

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

MEMORANDUM

The objects of this Bill are to—

- (a) ensure the provision of cyber security in the Republic;
- (b) provide for the protection of persons against cyber crime;
- (c) provide for child online protection;
- (d) facilitate identification, declaration and protection of critical information infrastructure;
- (e) provide for the collection of and preservation of evidence of computer and network related crime;
- (f) revise the admission, in criminal matters, of electronic evidence;
- (g) provide for registration of cyber security services providers; and
- (h) provide for matters connected with, or incidental to, the foregoing.

A. MWANSA,
Solicitor-General

**THE CYBER SECURITY AND CYBER CRIMES
BILL, 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 Coordinating Council

PART III

INSPECTORATE

8. Appointment of cyber inspectors
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

PART VI

INTERCEPTION OF COMMUNICATIONS

26. Prohibition of interception of communication
27. Central Monitoring and Coordination Centre
28. Lawful interception
29. Interception of communication to prevent bodily harm, loss of life or damage to property
30. Interception of communications for purposes of determining location
31. Prohibition of disclosure of intercepted communications
32. Disclosure of intercepted communications by Law Enforcement Officer
33. Privileged communications 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 of device
38. Assistance by Service Providers
39. Duties of Service Providers in Relation to Customers
40. Interception Capability of Service Providers

PART VII

LICENSING OF CYBER SECURITY SERVICE PROVIDERS

41. Prohibition from Conducting Cyber Security Services without a license
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. Identityrelated crimes
54. Publication of false 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 a computer
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