Digital Security Act, 2016

Act No. ..... of 2016

That it is justified and essential to enact rules for national digital security and digital offences remedy, protection, control, identification, investigation and for the purpose of justice and relevant issues;

That is why, the under mentioned laws are hereby enacted:

First Paragraph **Preliminary**	
Brief Headlines	Section-1: Headlines (1) This Act will be called as Digital Security Act, 2016. (2) Its application will be imposed on entire Bangladesh. (3) This will be effective immediately.
Definition	Section-2: If it is not otherwise contrary to any issue or relevancy, in this Act- (1) "Lawful Access" means any person will get access to any personal computer or digital device, network or digital system of any program or to any data system, if- a) that person has lawful access right to keep in his full control any computer or digital device, any program of network or digital system or data, or b) that person attains lawful permission from the person who has lawful access right to keep in his full control any computer or any program of network or digital system or data or information, or c) if any data or information or both which is Open Data or declared open to all under any other law, or d) for fulfillment of objective of this Act and for the interest of national security those law enforcing agencies have the right to do lawful interception; (2) "Unlawful Access" means all kinds of access beyond Lawful Access outlined in Section-2(1); (3) "Critical Information Infrastructure" means (a) those infrastructure are essential for running the country and the constitutional bodies and such kind of other assets, system and network, or data which is the imperial part of the government or the Judicial Division, of which intagnantcy or destruction, national integrity& sovereignty, economy, public health related issues that may be exposed to harmful impact; (b) Any of such infrastructure declared by the government;

	(4) e-Payment means- (a) of any person by whom for transfer of his fund to any other bank or any financing institutions or by any other media to any definite Account for depositing or withdrawl of money the given instruction or order authorrtative lawful transaction will mean; or (b) will mean for any buy or sale through automated teller machine or telephone number or internet or credit card or debit card or any other electronic or digital media through which money is transacted; or (c) will mean the definition under the jurisdiction of law that has been enacted time to time by the Government ; (5) "Data corruption or Computer corruption or damage" means such type of programs or computer or digital instructions which cause alteration or damage or interception to any asusal activities of such all programs or computer or digital device or computer system or computer or digital network wherein kept any record, data or transmission to program or on transmission activities; (6) "Data" means information, knowledge, incidence, ideas or instructions prepared under any definite system, computer or digital print-out, magnetic or optical or any other digital storage media, punch-cards, including punch-taps or in any other form or arrangement, computer or digital system or cnptr or digital network that have been processed, being processrd or will be processed or that have been kept in the computer memory; (7) "Program" means through readable medium words including machine, signal, circumscrbings or or in any other form published instructions, by any work is done by computer or to make effectual practically; (8) "Content" means all published information, data in the form of Digital Format; (9) "Computer or Digital device" means- (a) Any electronic, digital, magnetic , optical or equipment for fast speed information processing or system which using the electronic, digital, magneic and optical impulses complete the logical, arithmetic and memory functions and connects to any computer or digital device system or computer netrwork and within it all inputs, outputs, processing, storage, computer or digital divice software or communication facilties are also included; or (b) will mean mobile phone, tablet, smart device or any kind of equipment or digital input, output enabled all kinds of divices; (10) "Computer or Digital Network" means such kind of inter-connections with which there are satellite, micrwave, terrestrial-line, wireless equipment, wide area network, local area network, infrared, Wi-Fi, bluetooth or any other communication media or any Terminal equipment or two or more computer inter-connections, of such complex, whereat remains uninterrupted inter-connextions or nothing of such, through it to establish connections between two or more computers or digital appliances.

