# Cyber Security Act, 2023

(Act No. 39 of 2023)

[ September 18, 2023 ]

**The Digital Security Act, 2018 is repealed to ensure cyber security and make new provisions for the detection, prevention, suppression and prosecution of crimes committed through digital or electronic means and related matters.**

Whereas it is expedient and necessary to repeal the Digital Security Act, 2018 (Act No. 46 of 2018) to ensure cyber security and make new provisions for the detection, prevention, suppression and prosecution of crimes committed through digital or electronic means and related matters;

Therefore, it is hereby enacted as follows:-

## CHAPTER ONE

### early

**Short title and introduction**

1. (1) This Act shall be known as the Cyber Security Act, 2023 .

(2) It shall take effect immediately.

**definition**

2. (1) Unless there is anything contrary to the subject or context in this Act,

(a) “Appellate Tribunal” means the Cyber Appellate Tribunal constituted under section 82 of the Information and Communication Technology Act, 2006 (Act No. 39 of 2006);

(b) “database” means information, knowledge, facts, concepts or instructions presented in text, image, audio or video form, which—

(b) is or has been formally prepared by any computer or computer system or computer network; And

(a) prepared for use on any computer or computer system or computer network;

(c) “Agency” means the National Cyber Security Agency constituted under section 5;

(d) “Computer Emergency Response Team” or “Computer Incident Response Team” means the Computer Emergency Response Team or Computer Incident Response Team referred to in sub-section (2) of section 9;

(e) “computer system” means an interconnected system of one or more computers or digital devices capable of receiving, transmitting or storing data, individually or in conjunction with each other;

(f) “Council” means the National Cyber Security Council constituted under section 12;

(g) “Critical Information Infrastructure” means any such external or virtual information infrastructure as declared by the Government which controls, processes, transmits or stores any data or any digital or electronic information and which, if damaged or endangered—

(n) public safety or economic security or public health; And

(a) national security or state integrity or sovereignty,

It can have harmful effects;

(h) “National Computer Emergency Response Team” means the National Computer Emergency Response Team referred to in sub-section (1) of section 9;

(j) “Tribunal” means the Cyber Tribunal constituted under section 68 of the Information and Communication Technology Act, 2006 (Act No. 39 of 2006);

(j) “digital” means an even-number (0 and 1/binary) or digit-based operating system, and for the purposes of this Act, shall include electrical, digital magnetic, optical, biometric, electrochemical, electromechanical, wireless or electro-magnetic technology;

(k) “digital device” means any electronic, digital, magnetic, optical or data processing device or system, which performs logical, arithmetical and memory operations using electronic, digital, magnetic or optical impulses,

and any digital or computer device system; or connected to a computer network, and includes all input, output, processing, storage, digital device software or communication facilities;

(l) “Digital Forensic Lab” means the Digital Forensic Lab described in section 10;

(d) “police officer” means any such police officer not below the rank of Inspector;

(d) “program” means instructions expressed in sound, signal, record or in any other form in a machine-readable medium, by means of which any particular function may be effected or effected by a digital device;

(n) “Criminal Procedure Code” means the Code of Criminal Procedure, 1898 (Act No. V of 1898);

(v) "person" means any person or institution, company, partnership, firm or other body, in relation to a digital device, its controller and includes any entity or artificial legal entity created by law;

(h) “unlawful access” means access to any computer or digital device or digital network or digital information system without the permission of any person or authority or in violation of the conditions of such permission, or by such access interfere with the exchange of any information on the said information system; to suspend or interrupt or stop the provision or processing thereof, or to modify or augment or add or delete such data or collect any data through any digital device;

(d) “Director-General” means the Director-General of the Finance Agency;

(d) “defamation” means defamation as defined in section 499 of the Penal Code (Act No. XLV of 1860);

(n) “Malware” means any digital or electronic instructions, data, programs or apps which—

(n) alter, distort, destroy, damage or impair the performance of or adversely affect the performance of any computer or digital device;

(a) connects itself with any other computer or digital device to execute any program, data or instruction of the said computer or digital or electronic device or becomes active during the execution of any operation and thereby to the said computer or digital or electronic device causes any harmful change or event; or

(e) steals or creates automated access to information on any digital or electronic device;

(c) “spirit of liberation war” means those ideals of nationalism, socialism, democracy and secularism which motivated our brave people to dedicate themselves and sacrifice their lives as brave martyrs in the national liberation struggle;

(f) “cyber security” means the security of any digital device, computer or computer system;

(b) “service provider” means—

(n) any person who enables any user to communicate through a computer or digital process; or

(a) any such person, entity or organization that processes or stores computer data for or on behalf of the Service or users of the Service;

(2) All words or expressions used in this Act which have not been defined shall have the meaning assigned to them in the Information and Communication Technology Act, 2006 .

**Enforcement of laws**

3. (1) If any provision of any other Act is inconsistent with any provision of this Act, then the provisions of this Act shall prevail in so far as the provision of this Act is inconsistent with the provision of any other Act.

