Cyber Security Law
(2021, State Administration Council Law No.--)
1382 Myanmar Year, ------ month, ------- day
(2021/Month/Day)

National Administration Council hereby enact this law.

CHAPTER (1)
Names, Relations and enactment

1. This Law shall be called "Cyber security law".

2. Provisions in this law shall relate to the following matters.

(A) Offences committed by – anyone residing in the country or on vehicles and aircrafts registered in accord with any existing law; or a Myanmar citizen; or a foreigner temporarily or permanently residing in Myanmar; or offences committed locally and internationally inter alia.

(B) Arrangements, agreements, contracts and covenants made for local and outbound communications; matters related to economy or specific type of electronic information including exchange or storage of information.

(C) Any matter of communications made with anyone either directly or indirectly with regards to the cyber resource within the national cyber space; or between national and other cyber spaces.

3. The following expressions contained in this law shall have the following meanings.

(A) "Nation" means the Republic of the Union of Myanmar.
(B) "State Administration Council" means a national administration council formed under order 9/2021 by the Office of Commander-in-Chief, in accord with Article 419 of the Constitution of the Republic of the Union of Myanmar.
(C) "Central Committee" means a Central committee on cyber security formed by the State Administration Council.
(D) "Steering Committee" means a Steering committee on cyber security formed by the Central committee.
(E) "the Ministry" means a Union Ministry assigned by the State Administration Council to implement cyber security matters.
(F) "Relevant ministry" means a Union Ministry deemed as being related to cyber security matters and assigned by the State Administration Council.
(G) "Department" means a department assigned as an office of secretariat of the Central Committee and Executive Committee on Cyber security.
(H) "Investigation unit" means a task force formed under this law to investigate cyber security related violations and offences.
(I) "Personal data" means any data or information which can identify or have identified who someone is in what relations.
(J) "Official responsible to manage personal data" means a person assigned by the government department or an organization holding authority to collect, gather,

compile and use personal data and information under provisions contained in this law or any existing laws.

(K) "Administration" means collection, obtaining, transferring, dissemination, coordination, restriction, destruction, documentation, archiving, storing, changing, recollection of storages, advising, utilization and disclosure of personal data information.

(L) "Critical information infrastructure" means fundamental information infrastructures such as national security, security of public welfare, transportation, health and finance. This reference also includes other critical information infrastructures as defined and declared by the State Administration Council or the Ministry.

(M) "Official responsible for administration of critical information infrastructure" means a person implementing matters related to critical information infrastructure as defined by the State Administration Council.

(N) "Electronic information" means information created or sent or received or stored by digital electronic technology or electromagnetic wave technology or any other specific technology.

(O) "Electronic or Digital signature" means a symbol or sign arranged by oneself or on behalf of one by digital electronic technology or any other specific technology to verify the origin and non-modification or non-replacement of an electronic information.

(P) "Electronic or Digital certificate" means an electronic information or other records which ensure the relations between – electronic or digital signature issued by the authorized electronic or digital certificate issuer for the user; and the data creating signature.

(Q) "Authorized electronic or digital certificate issuer" means an authorized person who can issue an electronic or digital certificate that can verify the correctness and legality of an electronic or digital certificate.

(R) "Original sender" means a person who acts to create or initiate or send electronic information or anyone who does so on behalf of such a person.

(S) "Receiver" means a person intended to receive electronic information from the original sender. This expression shall not include any intermediary actors who facilitates electronic information for other persons.

(T) "Online service" means any business served via online by using a system similar to the cyber source or materials.

(U) "Online service provider" means any person or any business providing the online service to be used in Myanmar.

(V) "Cyber security provider" means any person who is operating any cyber security service by using either online service, or any systems or materials similar to cyber sources related with informative technology.

(W) A computer means a device that can perform recording, saving, transferring, storing, processing and restoring the information, and mathematical and logical methods usage in terms of either electrical technology or magnetic technology or light transmission technology. "Computer Program or Program" means directives or descriptions referring to the information which enables a specific task of a computer system in operating it.

(X) A computer program or program means any description or guideline providing the facts to run any function of the computer in order to operate any system of the computer.