	(11) "Company" means any business institution, partnership business, association or organization; (12) "Subscriber Information" means any information held in computer or digital device data form or in any other form which has been held by the provider for the services sent by the clinent. But this type of traffic or content data will not be included of it, in that the following issues may be established, or (a) Type of used communication services or any communication address, telephone and other access numbers, including information of bill payment regarding the place of communication equipment installation any other information which are published from service through service; (13) (a) "Tribunal" means Cyber Tribunal formed under Section 68 of this Act or information & Communication Technology (Amended) Act, 2006 (Act No. 39 of 2006). (14) "Trafic Data" means any Data related with communication through computer or digital or mobile network system which has been produced through computer or digital or mobile network system and forms any part of communication source, destination, rout, time, date, form, duration or type of communicatin chain. (15) "Digital or Electronic Forgery" means by one or more persons without any authority or in given authority as an access or through exercise beyond right create any input or output of any computer or digital divice or alter or delete or hide through incorrect data or information or incorrect program wrong or wrong work or in the wrong activities, information system orwill mean operating of computer or digital network ; (16) "Digital Pornography" means- (a) Any conversation that induces stimulation of sex, acting , moving show of body organs, nacked or half-nacked dance which are held through film, video picture, audio-visual pictures, static picture, graphics or any other means or displayable and which has no art or educational values; (b) Indecent Books of sex stimulation, periodicals, leaflets, web contents; (c) will mean the presentation of material, digital or electronic topics mentioned in Sub-clause (a) or (b) through digital media. (17) "Digital Child Pornography" means such elements that is visible through digital medium or by other means making colorful- (a) To involve any child within the area of sexual activities; (b) To engage any child in sexuality; (18) "Digital Information System" means through use of information technology in digital form for processing of data the used computer or in the digital device system or server or work station or terminal or storage system or storage media or communication device or network resources etc. shall be meant;

	(19) "Digital Communication" means by using the technology of electronic, digital, wireless, optical, electromagnetic or those have comparable capability dong transformation of any signal, symbol, sound, picture, moving pircture and injformation, electronic or optical signal or to exchange. (20) "Digital Record" means by any way from any data, record or manufactured picture from any data or portray or sound, which have been created in any electronic arrangement, microfilm or computer or any digital device preserved in micro-piece, received or sent. (21) "Password" means such type of data through which can attain access to computer or digital -----device, computer or digital service or use of computer or digital system. (22) "Unlawful Obstruction" means (a) to create obstruction to any electronic, digital system, magnetic, optical or verbal communication subject-matter any audio equipment, reading equipment or recording equipment; or (b) to create obstruction in the transmission of information from any informaton system (Computer network, Voice or Data network, Data storage or Data storage system, whereat involved with this work. (a1) person or company becomes the proprietor of these information; (a2) if the person or company does not get any power in relevant law for taking decision regarding this type of interception; (a3) if there is no concurrence of the person or company recipient of real responsibility of these information; (23) "Access" means computer or digital device, computer or digital network, computer program or in computer arrangement informaton oriented or doing accumulation, for recovering of information or intercepting the course of information, of information or data processing, for doing alteration of information or computer program, through output device for the purpose of print or by any other means in computer, computer network, computer program or in computer arrangement of such trasmission, instruction or communication to establish. (24) "Identity Information" means any information which is biological or physical or any other information which uniquely or jointly other information which identifies a person or system, whose name, photograh, address, date of birth, mother's name, father's name, signature, national identification card, birth and death, registration number, finger print, passport number, Bank account number, driving license, E-TIN number, electronic or digital signature, User name, Credit or Debit Card Number, Voice Print, Retina Image, Iris Image, DNA Profile, Security Question or any other identities which are available for the excellence of the technology;

	(25) 'Code of Criminal Procedure' means Code of Criminal Procedure, 1898 (Act No. V of 1898). (c) 'Judge, cyber tribunal' is the judge of the cyber tribunal formed under the section 68 of the Information & Communication Technology Act, 2006 (Act No. 39 of 2006). (26) 'Virus' means computer or digital direction or information or data or programme or apps that (i) creates adverse effect in the efficiency of doing works destroying the works done by any computer or digital device; or (ii) becomes active at the time of any command is given to any programme, data of the said computer or digital device connecting itself with another computer or digital device and occurs any incident in the said computer or digital device through this; (28) 'Director General' means the director general appointed under the section 5(2) and the additional director general, director, deputy director and assistant director authorized by him/her; (29) 'Child' means, whatever in other acts, all children aged maximum 18(eighteen) will be considered as children with a view to fulfilling the purposes of this act; (30) 'Terror Assets' means assets which may fully or partially be used in terrorist activities directly or indirectly or have been used or received through use and assets of any person, company or entity marked as the terrorist in Bangladesh and abroad. (31) 'Service Provider' means (a) any govt. or non-govt. person or institution who or which supplies ability of the communication through computer or digital system; or (b) Other person, entity or organization who or which processes or stores data on behalf of the user of the said services; (32) 'Assistance' means assistances in the investigation, prosecution, forfeiture and proceedings of the trial regarding this offence; (33) 'Social Media' means mutual interaction offline or online, data exchange, chat, videochat, e-mail, group or page or blog site. (34) 'Police Officer' means the officer with the rank of police super or above of Bangladesh Police. (35) 'Defamation' means the defamation mentioned in the section 499 of the Bangladesh Penal Code, 1860. (36) 'Obscene' means such things that pervert and pollute human mind and if these are published, any individual or institution will suffer final or defamatory loss.
Priority of the act	Section-3: Whatever in any other act effective in the time being, directions made under the rules of this act will remain effective.
Application of the act	Section-4 (1) If any person perpetrates any offence under this act outside Bangladesh for which he/she may be convicted under this act, for this reason, this act will be applicable in such a way that he/she has committed the offence in Bangladesh. (2) If any person commits any offence through any computer, computer system or computer installed in Bangladesh under this act, the provisions of the same will be applicable against this person in such way that the offence was committed in