(2) Notwithstanding anything contained in sub-section (1), the provisions of the Right to Information Act, 2009 (Act No. 20 of 2009) shall apply in respect of matters relating to Right to Information.

**Transnational application of law**

4. (1) If a person commits an offense under this Act outside Bangladesh which if committed in Bangladesh would have been punishable under this Act, the provisions of this Act shall apply as if the offense had been

committed by him in Bangladesh.

(2) If any person commits any offense under this Act within Bangladesh with the help of any computer, computer system, computer network or digital device located in Bangladesh from outside Bangladesh, the provisions of this Act shall apply against such person as if the entire process of said offense occurred in Bangladesh. has taken place

(3) If any person commits an offense under this Act outside Bangladesh from within Bangladesh, the provisions of this Act shall apply as if the entire process of said offense had been committed in Bangladesh.

## CHAPTER II

### National Cyber Security Agency

**Formation of agencies, offices, etc**

5. (1) For the purposes of this Act, the Government shall, by notification in the Official Gazette, constitute an agency to be called the National Cyber Security Agency consisting of 1 (one) Director General and such number of Directors as may be prescribed by rule.

(2) The head office of the Agency shall be at Dhaka, but the Government may, if necessary, establish its branch office at any place in the country outside Dhaka.

(3) The Agency shall be administratively attached to the Department of Information and Communication Technology.

(4) The powers, duties and functions of the Agency shall be determined by rules.

**Appointment of Director General and Directors, etc**

6. (1) The Director General and Directors shall be appointed by the Government from among persons having expertise in computer or cyber security and their terms of service shall be prescribed by the Government.

(2) The Director-General and Directors shall be whole-time employees of the Agency, and shall, subject to the provisions of this Act and the rules made thereunder, perform such functions, exercise powers and perform such duties as may be directed by the Government.

(3) If the post of Director General becomes vacant, or if the Director General is unable to perform his duties due to absence, illness or any other reason, the senior Director shall temporarily perform the duties of the Director General until the newly appointed Director General takes over the vacancy or until the Director General is able to perform his duties again.

**Agency manpower**

7. (1) The Agency shall have the necessary manpower as per the organizational structure approved by the Government.

(2) The terms and conditions of employment of the agency's workforce shall be determined by rules.

## CHAPTER III

### Preventive measures

**Ability to remove or block certain data**

8. (1) The Director General shall request the Bangladesh Telecommunication Regulatory Commission, hereinafter referred to as BTRC, to remove or, as the case may be, block any information-data published or disseminated through digital or electronic media on any matter within his jurisdiction, which poses a threat to cyber security. can

(2) If, subject to data analysis by law enforcement agencies, there is reason to believe that any data published or disseminated by digital or electronic means may affect the integrity, economic activity, security, defense, religious values or interests of the country or any part thereof; Law enforcement agencies may request BTRC, through the Director General, to remove or block such data if it disturbs public order, or promotes racial hatred and hatred.

(3) On receipt of any request under sub-sections (1) and (2), the BTRC shall, by intimation to the Government concerned, forthwith remove or, as the case may be, block the said data.

(4) For the purposes of this section, such other matters as may be necessary shall be prescribed by rule.

**Computer Emergency**

**Response Team**

9. (1) For the purposes of this Act, there shall be a National Computer Emergency Response Team under the Agency.

(2) Any critical information infrastructure declared under section 15 may, if necessary, with the prior approval of the Agency, constitute its own Computer Emergency Response Team or Computer Incident Response Team.

(3) The National Computer Emergency Response Team and the Computer Emergency Response Team or the Computer Incident Response Team shall consist of cyber security experts and, where necessary, members of law enforcement agencies.

(4) The National Computer Emergency Response Team and the Computer Emergency Response Team or the Computer Incident Response Team shall, in the manner prescribed by the rules, function round the clock.

(5) Without prejudice to the generality of sub-section (4), the National Computer Emergency Response Team and the Computer Emergency Response Team or the Computer Incident Response Team shall perform the following duties, namely:-

(a) ensuring emergency security of critical information infrastructure;

(b) promptly take necessary measures to remedy cyber or digital attacks and cyber or digital security breaches;

(c) taking necessary measures to prevent possible and imminent cyber or digital attacks;

(d) To carry out the purposes of this Act, with the approval of the Government, undertake general cooperative activities including exchange of information with any similar foreign team or organization; And

(e) performing other functions prescribed by rules.

(6) The Agency shall coordinate and supervise the National Computer Emergency Response Team, Computer Emergency Response Team or Computer Incident Response Team.

**Digital Forensic**

**Lab**

10. (1) For the purposes of this Act, there shall be, under the control and supervision of the Agency, one or more Digital Forensic Labs.

(2) Notwithstanding anything contained in sub-section (1), any digital forensic lab established under any Government authority or organization before the commencement of this Act shall, subject to the achievement of the standards prescribed under section 11, be recognized by the Agency and in that case The said lab shall be deemed to have been established under this Act.

(3) The Agency shall coordinate among digital forensic labs.

(4) Establishment, use, management and other matters of Digital Forensic Lab shall be determined by the rules.