(Y) A computer system means either any device or any set of integrated and or related devices that can process the data automatically by using a program. This expression shall also include any removable storage medium used while a computer system is running; or any computer program or information stored in such device of a computer system.

(Z) "Data" means completed or in-progress or planned directives, presumptions, data, knowledge, information as well as those which can be stored on computer memory in various forms that have either been prepared or under preparation systematically.

(AA) "Information" means data, text, image, video, code, software, application and database.

(BB) "Communication device" means communication devices or their infrastructures or related devices including those as determined by the Union Ministry, which can interconnect or establish connection by means of a specific technology.

(CC) "Network" means a communication device, computer or computer-like devices and other related systems and devices that can establish interconnection by using specific communication technology by means of cable or wireless or satellite-based or any other technology.

(DD) "Cyber source" means a computer, computer system, computer program or program, network, communication device and data.

(EE) "Access" means accessing a specific cyber source either whole or partially.

(FF) "Hacking" means wholly or partially obtaining data or information communicated by using a network.

(GG) "Malware" means a Malicious code which can interfere or harm a cyber source.

(HH) "Cyber security" means prevention of obtaining, disclosure, sending, disseminating, usage, interfering, changing or destruction of data, cyber source, electronic information and critical information infrastructures without permission.

(II) "Cyber space" means a platform on which electronic information can be sent, communicated, disseminated and received within a technological network or by connecting networks or exchanging vice versa by using information, database, electronic information, computer program, software or application with the use of cyber source on an Information technology network system.

(JJ) "National Cyber space" means a cyber space determined by the Central committee or steering committee.

(KK) "Cyber-crime" means violation or attempting or encouraging violation of any prohibitions contained in this law or any other existing laws on cyberspace by using any cyber source.

(LL) "Online communication" means utilization of any online communication including e-government infrastructure, e-commerce infrastructure, forum, blog and social media network either by an individual or an organization, either within a cyber space or national cyber space by means of specific cyber source or Internet of Things (IoT).

(MM) "Cyber fraud" means illegal access or hacking of data, information, electronic information, or data related to computer systems which are regularly run or stored on a cyber source – either by an individual or group or organization.

(NN) "Cyber-attack" means violation of or an attempt or encouragement or soliciting or coordination to violate any provisions contained in Anti-violence Law; including violence attack that targets national administration, finance, economy, rule of law, national security, public security and welfare by using a cyber source within a cyber space.

(OO) "Member state" means a country from international or regional organizations which is a member to conventions, covenants or agreements related to prevention and coordination of cyber security or cyber-crimes.

(PP) "Online gambling" means gambling by using any cyber source to organize lucky draws or play a game, with or without tolls, that involves an element of skill with the intent of winning money or any property which has money-alike worthiness or which is agreed to be exchanged into money.

CHAPTER (3)
Objectives

4. This law shall serve the following objectives.

(A) To be able to safely and securely use cyber source, critical information infrastructures and data stored with electronic technology, in building a national development.

(B) To be able to protect personal information of the public in accordance with the law.

(C) To be able to safeguard and protect from harassing, cyber-attacking, cyber-bullying, cyber-fraud and cyber-accidents by using electronic technology to harm the national peace and sovereignty.

(D) To be able to supervise in ensuring that cyber security services are systematically implemented in accord with the law.

(E) To prevent cyber-crimes.

(F) To support the digital economy.

(G) To recognize and legally protect the truthfulness and reliability of electronic information in conducting local and international communications using cyber sources.

CHAPTER (4)
Formation of Cyber Security Central Committee

5. State Administration Council shall –

(A) compose the Cyber Security Central Committee with the following to supervise cyber security matters.

(1) Co-chair State Administration Council	Chair
(2) Union Minister Ministry	Co-chair

(3) Union Ministers Relevant Ministries	Members
(4) An appointee by the State Administration Council	Secretary

(B) The composition of the Central committee formed in accordance with the Sub-section (A) shall be replaced as required.

6. The Central Committee shall have the following duties and responsibilities.

(A) Set policies, strategies and programs related to cyber security for the good and safe national cyber space of the nation.