	Bangladesh.

	(3) If any person commits any offence outside Bangladesh under this act from Bangladesh, the provisions of the same will be applicable against this person in such way that the offence was committed in Bangladesh.
Second Chapter Digital Security Agency	
Formation and functions of the digital security agency	Section-5. (1) The government cant form competent authority in accordance with this act under the information and communication technology division with a view to ensuring the national digital security; (2) The government can create a new office of 'Digital Security Agency' with necessary workforce with a view to fulfilling the purposes of this act. There will be a director general of this authority and the government will appoint additional director general, director, deputy director and assistant direct as well as other officers; (3) The director general will carry out all works vested on him/her under this act subject to the control and supervision of the government; (4) The additional director general, deputy director and assistant director will carry out all works vested on him/her under this act subject to the control and supervision of the government; (5) The qualifications, experiences and conditions of service of the director general, additional director general, director, deputy director and assistant director as well as other employees will be determined by the rules; (6) The head office of the director general will be located in Dhaka and branch office can be set up for a specific period or permanently in any place of the country; (7) There will be seal in the office of the director general which will be approved by the government and used in appropriate case; (8) One or more digital forensic labs will be set up under the control of the director general as per this act. Besides, the government can set up other necessary digital labs for ensuing the digital security and prescribing remedies if the digital security falls in threat; there will be arrangement of workforce with necessary technical knowledge in 'Digital Security Agency. (9) The qualifications and experiences of the officers and employees of 'Digital Security Agency' will be determined by the rules. (10) Additional secretary or officer with the designation of 2nd grade or a person specially experienced in digital security will be the director general of 'Digital Security Agency'. (11) 'Digital Security Agency' will be introduced as the digital security center of Bangladesh. (12) 'Digital Security Agency' with a view to providing security to all computers or

	digital system, network, mobile or digital communication (voice & data) network, preventing cyber crimes and such criminal activities- (a) Observing and managing cyber crimes; (b) Coordinating and monitoring the activities of other organizations involved in financial activities with Bangladesh Bank or Ministry of Finance through computer, computer system or computer network or mobile (voice & data) network; (c) Calling report in any matter regarding digital crimes from other organizations involved in computer, computer system or computer network or mobile (voice & data) network; (d) Reviewing the report received under the item (c) and taking measures accordingly; (e) Training will be provided on the cyber security to the officers and employees of the organizations involved with computer, computer or digital system or computer or digital network and the list of trained workforce will be preserved. (f) And activities as per other orders of the government regarding the cyber crime and security. (13) There will be a main team named 'Bangladesh Cyber Emergency or Incident Response Team (Bangladesh-CERT) under the 'Digital Security Agency'. There can be multiple CERT based on the ministry or sector for the government organizations with a view to ensuring the cyber security who will conduct the activities in coordination with Bangladesh-CERT and will be controlled by the rules of its formation and activities. If cyber security is hampered or cyber attack occurs anywhere in Bangladesh, 'Bangladesh Cyber Emergency or Incident Response Team (Bangladesh-CERT) will take immediate remedies in regard of the cyber attack. Bangladesh-CERT will sat with the director general, digital security agency, secretary of information and communication technology in meeting and present the monthly overall picture of digital security in Bangladesh.
National Digital Security Council	Section- 6. (1) A 'National Digital Security Council' will be formed with a view to discussing on the overall matters of the digital security and taking national important decisions on the digital security. (2) The formation and activities of 'National Digital Security Council' will be controlled by the rules.