**Quality Control of Digital Forensic Labs**

11. (1) The Agency shall, in accordance with the criteria prescribed by rule, ensure the quality of each digital forensic laboratory.

(2) In ensuring the quality standards prescribed under sub-section (1), every digital forensic laboratory shall, inter alia—

(a) conduct its operations by suitably qualified and trained manpower;

(b) ensure its physical infrastructural facilities;

(c) take necessary steps to maintain the security and confidentiality of information stored thereunder;

(d) use quality equipment to maintain technical standards for digital forensic testing; And

(e) carry out the work in the manner prescribed by the rules, following the scientific process.

## CHAPTER IV

### National Cyber Security Council

**National Cyber Security Council**

12. (1) For the purposes of this Act, there shall be constituted a National Cyber Security Council consisting of the following members, namely:-

(a) the Prime Minister, Government of the People's Republic of Bangladesh, who shall also be its Chairman;

(b) Ministers, Ministers of State and Deputy Ministers of the Ministry of Posts, Telecommunications and Information Technology;

(c) the Minister, Ministry of Law, Justice and Parliamentary Affairs;

(d) Advisor to the Prime Minister on ICT;

(e) the Principal Secretary to the Prime Minister;

(f) the Governor, Bangladesh Bank;

(g) Secretary, Department of Posts and Telecommunications;

(h) Secretary, Department of Information and Communication Technology;

(j) Secretary, Department of Public Safety;

(j) Foreign Secretary, Ministry of Foreign Affairs;

(k) Inspector General of Police, Bangladesh Police;

(l) Chairman, Bangladesh Telecommunication Regulatory Commission;

(d) the Director General, Directorate General of Defense Intelligence;

(d) the Director General, National Security Intelligence Agency;

(n) the Director General, National Telecommunication Monitoring Centre; And

(r) Director General, National Cyber Security Agency.

(2) The Director General shall provide secretarial assistance in the conduct of the Council.

(3) For the purpose of sub-section (1), the Council may, on the advice of the Chairman, at any time, by notification in the Official Gazette, co-opt any expert as its member for such period and conditions as may be prescribed.

**Powers of Council, etc**

13. (1) The Council shall, for the purpose of carrying out the provisions of this Act and the rules made thereunder, give necessary directions and advice to the Agency.

(2) The Council shall, inter alia, perform the following functions, namely:-

(a) providing necessary guidance for remediation of cyber security threats;

(b) advising on cyber security infrastructure development and manpower augmentation and upgrading;

(c) formulation of inter-institutional policies aimed at ensuring cyber security;

(d) taking necessary measures to ensure proper enforcement of laws and rules made thereunder; And

(e) perform any other function prescribed by law.

**Council meetings, etc**

14. (1) Subject to the other provisions of this section, the Council may prescribe the procedure of its meetings.

(2) The meeting of the Council shall be held on such date, time and place as may be fixed by its Chairman.

(3) The Chairman may call a meeting of the Council at any time.

(4) The Chairman shall preside at all meetings of the Council.

(5) No action or proceeding of the Council shall be invalid merely because of a vacancy in the office of any member of the said Council or a defect in the constitution of the Council and no question shall be raised in connection therewith.

## CHAPTER FIVE

### Critical Information Infrastructure

**Critical Information Infrastructure**

15. For the purposes of this Act, the Government may, by notification in the Government Gazette, declare any computer system, network or information infrastructure to be a critical information infrastructure.

**Security monitoring and inspection of critical information infrastructure**

16. (1) The Director General shall, from time to time, inspect and inspect any important information infrastructure and submit a report thereon to the Government to ascertain whether the provisions of this Act are being duly complied with.

(2) The critical information infrastructures declared under this Act shall, in the manner prescribed by the rules, submit an inspection report to the Government after inspecting its internal and external infrastructure every

year and inform the Director General of the contents of the said report.

(3) If the Director General has reason to believe that the activities of any person in any matter under his jurisdiction are threatening or harmful to the critical information infrastructure, he may, on his own initiative or on receiving any complaint from anyone, investigate the same.

(4) For the purposes of this section, security monitoring and inspection activities shall be carried out by a person who is an expert in cyber security.

## CHAPTER SIX

### Crime and Punishment

**Penalty for illegal access to critical information infrastructure, etc**

17. (1) If any person willfully or knowingly in any critical information infrastructure—

(a) enters unlawfully; or

(b) damages or destroys or disables it by unlawful entry or attempts to do so,

If such act of such person shall be an offence.

(2) If any person in sub-section (1)—

(a) commits any offense under clause (a), he shall be punished with imprisonment for a term not exceeding 3 (three) years, or with a fine not exceeding 25 (twenty five) lakhs, or with both; And

(b) commits any offense under clause (b), then he shall be punished with imprisonment not exceeding 6 (six) years, or with fine not exceeding 1 (one) crore, or with both.

**Unlawful access to computers, digital devices, computer systems, etc. and penalties**

18. (1) If any person willfully—

(a) unlawfully accesses or facilitates access to any computer, digital device, computer system or computer network; or

(b) unlawfully accesses, or assists in the entry of, any computer, digital device, computer system or computer network for the purpose of committing an offence, such act by such person shall be an offence.

