastructure.

(2) A backup of critical information created under sub-regulation (1) shall be stored in a format that will permit the retrieval of the information and

restoration of an infrastructure in the event of a compromise or destruction of the infrastructure.

Business continuity plan

19. A controller shall submit a business continuity plan to the Authority annually.

Risk assessment and evaluation or critical information infrastructure

20. (1) A controller shall conduct a risk assessment of the institution based on the following elements:

(a) evaluation of organisational security policies, procedures, codes of practice and the structuring of the security function of the institution;

(b) evaluation of the methodology applied in management of the security procedures and the availability of tools to ensure security of the computer system and of the mode of utilising the tools;

(c) technical analysis of the security of all components of the computer system by conducting system integrity tests to ensure system resistance to all kinds of dangers; and

(d) analysis and evaluation of dangers that could result from operating with any deficiencies discovered

during the risk assessment exercise.

(2) A risk assessment exercise may be carried out by the Authority or a licensed cyber security service provider.

(3) A person carrying out a risk assessment exercise shall, at the conclusion of the exercise, deliver to the controller and the Authority a report verified under the hand and seal, where applicable, of that person, confirming the completeness and correctness of the report.

(4) A report submitted to a person under sub-regulation (3) shall contain-

(a) a description and complete evaluation of the security of the critical information infrastructure, including the measures adopted since the previous risk assessment, if any, and the deficiencies observed in the implementation of recommendations;

(b) a detailed analysis of the organisational and technical deficiencies regarding the security procedures and tools adopted including an evaluation of the risks that could result from operating with the deficiencies discovered; and

(c) proposed organisational and

technical security solutions to be adopted in order to overcome the shortcomings noted.

(5) A controller shall cause a risk assessment of the institution to be carried out at least once every twelve months.

(6) Despite sub regulation (5) a controller shall ensure that a risk assessment of a critical information infrastructure is carried out within six months of the date of these Regulations.

(7) The Authority may extend the period referred to in sub-regulation (5), where there are special circumstances that require the extension of the stipulated period, on a request from a controller, in writing, submitted not less than ninety days before the deadline for the conduct of the risk assessment exercise.

(8) A controller shall, not later than ten days after the receipt of the risk assessment report, submit a copy of the report to the Authority at least once every twelve months.

(9) The Authority may, after studying the risk assessment report, request the controller to provide the Authority with further information, and may carry out an inspection of the institution for the purposes of verification of the matters relating to the risk assessment.

(10) The Authority may reject a risk assessment report where -

(a) the risk assessment is carried out in contravention of these Regulations or any other stipulated procedures; or

(b) the risk assessment report does not contain material information regarding the deficiencies identified by the exercise.

Cyber Security maturity assessment

21. (1) A controller shall undertake a cyber security maturity assessment within sixty days from the date of these Regulations and subsequently as the Authority may determine.

(2) A controller shall in conducting a risk assessment and implementing security measures take into account the cyber security maturity assessment determined by the Authority.

(3) A controller shall submit to the Authority a cyber security maturing assessment report as determined by the Authority.

Monthly Report

22. (1) A controller shall submit a monthly cyber security incident and threat report to the Authority as may be determined by the Authority in guidelines.

(2) A report in sub regulation (1) shall include statistics on the following:

(a) malware attack;

(b) spam attack;

(c) phishing attacks;

(d) web based attacks

(e) insider threat;

(f) ransomware attacks;

(g) malware attacks;

(h) failure or disruption of computer system;

(i) failure or disruption of a third party service provider;

(j) cyber attack; and

(k) botnets attacks.

Register of controllers

23. The Authority shall maintain a register of controllers in Form XI set out in the First Schedule.

Appointment of information technology auditors

24. A controller shall ensure that the Information Technology Auditor appointed to conduct a cyber audit on a critical information infrastructure holds the requisite licence to provide a cyber security service.

Report on cyber security incidents in respect of critical information infrastructure

25. (1) A controller shall report to the Authority any cyber security incident, including -

(a) unauthorised hacking of the critical

information infrastructure, interconnected computer or computer system to gain access to or control of the critical information infrastructure, interconnected computer or computer system;

(b) installation or execution of unauthorised software, or computer code, of a malicious nature on the critical information infrastructure, the interconnected computer or computer system;

(c) unauthorised interception using a computer or computer system of communication between the critical information infrastructure or the interconnected computer or computer system, and an authorised user of the critical information infrastructure or the interconnected computer or computer system, as the case may be;

(d) denial of service attack or other unauthorised act carried out through a computer or computer system that adversely affects the availability or operability of the

critical information infrastructure or the interconnected computer or computer system.

(2) A controller shall report a cybersecurity incident to the Authority as soon as practicable but not later than two hours of becoming aware of the occurrence in Form XII set out in the First Schedule.

(3) The report referred to in sub-regulation (1) shall contain the following information:

(a) the critical information infrastructure affected;

(b) the name and contact details of the controller;

(c) the nature of the cybersecurity incident, whether it was in respect of the critical information infrastructure or an interconnected computer or computer system, when and how it occurred;

(d) the effect of the cybersecurity incident on the critical information infrastructure or any interconnected computer or computer system;

(e) the name, designation, organisation and contact details of the individual reporting the incident to the Authority;

(4) A controller shall within five calendar days after the submission of the report referred to in sub regulation (1) provide a report in Form XIII set out in the First Schedule containing:

(a) the cause of the cybersecurity incident;

(b) the impact of the cybersecurity incident on the critical information infrastructure, any interconnected computer or computer system; and

(c) remedial measures undertaken.

(5) A controller may submit a report electronically through the Authority's website or electronic mail.

Obligation to report cyber security incidents

26. (1) A controller shall establish mechanisms and systems for the detection and reporting of incidents to the Authority's incident monitoring system as prescribed by the Authority.

(2) A controller who fails to comply with sub-regulation (1) commits an offence.

Provision of information to the Authority

27. The Authority may request the controller to submit documents or any information that the Authority may require for the purposes of these Regulations in Form XIV set out in the Schedule.

Audit

28. (1) A controller shall ensure that a critical information infrastructure is audited annually.

(2) A controller who fails to comply with sub-regulation (1) commits an offence and is liable on conviction to a fine not exceeding five hundred thousand penalty units or to imprisonment for a term not exceeding five years or to both.

Fees

29. The fee payable for registration of critical information infrastructure and externalization of critical information is as set out in the Second Schedule.

Transitional provision

30. (1) The following transitional periods shall, unless directed otherwise by the Authority, apply following the issuance of these Regulations:

(a) a controller shall within one month submit the first monthly incident and threat report;

(b) a controller shall submit the first audit report within six months;

(c) a controller shall within two months implement incident detection and reporting mechanisms to the Authority; and

(d) a controller shall within twelve months localise critical information that was externalised.

(2) The Authority may, in consultation with the Data Protection Commissioner prescribe terms and conditions for the return of the externalised critical information.