Third Chapter	
Essential Information Infrastructure	
Declaring few specific computer systems or networks as national vulnerable information infrastructure	Section-7. (1) The director general can announce few specific computer systems, networks or information infrastructures engaged for the economic and social welfare of national security or citizens of Bangladesh the essential information infrastructure through government gazette. (2) The director general will prescribe minimum standard, directions, rules and processes on the following matters as per the sub-section (1), such as: a) Protecting and preserving the essential information infrastructure. b) General management of the essential information infrastructure. c) Access, transfer and control of the information of any essential information infrastructure. d) Infrastructural and systematic rules and policy for the security of the validity and integrity of the information and data of any essential information infrastructure. e) Storage or archiving the information or data of the essential information infrastructure. f) Emergency plan in the incident of damage of the essential information infrastructure or any part of it; and g) Other necessary directions for the adequate security, proper management and control of the information or data of the essential information structure or other properties.
Observation and inspection of the essential information infrastructure	Section- 8. (1) The director general can give direction time to time to observe and inspect any essential information infrastructure for ensuring whether the provisions of this act have been observed or not. (2) If there are logical reasons to believe to the director general that any person or institution is threatening or detrimental to any essential information infrastructure, he/she can inquire into it spontaneously or on receipt of complaints from anyone. (3) The director general can formulate regulations in regard of conducting the observation and inspection of the infrastructure under the sub-section (1).
Fourth Chapter **Offence and Penalty**	
Offences against the essential information infrastructure	Section 9: If any persons commits any offence against the essential information infrastructure, he/she will be convicted to maximum 14 (fourteen) years imprisonment or fined maximum one crore taka or both.
Forgery regarding the computer or digital devices	Section 10. (1) If any person willingly or deliberately makes harm to information, deletes, destroys, tries to get advantages of him/her or other person or make harm to others with a view to proving the information through adding new information or distorting the same in any computer, computer programme, computer system or computer network or device, social media or digital network, this will be deem as offence. (2) If any person commits any offence under the sub-section 1), he/she will be

	convicted to maximum five years imprisonment, or fined maximum three lac taka or both.
Fraudulence regarding computer	Section 11. (1) If any person willingly or deliberately makes harm to information, deletes, destroys, tries to get advantages of him/her or other person or make harm to others with a view to proving the information through adding new information or distorting the same in any computer, computer programme, computer system or computer network or device, social media or digital network, this will be deem as offence. (2) If any person sends any electronic message to the receiver with a view to cheating for which make harm or loss to the receiver for providing wrong information, it will be considered as an offence. (3) If any person commits any offence under the sub-section 1), he/she will be convicted to maximum five years imprisonment, or fined maximum three lac taka or both.
Fraudulence over identity and impersonation	Section-12. (1) If any person using any computer, computer programme, computer system or computer network or any digital device, digital system, digital network or social media, willingly or deliberately- (a) impersonates or shows any information of others as his/her own, with a view to cheating or deceiving; or (b) impersonates of any living or dead person through deliberate forgery: 1. for the advantages of his/her or others; 2. for acquiring the title and interest of any property; 3. for making harm to anyone impersonating of any other person, entity or company; His/her such acts will be considered as offences. (2) If any person commits any offence under the sub-section (1), he/she will be convicted to maximum five years imprisonment, or fined maximum three lac taka or both.
In emergency situations, the power of the director general to give directions	Section-13. (1) If the director general is hereby pleased that it is expedient and necessary to give directions for the interests of protecting the sovereignty, integrity, security of Bangladesh and friendly relationship of Bangladesh with other countries, public discipline and security, he/she can give directions to law enforcing agencies of the government by order mentioning written reason for obstructing the broadcast of information through any computer resource. (2) If any order is given under the sub-section (1), any client or the supervisor of the computer resource should be bound to provide all facilities and technical assistance to the said agency for decrypting any information as per the direction mentioned in the order. (3) The breach of the direction mentioned in the sub-sections (1) or (2) will be an offence. If any person violates the direction mentioned in the sub-section (1) & (2), he/she will be convicted to maximum five years imprisonment, or fined maximum three lac taka or both.
Digital or	Section-13.