(2) If any person in sub-section (1)—

(a) commits an offense under clause (a), shall be punished with imprisonment not exceeding 6 (six) months, or with fine not exceeding two (two) lakhs of rupees, or with both;

(b) commits any offense under clause (b), then he shall be punished with imprisonment not exceeding 3 (three) years, or with fine not exceeding 10 (ten) lakhs, or with both.

(3) If the offense committed under sub-section (1) is committed in relation to any computer, digital device, computer system or computer network protected by critical information infrastructure, he shall be liable to imprisonment for a term not exceeding 3 (three) years, or to imprisonment for a term not exceeding 10 ( 10) Shall be punished with a fine of one lakh rupees, or with both penalties.

**Damages and penalties for computers, computer systems, etc**

19. 19. (1) If a person-

(a) collects any data, database, information or excerpt thereof from any computer, computer system or computer network, or collects information from such computer, computer system or computer network, including transferable stored data, or collects copies or parts of any data; do;

(b) intentionally introduces or attempts to introduce any infectious, malware or harmful software into any computer, computer system or computer network;

(c) intentionally damages, or attempts to damage, any computer, computer system, computer network, data or computer database or damages or attempts to damage any other program stored on such computer, computer system or computer network;

(d) obstructs or attempts to obstruct any authorized or authorized person's access to any computer, computer system or computer network;

(e) knowingly generates or attempts to generate or market spam or send unsolicited electronic mail for the purpose of marketing any product or service, without the consent of the sender or subscriber; or

(f) wrongfully interferes with or tampers with any computer, computer system or computer network, accepts the services of any person or collects or attempts to collect charges as another,

If such act of such person shall be an offence.

(2) If any person commits an offense under sub-section (1), he shall be punished with imprisonment for a term not exceeding seven (7) years, or with a fine not exceeding ten (10) lakhs, or with both.

**Offenses and penalties related to modification of computer source code**

20. (1) If any person willfully or knowingly conceals, destroys or alters the computer source code used in any computer program, computer system or computer network, or attempts through any other person to conceal, destroy or alter such code, program, system or network. , and if the said source code is recoverable or maintainable, it shall be an offense for such person to do so.

(2) If any person commits an offense under sub-section (1), he shall be punished with imprisonment for a term not exceeding 3 (three) years, or with fine not exceeding 3 (three) lakhs, or with both.

**Punishment for hatred, misinformation and defamatory propaganda about the Liberation War, the spirit of the Liberation War, Father of the Nation Bangabandhu Sheikh Mujibur Rahman, the National Anthem or the National Flag.**

21. (1) If any person conducts or supports any propaganda of hatred, misinformation and defamation about the liberation war of Bangladesh, the spirit of the liberation war, the Father of the Nation Bangabandhu Sheikh Mujibur Rahman, the national anthem or the national flag through digital or electronic means, then such act of such person shall be a crime

(2) If any person commits an offense under sub-section (1), he shall be punished with imprisonment for a term not exceeding 5 (five) years, or with a fine not exceeding 1 (one) crore rupees, or with both.

**Digital or electronic fraud**

22. (1) If any person commits fraud by using digital or electronic means, such act by such person shall be an offence.

(2) If any person commits an offense under sub-section (1), he shall be punished with imprisonment for a term not exceeding 2 (two) years, or with fine not exceeding 5 (five) lakh rupees, or with both.

Explanation.-For the purpose of this section, “digital or electronic forgery” means any person without right or in excess of a given right or through the exercise of unauthorized access to the input or output of any computer or digital device to prepare, alter, delete or conceal any corrupt data or program; Information or error processing, information system, computer or digital network management.

**Digital or electronic fraud**

23. (1) If any person commits fraud by using digital or electronic means, such act by such person shall be an offence.

(2) If any person commits an offense under sub-section (1), he shall be punished with imprisonment for a term not exceeding 5 (five) years, or with fine not exceeding 5 (five) lakhs, or with both.

Explanation.-For the purposes of this section, “digital or electronic fraud” means the alteration by any person of any information in any computer program, computer system, computer network, digital device, digital system, digital network or social media, intentionally or knowingly or without permission; Delete, add new information or reduce its value or usefulness by distorting it, attempting to obtain any advantage or damage to himself or any other person or resort to deception.

**Identity fraud or impersonation**

24 (1) If any person intentionally or knowingly uses any computer, computer program, computer system, computer network, any digital device, digital system or digital network-

(a) impersonates another person or misrepresents any other person's personal information with intent to defraud or deceive; or

(b) willfully and fraudulently assumes the identity of any living or dead person for the following purposes,-

(b) benefiting or causing to be benefited by himself or any other person;

(a) acquiring any property or interest in property;

(e) harming any person or entities;

If such act of such person shall be an offence.

(2) If any person commits an offense under sub-section (1), he shall be punished with imprisonment for a term not exceeding 5 (five) years, or with fine not exceeding 5 (five) lakhs, or with both.