(B) Implement cyber security related policies, strategies and programs; supervising and coordinating to be able to cooperate with foreign countries and international and regional organizations.

(C) Promote training of human resources required to develop and enhance cyber security works.

(D) Promote for the development of cyber security and cyber affairs related infrastructures.

(E) Instruct and coordinate among relevant government departments, government organizations and other organizations to ensure betterment of cyber security; prevent cyber-crimes; and to support rule of law and judiciary sector.

(F) Instruct relevant ministries to plan and draft cyber securities of critical information infrastructures.

(G) Instruct the executive department to review, investigate, advise, present and report cyber security programs.

(H) Inform, restrict and limit local and international cyber security service provider operators and organizations to act in accordance with the cyber security guidelines and programs of critical information infrastructures.

(G) In order to effectively implement objectives contained in this law, determine the information storage of business and operators from the online communication sector in which the public engages through national cyber space.

(I) Execute duties and tasks assigned by the State Administration Council from time to time.

7. (A) State Administration Council shall determine the secretariat unit of Central and Steering Committees.

(B) The secretariat formed in accord with Subsection (A) shall perform under the supervision of the Ministry.

8. The secretariat unit shall –

(A) Incur the expenditures and

(B) Undertake the office works – of the Central and Steering Committee.

CHAPTER (5)

Formation of Cyber Security Steering Committee and its Responsibilities

9. The Central committee, with the approval from the State Administration Council, shall form the following Cyber Security Executive Committee.

(A) Union Minister Ministry	Chair
(B) Deputy minister or Permanent Secretary Relevant Ministries	Members
(C) Cyber security professionals	Members
(D) Representatives from Non-governmental organization	Members
(E) Director General Department	Secretary

10. The duties and responsibilities of the Executive committee is as follows:
   a) coordinates activities in order to identify, prevent cyber-crimes and cyber security
   b) implements training activities in order to ensure the development of cyber security policy, strategies, action plan, infrastructure, and human resources by the central committee to better develop cyber security, cyber-crimes prevention and identification issues
   c) prepares an in-time response system if there is any cyber-attack
   d) coordinates with other relevant ministries to ensure national cyber security
   e) observes and reports to the central committee in accordance with provisions of the cyber security and cyber-crimes related conventions, treaties and agreements so that the country can be a member state.
   f) implements and cooperates in accordance with the provisions of the cyber security and cyber-crimes related conventions, treaties and agreements that the state is a member of
   g) forms necessary working groups and assign their responsibilities with the agreement for the central committee in order to do the cyber security activities
   h) announcing, informing and preventing of cyber security, cyber terrorism and cyber threats news and recommendation to the public
   i) educates and implements trainings on cyber security issues
   j) supervision of emergency response teams for cyber security breach in different sectors
   k) permits, rejects, and sanctions of the license of services mentioned in this law in accordance with policy, strategy and action plan, frameworks
   l) drafts and reports to the central committee with progress reports and other necessary reports
   m) carries out cyber security duties assigned by the central committee as relevant
   n) cooperates with neighbouring countries, regional organizations, international organizations with regards to information sharing, investigation, sanctioning, cooperation and scrutiny

o) scrutinizes and permits cyber security teams or organizations, sanctions on cyber security teams or organizations formed without permission
p) implements the regulation to collect data from the online communication businesses
q) scrutinizes, recommends and reports on the information technology equipment and devices produced within the country or imported from abroad whether they are in line with cyber security policy and standards or not

11. Steering committee with the agreement of the central committee shall form the following working committee in order to implement the objectives of this law:
a) Cyber Security Working Committee
b) Cyber-Crimes Working Committee
c) Cyber Protection Working Committee
d) Other necessary Working Committees

12. Steering committee shall form an Investigation team with the agreement of the central committee if the works outlined in this law require investigation.