cyber terrorist activities	(1) If any person, entity, company or foreign national- (a) with a view to restrain the government or any company or any person to do any work through creating panic among people for endangering the integrity, solidarity, public security or sovereignty of Bangladesh- (i) hampers any person to access in any computer, computer programme, computer system or computer network or device, social media or digital network or makes attempts to do so; or (ii) illegally access to any computer, computer programme, computer system or computer network or device, social media or digital network of others or makes attempts to do so or abets, instigates others or hatches conspiracy; or (iii) makes damage to any person to access in any computer, computer programme, computer system or computer network or device, social media or digital network of any person, entity or the republic or makes attempts to do so; or (iv) uses any programme, pollutant or virus or keeps in his/her possession with a view to fulfilling the purposes mentioned in the sub-sections (i), (ii) and (iii); (b) commits any offence as mentioned in the sub-sections (i), (ii) and (iii) with a view to hampering the security and making harm to the properties of any country or makes attempts to do so or abets, instigates others or hatches conspiracy; or (c) commits any offence as mentioned in the sub-sections (i), (ii) and (iii) with a view to restraining any international organization from doing any work or takes initiative to do so or instigates or abets or hatches conspiracy in such offences; (d) uses any programme, pollutant or virus or keeps in his/her possession with a view to fulfilling the purposes mentioned in the items (ii) or (iii) in a willing or deliberate manner; (e) abets, instigates or hatches plot to commit any offence mentioned in the UN convention under the schedule A of the Anti-Terrorism Act, 2009 (Act No. 16 of 2009 through any computer, computer programme, computer system or computer network or device, social media or digital network or makes attempts to do so. (f) (In any conflicting adverse situation), does any act with a view to make any serious harm to any computer, computer programme, computer system or computer network or device, social media or digital network of any civil or state organization that didn't actively take part in hostilities in a situation of armed conflict and intimidates people or damages relationship of Bangladesh with other countries and international organizations or makes bound to restrain to do any work which is detrimental to the foreign policy of Bangladesh.

	(g) If anyone carries out any propaganda, campaign against the Liberation War of Bangladesh or the spirit of the Liberation War or Father of the Nation or abets in

	such acts, it will be considered that such person, entity or foreign national has committed an offence; (2) If any person or foreign national- (i) commits any offence under the sub-items (ii) and (ii) of the item (a) of the sub-section (1), he/she will be convicted to maximum 14 (fourteen) years imprisonment or fined maximum one crore taka or both; (ii) commits any offence under the sub-item (iii), he/she will be convicted to maximum 10 (ten) years imprisonment or fined maximum twenty five lac taka or both; (iii) commits any offence under the sub-item (iv), he/she will be convicted to maximum 7 (seven) years imprisonment or fined maximum ten lac taka or both; (3)If any person or foreign national commits any offence under the items (b), (c), (d), (e), (f) or (g)of the sub-section (1), he/she will be awarded life imprisonment or fined one crore taka or both. (4) If any person or entity or company perpetrates terrorist acts, (a) actions can be taken against the said person or entity or company under this section and fine can be imposed threefold of the properties relating to the said offence or maximum 1 (one) crore taka; and (b) The chief of the company whatever he/she is termed in the name of chairman, managing director, chief executive or others, he/she will be convicted to maximum 14(fourteen) years imprisonment or fined twofold of the properties relating to the offence or maximum 30 (thirty) lac taka or both.
Punishment for violating the confidentiality	Section- 14. (1) If any person takes the photograph of others willingly or deliberately and publish or send or distort the same with an ulterior motive, such act will be considered as the violation of the personal confidentiality. (2) If any person commits any offence under the sub-section (1), he/she will be convicted to maximum fiveryears imprisonment or fined maximum ten lac taka or both. Interpretation- For fulfilling the objectives of this section (a) 'Send' means sending any visible image to any person/s with a view to exhibiting the same; (b) 'Taking scenes' regarding the image means recording video tape, film, photograph in any way; (c) 'Private parts' means nude or secret parts wearing underwear, surroundings of the genitals, buttocks or breasts; (d) 'Scope of the situation of violating the confidentiality' means any person may have reasonable longing in any situation that (i) any person can be nude secretly, it was captured avoiding his/her attention in his/her personal area; or (ii) Any person irrespective of government or personal was in such an area where he wasn't visible to public.
Pornography, child	Section- 15. (1) If any person-