**Offensive, false or threatening, transmission of information, publication, etc**

25. (1) If any person on the website or any other digital or electronic medium—

(a) knowingly or knowingly transmits, transmits, publishes or disseminates any information that is offensive or intimidating or is intended to annoy, insult, defame or degrade any person, whether or not known to be false; or

(b) publishes, or disseminates or assists in the dissemination of, any information in a wholly or partially distorted form, whether defaming the image or reputation of the State, or spreading misinformation, or otherwise, whether known to be slanderous or false,

If such act of such person shall be an offence.

(2) If any person commits an offense under sub-section (1), he shall be punished with imprisonment for a term not exceeding 2 (two) years, or with fine not exceeding 3 (three) lakhs, or with both.

**Penalties for collection, use, etc. of contact information without permission**

26. (1) It shall be an offense for any person to collect, sell, possess, supply or use the identity information of another person without lawful authority.

(2) If any person commits an offense under sub-section (1), he shall be punished with imprisonment for a term not exceeding 2 (two) years, or with a fine not exceeding 5 (five) lakhs, or with both.

Explanation.-For the purposes of this section, “identifying information” means any external, biological or physical information or any other information which, singly or collectively, identifies a person or system, whose name, photograph, address, date of birth, mother's name, father's name, Signature, National Identity Card, Birth and Death Registration Number, Finger Print, Passport Number, Bank Account Number, Driving License, E-TIN Number, Electronic or Digital Signature, Username, Credit or Debit Card Number, Voyage Print, Retina Image, Iris Image, DNA profile, security question or any other identification that is readily available for technology optimization.

**Crime and Punishment of Cyber Terrorism**

27. 27. (1) If a person-

(a) interferes with lawful access to or unlawfully accesses any computer or computer network or Internet network with intent to endanger national integrity, security and sovereignty and to instill fear among the public or any section thereof;

(b) causes contamination of any digital device or introduces malware which causes or is likely to cause death or serious injury to any person; or

(c) impairs or destroys the provision of essential goods and services to the public or adversely affects any critical information infrastructure; or (d) intentionally or knowingly accesses or accesses any computer, computer network, Internet network, stored data or computer database or accesses any such stored data or computer database in a manner prejudicial to friendly relations with a foreign state or to public order; may be used for any purpose or may be used for the benefit of any foreign state or any person or group,

In that case, the similar act of the person will be a cyber terrorism crime.

(2) If any person commits an offense under sub-section (1), he shall be punished with imprisonment for a term not exceeding 14 (fourteen) years, or with a fine not exceeding one (one) crore, or with both.

**Publication, transmission, etc. of any**

**such information offensive to religious values or sentiments on the website or in any electronic format**

28. (1) If any person or group deliberately or knowingly publishes or disseminates on the website or in any other electronic format anything that offends religious sentiments or religious values with the intention of inciting or offending religious sentiments or religious values, that person shall A similar act shall be an offence.

(2) If any person commits an offense under sub-section (1), he shall be punished with imprisonment for a term not exceeding two (2) years, or with fine not exceeding five (five) lakhs of rupees, or with both.

**Publication, dissemination, etc. of defamatory information**

29. If any person publishes or disseminates defamatory information as described in section 499 of the Penal Code (Act No. XLV of 1860) on a website or in any other electronic format, such act of such person shall be an offense and he shall be liable to a fine not exceeding 25 (twenty five) lakhs of rupees. Shall be fined.

**Offenses and punishments for unauthorized e-transactions**

30. 30. (1) If a person-

(a) conducts e-transactions without lawful authority using any digital or electronic medium from any bank, insurance or other financial institution or mobile financial service provider; or

(b) carry out e-transactions despite the declaration of invalidity of any e-transactions issued by the Government or Bangladesh Bank, from time to time,

If such act of such person shall be an offence.

(2) If any person commits an offense under sub-section (1), he shall be punished with a fine not exceeding 25 (twenty five) lakhs of rupees.

Explanation.-For the purposes of this section, “e-transaction” means any instruction, order or authority given by a person to transfer his funds to a bank, financial institution or a specified account number by digital or electronic means, or to withdraw or withdraw funds. Financial transactions and money transfer through any digital or electronic medium.

**Offenses and**

**punishments for disturbing law and order, etc**

31. (1) If any person intentionally publishes or broadcasts on the website or in digital format anything which creates enmity, hatred or hatred between the various classes or communities concerned or destroys communal harmony or creates unrest or disorder or deterioration of law and order; If the person commits or is about to commit a similar act, it shall be an offence.

(2) If any person commits an offense under sub-section (1), he shall be punished with imprisonment for a term not exceeding 5 (five) years, or with a fine not exceeding 25 (twenty five) lakhs, or with both.

**Crimes and penalties related to hacking**

32. If any person commits hacking, it shall be an offense and shall be punishable with imprisonment not exceeding 14 (fourteen) years, or with fine not exceeding 1 (one) crore, or with both.

Explanation.-For the purposes of this section, “hacking” means—

(a) steal, destroy, destroy, alter or reduce the value or usefulness of or otherwise damage any information in a computer database; or

(b) causing damage to any computer, server, computer network or other electronic system not owned or occupied by the user.