CHAPTER (6)
Protection of Personal Information

13. The person responsible for managing and keeping the personal information shall –
(a) systematically keep, protect and manage the personal information based on its types, security levels in accordance with the law
(b) not allow, disclose, inform, distribute, dispatch, modify, destroy, copy and submit as evidence of the personal information of an individual without the consent or the permission in provision of an existing law to any individual or organization.
(c) not utilize personal information for managing issues that are not in compliance with the objectives
(d) systematically destroy the personal information that are collected to be used for a period of time after a certain period

14. The investigation team who receives information that includes personal information in accordance with the existing laws or the person mandated or instructed on their behalf shall keep the information confidential except disclosing the information in hand in accordance with the law.

15. Personal Information Management shall not include the followings:
(a) prevention, search and enquiry, investigation, submission of evidence in a court by the government agency, investigation team or rule of law team assigned by the government for cyber security, cyber-attacks, cyber terrorism, cyber misuse and cyber accident, cyber-crimes
(b) search and enquiry, investigation, data collection, prosecution and submission of evidence in a court by the government agency, investigation team or rule of law team mandated to work on criminal issues
(c) enquiry, investigation, data collection and info-sharing and coordination carried out if the cyber security and cyber-crimes issues are of concerns to the state sovereignty, stability, national security

(d) when carrying out activities in sub-section (c), either the central committee or relevant ministry or department having separate authority and working on it in accordance with those definitions.

CHAPTER (7)
Protection of the Critical information infrastructure

16. The important information infrastructures are as follows;
(a) e-Government Services
(b) electronic information and infrastructure on finance and budgeting
(c) electronic information and infrastructure on water resources
(d) electronic information and infrastructure on transportation
(e) electronic information and infrastructure on communication
(f) electronic information and infrastructure on public health
(g) electronic information and infrastructure on electricity and energy
(h) electronic information and infrastructure on natural resources
(i) electronic information and infrastructure classified for private use only.

17. The Central committees shall;
(a) Amend the list of the important information infrastructure with the approval of the State Administration Council as necessary.
(b) Give instruction to the ministry to inform the process of identifying and amending the list of the important information infrastructure on the specific sectors to the official responsible for managing and maintaining important information of the concerned ministry and government institutions.
(c) Set up policies to keep, record and maintain the information on the important information infrastructure.

18. The Steering Committee shall inspect the readiness of cyber security of critical information infrastructure; and give instructions to ensure it meets the specified standards.

19. Concerned ministries and government institutions shall perform the followings;
(a) Drafting action plans on cybersecurity for critical information infrastructure;
(b) Establishing response teams for cybersecurity breaches;
(c) Submitting cybersecurity report to the Steering Committee.

20. The official responsible to manage and maintain the critical information infrastructure shall;
(a) keep the information on critical information infrastructure at a place permitted by the ministry;
(b) follow the regulations in disseminating, producing, transferring, receiving and saving information on important information infrastructure;
(c) submit the cybersecurity report to concerned ministries annually at a minimum.

21. Steering committee shall coordinate with respective cyber security breach response team to implement protections of critical information infrastructure.

CHAPTER (8)
Electronic Transaction and Electronic Certificate

22. If there is no agreement otherwise, parties entering contracts can use electronic technology in offering, accepting offering or other necessary data.

23. Electronic information shall be deemed as that of the original sender if it is sent either by the original sender himself or by a person authorized to send on behalf of the sender or through an automatic information system arranged by the sender himself or by a person acting on behalf of the sender.

24. It shall be deemed correct that the electronic information of the original sender is sent either by means agreed between the receiver and the original sender; or by the person authorized to send on behalf of the original sender by means of original agreements.

25. The receiver –

(A) shall be deemed of having received information for any of the following methods:

(1) The receiver replying himself or by an automated system or by any other means;

(2) The receiver displays a sufficient demonstration towards the original sender or a person authorized to act on behalf of the sender that he or she had received.

(B) can make a separate agreement to acknowledge the receipt.

26. Unless a specific agreement was made about the time of sending and receiving between the original sender and the receiver;

(a) the time sent is the time when the information arrives at the system for which original sender or a competent authority on behalf of the original sender uses for sending the information.

(b) the time received is when it arrives at the system used for receiving the information.