pornography and offences concerned	(a) publishes pornography through to any computer, computer programme, computer system or computer network or device, social media or digital network; or (b) publishes any advertisement or make any cause to publish this, there is a possibility to distributed or exhibit pornography or obscene elements; or (c) access to any computer, computer programme, computer system or computer network or digital device, digital system or digital network with an ulterior motive; (2) If any person- (a) publishes child pornography through to any computer, computer programme, computer system or computer network or device, social media or digital network; or (b) publishes any advertisement or make any cause to publish this, there is a possibility to distributed or exhibit child pornography or obscene elements related to children; or (c) access to any computer, computer programme, computer system or computer network or digital device, digital system or digital network with an ulterior motive; It will be considered that the said person has committed the offence of pornography or child pornography. (3) If any person commits any offence under the items (a), (b) and (c) of the sub-section 1), he/she will be convicted to maximum 7(seven) years imprisonment or fined five lac taka or both. (4) If any person commits any offence under the items (a), (b) & (c) of the sub-section (2), he/she will be convicted to maximum 10 (ten) years imprisonment or fined 10 (ten) lac taka or both.
Defamation, false and obscene, hurting the religious feelings	Section- 16. (1) If any person defames any person or institution in website or any electronic arrangement under the section 499 of the Penal Code (Act No. 45 of 1860), it will be an offence. (2) If any person publishes or broadcasts in the website or any electronic device deliberately which is false or obscene and perverts or pollutes human mind, makes defamation in terms of money or belittles socially, it will be considered as an offence; or (3) If any person publishes in any website or electronic arrangement that hurts the religious feelings of others after seeing that, it will be considered as an offence. (4) If any person commits any offence under the sub-sections (1), (2) & (3), he/she will be convicted to maximum 5 (five) years imprisonment or fined 5 (five) lac taka or both.

Creating hostility and	If any person publishes anything in the website or the electronic arrangement that will create hostility among different classes of people on sight or deteriorates the

deterioration of the law and order	law and order or there is a possibility of such thing, he/she will be convicted to maximum 7 (seven) years imprisonment or fined 7 (seven) lac taka or both.
Perpetration of offences by the company	Section-16: If any company commits any offence under this act, it will be considered that the owner, chief executive, director, manager, secretary or any officer or employee or representative of the company have committed the offence.
Fifth Chapter Investigation and Search	
Inquiry of the offence	Section-17. (1) Whatever in the code of criminal procedure, the director general or any officer authorized by him/her or any police officer not less than the rank of sub-inspector can investigate into any offence or other matters concerned and he/she can enter in any place in compliance with the fixed method, if necessary. (2) In case of the investigation into any offence, the director general or any officer authorized by him/her can apply the power as the officer-in-charge of the police station can apply power under the code of criminal procedure. (3) Whatever in the sub-sections (1) & (2), any officer authorized by the director general or any police officer can't investigate into any offence under this act. (4) If it appears at any stage of the investigation into any case, it is necessary to vest the responsibility of the investigation into this case- (a) to the director general or the officer authorized by him/her from the police officer, or (b) to the police officer from the director general or the officer authorized by him/her, the government or in some cases, the cyber tribunal can transfer the responsibility of investigating into the offence to the director general or the officer authorized by him/her from the police officer or to the director general or the officer authorized by him/her from the police officer. (5) (a) The investigating officer will complete the investigation within two months from the day of getting the responsibility. (b) If the investigating officer fails to complete the investigation with the timeframe mentioned in the sub-section (5)(a), he/she can extend the timeframe submitting reasons in writing. (c) If the investigating officer fails to complete the investigation within the timeframe mentioned in the sub-section (5)(b), he/she will inform it to the director general and in cases, judge, cyber tribunal in a form of report and the director general will complete the investigation within next one month subject to the permission of the judge, cyber tribunal. (d) If the investigating officer fails to complete the investigation under the sub-section (c), the director general and in some cases, the judge, cyber tribunal can extend the timeframe reasonably. (6) For the interest of the proper investigation into the cyber crimes, the government will ensure the use of all modern technologies including one or more digital forensic labs under the director general.
Rights of access and inspection	Section- 18. (1) For the interest of any investigation into the offence under this act, the director general or the officer with the rank of police super or officer authorized by him/her