**Aiding and abetting crime and its punishment**

33. (1) If any person assists in the commission of any offense under this Act, such act by such person shall be an offence.

(2) If any person commits an offense under sub-section (1), he shall be punished with the same punishment as is prescribed for the original offence.

**Crime and Punishment of False Cases, Filing of Complaints, etc**

34. (1) If any person files or makes a suit or complaint against that person without any just or lawful cause for filing a suit or complaint under any other section of this Act with intent to injure another person, it shall be an offense and punishable by law or The person filing the complaint and the person who filed the complaint shall be punished with the penalty prescribed for the original offence.

(2) If any person files any suit or complaint under sub-section (1) under more than one section of this Act, the amount of penalty for the main offense for which the amount of penalty is higher among the offenses mentioned in the said section shall be determined as the amount of penalty.

(3) The Tribunal may, on the written complaint of any person, entertain and try cases of offenses committed under sub-section (1).

**Offenses committed by the company**

35. (1) In case of the commission of any offense under this Act by any company, every such owner, chief executive, director, manager, secretary, partner or any other officer or employee or representative of the company having direct connection with the said offense shall be deemed to have committed the said offence. , unless he is able to prove that the said offense was committed without his knowledge or that he tried his best to prevent the said offence.

(2) If the company mentioned in sub-section (1) is an organization with legal personality, apart from the person being charged and convicted, the said company may be separately charged and convicted in the same proceedings, but only fine shall be imposed on it as per the relevant provisions.

Explanation.-For the purposes of this section,-

(a) “company” shall include any commercial establishment, partnership, association, association or organization;

(b) in the case of a commercial enterprise, "director" shall include any partner or member of the board of directors thereof.

**Power to order compensation**

36. If a person causes financial loss to another person by digital or electronic fraud under section 22, digital or electronic fraud under section 23 or by impersonation or impersonation under section 24, the Tribunal may, as compensation, award an amount equal to the loss caused or such amount as it thinks fit. may order the aggrieved person to pay.

**Service provider not**

**liable**

37. A service provider shall not be liable under this Act or any rule made thereunder for having arranged to obtain information, if he is able to prove that the offense or violation concerned was committed without his knowledge or that he has made every effort to prevent the said offense from being committed.

## CHAPTER VII

### Investigation and prosecution of crimes

**investigations, and so on**

38. (1) The Police Officer, hereinafter referred to in this Chapter as the Investigating Officer, shall investigate any offense committed under this Act.

(2) Notwithstanding anything contained in sub-section (1), if it appears at the commencement of any case or at any stage of investigation that it is necessary to constitute an inquiry team for the proper investigation of the case, the Tribunal or the Government may, by order, Under the control and conditions of the authority or agency specified in the order, the investigating agency may form a joint investigation team consisting of law enforcement agencies and agencies.

**Time limit for investigation, etc**

39. (1) Investigating Officer-

(a) shall complete the investigation within 90 (ninety) days from the date of receipt of responsibility for the investigation of any crime;

(b) if he fails to complete the investigation within the time prescribed under clause (a), he may, subject to the approval of his controlling officer, extend the period of investigation by an additional fifteen (15) days;

(c) If he fails to complete any investigation work within the time prescribed under clause (b), he shall inform the Tribunal in the form of a report recording the reason thereof, and with the permission of the Tribunal, complete the investigation work within the next 30 (thirty) days.

(2) If the investigating officer under sub-section (1) fails to complete any inquiry function, the Tribunal may extend the period of inquiry, by a reasonable time.

**Powers of Investigating Officer**

40. (1) In connection with the investigation of any offense under this Act, the Investigating Officer shall have the following powers, namely:-

(a) taking possession of a computer, computer program, computer system, computer network or any digital device, digital system, digital network or any program, data stored on a computer or compact disk or removable drive or by any other means; ;

(b) taking necessary steps to collect traffic data from any person or organization; And

(c) performing such other functions as may be necessary for carrying out the purposes of this Act.

(2) While conducting an investigation under this Act, the investigating officer may take the assistance of any expert person or specialized institution for the purpose of investigation of any offence.

**Search and seizure by warrant**

41. If any police officer has reason to believe that—

(a) any offense under this Act has been committed or is likely to be committed; or

(b) any computer, computer system, computer network, data or evidence relating thereto is kept at any place or with any person in connection with an offense committed under this Act,

If so, he may, by recording reasons for such belief, obtain a search warrant by applying to the Tribunal or, as the case may be, the Chief Judicial Magistrate or the Chief Metropolitan Magistrate and perform the following functions,

(b) interception of any traffic data in the possession of any service provider;

(a) Interference with any wire or electronic communication, including customer information and traffic data, at any stage of communication.