CHAPTER (9)
Providing Service

27. The cyber security service providers shall perform the following;

(a) planning and implementing cyber security preventing measures to support the Department and Cyber Security Breach Emergency Response teams;

(b) providing warnings on cyber security risks and preventive guidance;

(c) developing response plans and solutions against malicious codes, cyber-attacks, hacking, or other security breaches.

28. Internet Service provider in Myanmar shall ensure the following –

(a) The device that stores the user's information must be kept in a place designated by the Ministry.

(b) Internet Service provider must be registered in accord with the Myanmar company law.
(c) Taxes must be paid in accord with the provisions set forth in relevant laws if it is due to claim any tax relating to the business conducted through internet service or similar profitable business.

29. Prevention, removal, destruction and cessation shall be made accordingly in a timely manner, following the provision of information by the department that an online service provider in Myanmar causes any of the following on cyber space.
(a) Speech, texts, image, video, audio file, sign or other ways of expressions causing hate, disrupting the unity, stabilization and peace.
(b) Misinformation and disinformation
(c) Sexually explicit material that is not culturally appropriate for Myanmar society to see; Photos, Audio file, Videos, Texts, Signs, Symbols and other expressions
(d) Child pornography; Photo, Video, Texts, Symbols and other expressions
(e) written and verbal statement against any existing law

30. The online service provider in Myanmar shall retain the following information from the service users for up to three years from the first date of use of the service.
(a) Username, Internet Protocol (IP) address, telephone number, identification card number and address of the service users.
(b) User record of the service user.
(c) Other information as directed by the Department.

31. An online service provider in Myanmar may provide all or part of the information contained in Section 30 if the assigned person or authorized organization requested under any existing law.

CHAPTER (10)
Obtaining License

32. Anyone willing to operate as an authorized electronic certification issuer in Myanmar must apply to the Department in accordance with the requirements for obtaining a license.

33. Anyone willing to operate a cybersecurity service in Myanmar must apply to the Department in accordance with the requirements for obtaining a business license.

34. Anyone willing to operate an online service shall register at the Department in accordance with the relevant criteria.

35. The Department shall review relevant license application and license renewal pursuant to the stipulations; and shall issue the licenses to applying individual or organization with the approval of the Steering committee.

CHAPTER (11)
Cyber Fraud

36. Any of the following acts performed on a particular cyber source by anyone without permission shall be deemed unauthorized access to information, a specific computer system, program or relevant information regularly run or stored on a specific cyber source.

(a) Changing, modifying, or deleting a program or data and its related status or properties,

(b) Copying, transferring, or relocating a cyber source to one of the followings,

(1) transferring a program or data form its original place of storage to either another cyber source, or a device, or a storage device;

(2) Within the same cyber source or a device or a storage device but to a different location in its system;

(3) Using a computer program or data;

(4) Obtaining data from a computer system by running computer system, or by any other mean.

37. If any of the following acts relating to a computer system or computer program or a specific data is performed without permission, it shall be deemed as an illegal modification of a quality of a particular computer system –

(a) Changing any program or data stored by a respective computer system;

(b) Deleting any program or data stored by a respective computer system,

(c) Putting additional information to a program or data stored by a respective computer system;

(d) Any action that can interrupt the regular functions of a computer system.

38. If any of the following acts relating to a computer system or computer program or a specific data is performed without permission, it shall be deemed as an illegal modification of the facts of a particular computer system –

(a) Changing any program or data stored by a respective computer system;

(b) Deleting any program or data stored by a respective computer system,

(c) Putting additional information to a program or data stored by a respective computer system;

(d) Any action that can interrupt the regular functions of a computer system.

39. The following acts related to a computer system or program or data shall be deemed as controlling;

(a) Controlling any computer or computer system or network, or similar action;

(b) Controlling and executing any computer or computer system or network by another computer system (software/tool).

40. If any of the following states occur to a computer system or a program or data, it shall be deemed as an illegal access to a computer system by a person by any means.

(a) If that person is not the authorized one to oversee the litigated context which shall be assessed relevant with any computer system;

(b) If that person is not the one who does not have permission from the responsible person to oversee the litigated context which shall be assessed relevant with any computer system;

41. Intervention made to a computer program or data by a person with any of the following methods shall be deemed an illegal intervention.