	will exercise the following powers: (a) To take the possession of computer, computer programme, computer system or computer network or any digital device, digital system or digital network or any progamme, information, data which have been stored in any compute or compact disc or removable drive or any other way or access into the same; (b) To make any person or organization bound to supply the traffic of information or data; (c) To do what is reasonably required to do with a view to fulfilling the purposes of this act. 2. Under this act, the director general or the police officer can take the assistance of any expert person or specialized organization for the interest of the investigation and the government will bear the costs in this connection.
Access, search and seizure by dint of warrant	Section- 19. If there is reason of the director general or the officer with the rank of police officer to believe that (a) any offence has been committed or there is a possibility to be committed under this act or (b) If any computer, computer system or computer network, information, data or evidences regarding this, is kept in any place or to any person, the following works can be done writing down the reasons of such belief and collecting the search warrant through the application to the cyber tribunal or chief judicial magistrate or chief metropolitan magistrate, in some cases- i) to take in the information and data of any traffic in the possession of any service-provider; ii) To create any telegram or electronic communication obstacle including client information and data of the traffic at any stage of the communication.
Search, seizure and arrest without warrant	Section 20. (1) If there is reason of the director general or the officer with the rank of police officer to believe that any offence under this act has been committed any place or being committed or there is a possibility of the perpetration of such offence or there is a possibility that the evidences will be lost, damaged, deleted, altered or unavailable in any way and adequate time isn't get for collecting the warrant, he/she can do the following works accompanied by an executive magistrate from the district magistrate, in case of district, and the upazilanirbahi officer, in case of upazila, and writing down the reasons of belief: (a) He/she can search entering into that place and if he/she is obstructed, actions can be taken as per the code of criminal procedure; (b) During carrying out search in that place, he/she can seize the computer, computer system or computer network, information, data and other materials used in perpetrating the offence and seize any document that can help to prove the offence; (c) He/she can search the body of anyone present there; (d) He/she can arrest any person present there on suspicion that he/she has committed offences under this act; After the completion of the search, the police personnel, sub-inspector or above, present there will submit a report, in some cases, to the cyber tribunal

	or chief metropolitan magistrate or chief judicial magistrate. (2) Any sub-inspector or any officer above this rank can't access to any suspected computer, computer system or computer network or information-data, if he/she has no sufficient knowledge in information and communication technology and he/she is sufficiently expert to do these works.
Data preservation	Section-21. (1) If there is reason of the director general or the officer with the rank of police officer to believe that it is necessary to preserve any data and information stored in the computer for the interest of the investigation and there is a possibility to destroy, alter or make data unavailable, he/she can give direction to the person or institution responsible for the computer or computer system to preserve data for 90 (ninety) days. (2) But in regard of the application, the cyber tribunal can extend the period of preserving data. But it can't be more than 180 (one hundred eighty) days.
Not interrupting the normal use of computer	Section 22. (1) The director general or the police officer will conduct the investigation in such a way so that legal use of the computer, computer system or computer network or part of it can be interrupted due such investigation. (2) Any computer, computer system or computer network or part of it can be seized, if (a) it is not possible to access in this computer, computer system or computer network or part of it; (b) there is a possibility of destruction, alteration or unavailability of data for preventing the offence or not to seize for preventing the current offence.
Method of the search	Section-23: If there is nothing different in the act, provisions of the code of criminal procedure should be applicable in case of investigations, warrants, searches, arrests and attacks under this act.
Assistance in the investigation	Section- 24. Under this act, any person, entity or service-provider will be bound to assist in providing information or in the investigation of the investigating officer.
Confidentiality of the information found in the investigation	Section- 25. (1) If any person or entity or service-provider reveals any information, no case can be filed against that person, entity or service provider under the civil or criminal law. (2) Under this act, all persons or entities or service-providers will keep the information confidential for the interest of the investigation. (3) If any person violates the provisions of the sub-sections (1) & (2), it will be as an offence and he/she will be convicted to 2 (two) years imprisonment or fined 1 (one) lac taka or both.

Taking the offence for trial	Section- 26. (1) Whatever in the code of criminal procedure, cyber tribunal will take any offence for the trial on the basis of the report from the director general or any officer authorized by him/her or any police officer not below than the rank of the sub-inspector.

