
**THE CYBER SECURITY AND CYBER CRIMES
ACT, 2021**

ARRANGEMENT OF SECTIONS

PART I
PRELIMINARY PROVISIONS

Section

1. Short title and commencement
2. Interpretation
3. Supremacy of Act

PART II
REGULATION OF CYBER SECURITY SERVICES

4. Cyber security regulator
5. Functions of Authority
6. Constitution of Zambia Computer Incidence Response Team
7. Constitution of National Cyber Security, Advisory and Co-ordinating Council

PART III
INSPECTORATE

8. Appointment of cyber inspector
9. Power to inspect and monitor
10. Data retention notice
11. Power to access, search and seize
12. Obstruction of cyber inspector
13. Appointment of cyber security technical expert
14. Emergency cyber security measures and requirements

PART IV
INVESTIGATION OF CYBER SECURITY INCIDENTS

15. Power to investigate

PART V
PROTECTION OF CRITICAL INFORMATION INFRASTRUCTURE

16. Scope of protecting critical information infrastructure
17. Declaration of critical information
18. Localisation of critical information
19. Registration of critical information infrastructure

-
20. Change in ownership of critical information infrastructure
 21. Register of critical information infrastructure
 22. Auditing of critical information infrastructure to ensure compliance
 23. Duty to report cyber security incident in respect of critical information infrastructure
 24. National cyber security exercises
 25. Non-compliance with Part V

PART VI

INTERCEPTION OF COMMUNICATION

26. Prohibition of interception of communications
27. Central Monitoring and Co-ordination Centre
28. Lawful interception
29. Interception of communication to prevent bodily harm, loss of life or damage to property
30. Interception of communication for purposes of determining location
31. Prohibition of disclosure of intercepted communication
32. Disclosure of intercepted communication by law enforcement officer
33. Privileged communication to retain privileged character
34. Prohibition of random monitoring
35. Protection of user from fraudulent or other unlawful use of service
36. Interception of satellite transmission
37. Prohibition of use of interception device
38. Assistance by service provider
39. Duties of service provider in relation to customers
40. Interception capability of service provider

PART VII

LICENSING OF CYBER SECURITY SERVICE PROVIDERS

41. Prohibition from providing cyber security service without licence
42. Application for licence
43. Renewal of licence
44. Refusal to grant or renew licence
45. Validity of licence
46. Revocation or suspension of licence

PART VIII

INTERNATIONAL COOPERATION IN MAINTAINING
CYBER SECURITY

- 47. Identifying areas of cooperation
- 48. Entering into agreement

PART IX

CYBER CRIME

- 49. Unauthorised access to, interception of or interference with
computer system or data
- 50. Illegal devices and software
- 51. Computer related misrepresentation
- 52. Cyber extortion
- 53. Identity related crimes
- 54. Publication of information
- 55. Aiding, abetting, counselling etc
- 56. Prohibition of pornography
- 57. Child pornography
- 58. Child solicitation
- 59. Obscene matters or things
- 60. Introduction of malicious software into computer system
- 61. Denial of service attacks
- 62. Unsolicited electronic messages
- 63. Prohibition of use of computer system for offences
- 64. Application of offences under this Act
- 65. Hate speech
- 66. Minimisation etc of genocide and crimes against humanity
- 67. Unlawful disclosure of details of investigation
- 68. Obstruction of law enforcement officer or cyber inspection
officer
- 69. Harassment utilising means of electronic communication
- 70. Cyber terrorism
- 71. Cyber attack
- 72. Cognizable offence

PART X

ELECTRONIC EVIDENCE

- 73. Admissibility of electronic evidence

PART XI

GENERAL PROVISIONS

- 74. Appeals
- 75. Search and seizure
- 76. Prohibition of disclosure of information to unauthorised persons
- 77. Assistance
- 78. Production order
- 79. Expedited preservation
- 80. Partial disclosure of traffic data
- 81. Collection of traffic data
- 82. No monitoring obligation
- 83. Limitation of liability
- 84. Extradition
- 85. Evidence obtained by unlawful interception not admissible
in criminal proceedings
- 86. General penalty
- 87. Power of court to order cancellation of licence, forfeiture
etc.,
- 88. Guidelines
- 89. Exemptions
- 90. Regulations

GOVERNMENT OF ZAMBIA

ACT

No. 2 of 2021

Date of Assent: 23rd March, 2021

An Act to provide for cyber security in the Republic; provide for the constitution of the Zambia Computer Incidence Response Team and provide for its functions; provide for the constitution of the National Cyber Security Advisory and Coordinating Council and provide for its functions; provide for the continuation of the Central Monitoring and Co-ordination Centre; provide for the protection of persons against cyber crime; provide for child online protection; facilitate identification, declaration and protection of critical information infrastructure; provide for the collection of and preservation of evidence of computer and network related crime; provide for the admission; in criminal matters, of electronic evidence; provide for registration of cyber security service providers; and provide for matters connected with, or incidental to, the foregoing.

[24th March, 2021

ENACTED by the Parliament of Zambia.

Enactment

PART I

PRELIMINARY PROVISIONS

1. This Act may be cited as the Cyber Security and Cyber Crimes Act, 2021, and shall come into operation on the date appointed by the Minister by statutory instrument.

Short title
and
commence-
ment

2. In this Act, unless the context otherwise requires—

Interpretation

“access” has the meaning assigned to the word in the Electronic Communications and Transactions Act, 2021;

Act No. 4 of
2021

“advanced electronic signature” has the meaning assigned to the words in the Electronic Communications and Transactions Act, 2021;

Act No. 4 of
2021

“article” means any data computer program, computer data storage medium or computer system which—