**Search, seizure and arrest**

**without warrant**

42. (1) If any police officer has reason to believe that an offense under this Act has been or is being committed or is likely to be committed at any place or that evidence has been lost, destroyed, erased, altered or otherwise made scarce. Provided, that he may, recording reasons for such belief, perform the following acts,

(a) enter and search the said place and, if the entry is obstructed, take necessary action in accordance with the Code of Criminal Procedure;

(b) confiscation of any computer, computer system, computer network, data or other equipment used in the commission of the crime found during the search of the said place and any document helpful in proving the crime;

(c) searching the body of any person present at the said place;

(d) If it is suspected that any person present at the said place has committed or is committing any offense under this Act, arrest that person.

(2) After conducting the search under sub-section (1), the police officer shall submit to the Tribunal a report of the conduct of the search.

**Data storage**

43. (1) The Director General, in his discretion, or on the application of the Investigating Officer, if he believes that any information stored in a computer or computer system is required to be preserved for the purposes of an investigation under this Act and destroys, destroys, alters or makes such information unavailable If there is a possibility, then the person or organization in charge of the computer or computer system can be instructed to store such information for up to 90 (ninety) days.

(2) The Tribunal may, on application, extend the retention period of the said data, provided that it shall not exceed a total of 180 (one hundred and eighty) days.

**Do not disrupt the normal use of the computer**

44. (1) The investigating officer shall conduct the investigation in such a manner as not to interfere with the lawful use of the computer, computer system, computer network or any part thereof.

(2) Any computer, computer system, computer network or any part thereof shall be seized, if—

(a) access to the relevant computer, computer system, computer network or any part thereof is not possible;

(b) If the relevant computer, computer system, computer network or any part thereof is not seized for the prevention of crime or ongoing crime, the data is likely to be lost, destroyed, altered or made scarce.

**Assist in investigation**

45. While conducting an investigation under this Act, the investigating officer may request any person or entity or service provider to provide information or assist in the investigation and if any such request is made, the concerned person, entity or service provider shall be obliged to provide necessary assistance including providing information.

**Confidentiality of information obtained in investigation**

46. (1) Any person, entity or service provider providing or disclosing any information for the purpose of investigation shall not be prosecuted under civil or criminal law against such person, entity or service provider.

(2) All persons, entities or service providers concerned with the investigation under this Act shall maintain the confidentiality of information related to the investigation.

(3) If any person contravenes the provisions of sub-sections (1) and (2), such contravention shall be an offense and shall be liable to imprisonment for a term not exceeding 2 (two) years or to a fine not exceeding 1 (one) lakh rupees, or shall be punished with both penalties.

**Criminal prosecution, etc**

47. (1) Notwithstanding anything contained in the Code of Criminal Procedure, the Tribunal shall not take cognizance of any offense without the written report of a police officer.

(2) The Tribunal shall, subject to consistency with the provisions of this Act, follow the procedure laid down in Chapter 23 of the Code of Criminal Procedure for trial in a Court of Session in the trial of an offense under this Act.

**Criminal trials and appeals**

48. (1) Notwithstanding anything contained in any other law for the time being in force, offenses committed under this Act shall be triable only by the Tribunal.

(2) If any person is aggrieved by the judgment passed by the Tribunal, he may file an appeal in the Appellate Tribunal.

**Application of Criminal Procedure Code**

49. (1) Unless otherwise provided in this Act, the provisions of the Code of Criminal Procedure shall apply to the investigation, trial, appeal and other matters of any offence.

(2) The Tribunal, the Appellate Tribunal and, as the case may be, the Police Officer in the performance of the duties assigned to them, in accordance with the provisions of this Act, in respect of the following matters, Part-II and Part-II of Chapter VIII of the Information and Communication Technology Act, 2006 (Act No. 39 of 2006); - 3 shall follow the provisions, namely:-

(a) the procedure of the Tribunal and Appellate Tribunal;

(b) time limit for delivery of judgment;

(c) not bar the imposition of any other penalty in respect of fine or confiscation;

(d) power of detention or arrest in public places, etc.;

(e) method of search; And

(f) Jurisdiction of Appellate Tribunal and procedure for hearing and disposing of appeals.

(3) The Tribunal shall exercise all the powers of a Court of Session exercising original jurisdiction under the Code of Criminal Procedure.

**Taking expert opinion, training, etc**

50 (1) The Tribunal or the Appellate Tribunal, while conducting the proceedings, may take the opinion of any person experienced in computer science, digital forensics, electronic communication, data protection etc.

(2) The government or agency may provide specialized training in computer science, digital forensics, electronic communication, data security and other necessary subjects to all persons concerned with the implementation of this Act.

**Time limit for disposal of case**

51. (1) The Judge of the Tribunal shall dispose of the case within 180 (one hundred and eighty) working days from the date of framing of complaint in any case under this Act.

(2) If the Judge of the Tribunal fails to dispose of any case within the time prescribed under sub-section (1), he may extend the said period by a maximum of 90 (ninety) working days after recording the reason thereof.

(3) If the Judge of the Tribunal fails to dispose of any case within the time prescribed under sub-section (2), he may continue the proceedings of the case after notifying the matter in the form of a report to the High Court Division recording the reasons thereof.