	(2) If any tribunal is hereby satisfied that if any police officer or authorized officer has failed to take the allegations of the offence on request, the tribunal can directly take any allegation without the report mentioned in the sub-section (1). (3) In spite of not having recommendations of taking the allegation of the perpetration of the offence or taking actions in this regard against any person in the report mentioned in the sub-section, the tribunal can take the allegation concerned for the trial regarding the said person mentioning the reasons, if the tribunal thinks it is necessary for the interest of the justice. (4) During the trial of the offences under this act, tribunal will follow the method mentioned in the chapter 23 of the code of criminal procedure in consistence with the provisions of this act. (5) No tribunal can postpone the proceedings of any case if it is not necessary for the justice and not recording the reasons in writing. (6) Tribunal, on the basis of the application submitted to him or at his/her own initiative, can give direction to any police officer, or in some cases, the director general or any officer authorized by him/her for further investigation of any case regarding any offence perpetrated under this act and submit the report within the timeframe determined by him/her.
Forming cyber tribunal	Section- 27. The provisions of appeal will be applicable in the cyber appellate tribunal formed as per the sections 82, 83 & 84 of the Information & Communication Technology Act, 2006 (Act No. 39 of 2006).
Timeframe fixed for the disposal of the case	Section-28. (1) The judge will complete the trial of the case within 180 (one hundred eighty) days from the day of framing charges under this act. (2) If the judge fails to dispose any case within the timeframe fixed under the sub-section (1), he/she can extend the timeframe for maximum 90 (ninety) days recording the reasons in writing. (3) If the judge fails to dispose the case within the timeframe under the sub-section (2), he/she can continue the proceedings of the case informing the reason in the form of the report to the High Court Division and the director general.
Cognizability and bailability of the offences	Section- 29: The offences under this act (a) The offences mentioned in the sections 9, 13 & 15 are cognizable and Non-bailable. (b) The offences mentioned in the sections 10, 11, 12, 14, 24 & 25 are non-cognizable and bailable.

Provisions regarding the bail	Section-30. The judge won't release any convicted person in the offences punishable under this act, if- (a) the prosecution is given the opportunity of the hearing on the order of the same bail; (b) If the judge is satisfied that (i) there are logical reasons to believe that the convicted person can't be indicted in

	the trial. (ii) Offences aren't grievous in the literal sense and the punishment won't be harsh though the offences are proved; and (c) He/she records the reasons of such satisfaction.
Forfeiture	Section- 31. (1) If any offence is perpetrated, the computer, computer system, floppy, compact disc (CD), tape drive or any ancillary computer accessories by which the offence is committed, will be forfeited as per the order of the trial court of the said offence. (2) If the court is hereby satisfied that the person whose possession the computer, computer system, floppy, compact disc (CD), tape drive or any ancillary computer accessories are found, isn't found guilty, the said computer, computer system, floppy, compact disc (CD), tape drive or any ancillary computer accessories won't be forfeited. (3) If any computer, computer system, floppy, compact disc (CD), tape drive or any ancillary computer accessories are found with the computer, computer system, floppy, compact disc (CD), tape drive or any ancillary computer accessories which are subject to be forfeited, will be forfeited. (4) Whatever in this section, if any computer and other equipments relating to this is used for perpetrating any offence mentioned in the sub-section (1), this won't be forfeited.
Sixth Chapter International and regional assistance	
International and regional assistance	Section 32: In question of the international and regional assistance for conducting the investigation, prosecution and proceedings in regard of any offence under this act, all provisions of the Mutual Assistance Act, 2012 (Act No. 4 of 2012) will be applicable.
Seventh Chapter Miscellaneous	
Acts done in good faith	Section-33: If any person is affected or there is a possibility to be affected for any act done in good faith at the time of performing the duties under this act, no civil or criminal case or any other legal proceedings can't be initiated against any officer or person responsible for this.
Removing the difficulties	Section-34. (1) In case of making the provisions of this act effective, if any difficulty arises due to the absurdity in the said provision, the government can take any necessary measure by the order published in the government gazette for removing this. (2) Each order under this section should immediately be presented in the parliament as soon as possible.

Power of formulating rules	Section- 35. The government can formulate rules regarding the following all matters or any of it with a view to fulfilling the purposes of this act by the gazette notification and additionally in the electronic gazette notification, such as: a) To establish digital forensic lab; b) To conduct the digital forensic lab by the director general; c) Methods of traffic data or information review or collection and the method of

	storage; d) Interference, review or decryption and protection; e) Vulnerable information infrastructure security; f) Method of international and regional assistance. g) Bangladesh CERT formation, management and coordination with other CERTs; h) Cloud computing, meta data and i) Other necessary matters.
Publication of the text translated into English	Section- 36: (1) After the formulation of this act, the government will publish an authentic English text of this act translated into English. (2) Dispute between the Bengali & English texts, Bengali text will get priority.