**Commissibility and bailability of offences**

52. of this Act—

(a) the offenses mentioned in sections 17, 19, 27 and 32 shall be cognizable and non-bailable;

(b) The offenses mentioned in clause (b) of sub-section (1) of section 18, sections 20, 21, 22, 23, 24, 25, 26, 28, 29, 30, 31 and 46 are non-commissionable and bailable. shall; And

(c) The offenses mentioned in clause (a) of sub-section (1) of section 18 shall be non-committable, bailable and subject to the consent of the court.

**confiscation**

53. (1) If any offense under this Act is committed, the computer, computer system, floppy disk, compact disk, tape-drive or any other accessory computer material or object in relation to or in connection with which the said offense is committed shall be forfeitable as per the order of the Tribunal.

(2) Notwithstanding anything contained in sub-section (1), if the Tribunal is satisfied that the person in whose possession or control the said computer, computer system, floppy disk, compact disk or any other

computer accessory is found to be If the computer, computer system, floppy disk, compact disk, tape drive or any other related computer equipment is not liable for the commission of the crime related to the equipment, it shall not be confiscated.

(3) With any computer, computer system, floppy disk, compact disk, tape drive or any other ancillary computer equipment liable to confiscation under sub-section (1), if any lawful computer, computer system, floppy disk, compact disk, tape drive or If any other computer equipment is found, they are also subject to seizure.

(4) Notwithstanding anything contained in the other provisions of this section, if any computer or any equipment or apparatus connected therewith is used in the commission of any offense by any Government or statutory body, the same shall not be forfeitable.

## CHAPTER VIII

### Regional and international cooperation

**Regional and international cooperation**

54. The provisions of the Mutual Assistance in Criminal Matters Act, 2012 (Act No. 4 of 2012) shall apply if regional and international cooperation is required in the investigation and prosecution of any offense committed under this Act .

## CHAPTER NINE

### Misc

**delegation of power**

55. The Director General may, if necessary, delegate any power or duty conferred on him under this Act, by order in writing, to any employee of the Agency and any other person or police officer.

**Evidential value**

56. Notwithstanding anything to the contrary contained in the Evidence Act, 1872 (Act No. I of 1872) or any other law, any forensic evidence obtained or collected under this Act shall be admissible in evidence at trial.

**Troubleshooting**

57. If any ambiguity is observed in the implementation of the provisions of this Act, the Government may, by order published in the Official Gazette, take necessary measures to remove the said difficulty.

**Power to make rules**

58. (1) For the purposes of this Act, the Government may, by notification in the Official Gazette, make rules.

(2) Without prejudice to the generality of sub-section (1), the Government may, by notification in the Official Gazette, make rules, inter alia, in respect of all or any of the following matters, namely:-

(a) Establishment of Digital Forensic Lab;

(b) Supervision of Digital Forensic Lab by the Director General;

(c) review of traffic data or information and methods of collection and storage thereof;

(d) interception, review or decryption procedures and safeguards;

(e) security of critical information infrastructure;

(f) mechanisms for regional and international cooperation in cyber security;

(g) formation, management and co-ordination of emergency response teams with other teams; And

(h) Cloud Computing, Metadata.

**Revocation and Custody**

59. (1) The Digital Security Act, 2018 (Act No. 46 of 2018), hereinafter referred to as the said Act, is hereby repealed.

(2) Immediately before the said repeal, pending cases under the said Act in the concerned Tribunal and appeals against the order, judgment or punishment given in similar cases shall be conducted and disposed of in the concerned Appellate Tribunal as if the said Act had not been repealed.

(3) All the cases in which a report or complaint has been made or a charge sheet has been filed or the case is under investigation due to an offense under the said Act shall also be deemed to be a case under trial in the Tribunal referred to in sub-section (2).

(4) Notwithstanding the repeal under sub-section (1), under the said Act—

(a) all movable and immovable properties, documents and liabilities, if any, of the constituted Digital Security Agency shall be vested in the National Cyber Security Agency;

(b) rules made, orders issued, instructions, notifications or guidelines or any measures made, notified or adopted shall, subject to their being consistent with the provisions of this Act, remain in force until repealed under this Act, and the same made, issued under this Act, shall be deemed to have been made, notified or received;

(c) all officers and employees including the Director General and Directors of the constituted Digital Security Agency shall be deemed to be the Director General, Directors and officers of the National Cyber Security Agency, and shall be employed or employed in the National Cyber Security Agency on the same terms as they were employed or employed in the Digital Security Agency; shall be deemed to have stayed;

(d) the National Computer Emergency Response Team and the Computer Emergency Response Team constituted under this Act shall be deemed to be the National Computer Emergency Response Team and the Computer Emergency Response Team;

(e) a digital forensic lab established shall be deemed to be a digital forensic lab established under this Act;

(f) A computer system, network or information infrastructure declared as critical information infrastructure shall be deemed to be a declared critical information infrastructure under this Act.

**Publication of translated texts in English**

60. (1) After the commencement of this Act, the Government shall, by notification in the Official Gazette, publish an authentic English text of the original Bengali text of this Act.

(2) In case of conflict between the English text and the original Bengali text, the Bengali text shall prevail.