(a) If the person is not the authorized person for a specific computer system;

(b) If the person is not the authorized one to decide whether to make the aforementioned intervention or not;

(c) If the person is not the one who has a permission from a responsible person to make interventions for a specific computer system.

42. The security cameras shall be installed in crowded places, public places, and where necessary for security in accordance with the specified rules and regulations.

CHAPTER (12)
Protecting and Responding Cyber Crimes and Cyber Attacks

43. Cybersecurity Working Committee, Cyber Crime Working Committee, and Cyber Protection Working Committee shall implement the followings regarding any events of cyber security threats, cyber-attacks, cyber terrorism, cyber fraud, or cyber incident;

(a) Accessing potential impacts or impacts of cybersecurity threats, cyber-attacks, cyber terrorism, cyber fraud, or cyber incidents;

(b) Preventing any other consequences of cybersecurity threats, cyber-attacks, cyber terrorism, cyber fraud, or cyber incidents from occurring;

(c) Preventing cybersecurity threats, cyber-attacks, cyber terrorism, cyber fraud, or cyber incidents from occurring;

(d) To increase the levels of cybersecurity, retrieving, storing, transferring, and monitoring the information which is stored, received, sent, or created in a computer or computer system aiming;

(e) Investigating and taking actions against cybersecurity threats, cyber-attacks, cyber terrorism, cyber fraud, or cyber incidents.

44. The online service provider or the cybersecurity service provider shall coordinate and collaborate to implement the activities prescribed in Section 43.

45. Cybersecurity Working Committee, Cyber Crime Working Committee, and Cyber Protection Working Committee, in implementing activities prescribed under Section 43, can inspect the computer or computer system of the following persons who are considered to be related to any cybersecurity threats, cyber-attacks, cyber terrorism, cyber misuse, or cyber incidents;

(a) The user or the person suspected as the user who uses any computer or any computer system or any network which are considered to have been related to any cybersecurity threats, cyber-attacks, cyber terrorism, cyber fraud, or cyber incidents;

(b) The person who is related with any person mentioned in sub-section (a).

46. Cybersecurity Working Committee, Cyber Crime Working Committee, and Cyber Protection Working Committee shall return the computer or computer systems to the provider systematically after assessing, analysing, and investigating that computer or computer systems.

47. State Administration Council can grant a relevant person or organization the authority to intervene, in order to conduct interventions prescribed under existing laws.

48. The companies and organizations providing services as prescribed in Communication Law shall arrange and prepare for the relevant person or organization granted with authority in accord with Section 47 to be able to intervene.

49. A relevant person or organization granted with authority to intervene as per Section 47 shall conduct any of the following interventions without interfering the fundamental rights of the citizens;

(a) Preventing issues that can harm the sovereignty and territorial integrity of the State;
(b) Performing acts of State Defence and security;
(c) Performing acts of Rule of Law and public order;
(d) Investigating crimes;
(e) Issues permitted in accordance with the existing law;
(f) Acts to safeguard and protect public life, property and public welfare.

50. The ministry, or the department or the organization assigned by the ministry can visit and check and oversee the site of any online service provision business, and can ask to present labels either to serve the purpose of state defence and security or for the public interests.

51. In the event of a need to act for the public interests, the ministry can conduct the following with the approval of the State Administration Council;

(a) Temporarily prohibiting any online service provision in Myanmar;
(b) Temporarily controlling the devices related to online service provision in Myanmar temporarily;
(c) Final ban to any of the online service provision businesses in Myanmar.

CHAPTER (13)
Seizing Evidential Materials and Submitting Expert's Witness

52. The Inspection Body shall, if required to seize evidential materials to inspect for rule of law processes, handle and seize them pursuant to provisions under this Law and any other existing laws.

53. The Inspection Body can submit to the court the evidential materials in electric or digital form pursuant to the stipulations after assessing, analysing and studying them.

54. The Digital Forensic Lab will be established in order that the respective working committees could implement their duties, and expert witnesses can be submitted to the court in the form of digital evidential materials pursuant to the stipulations.

CHAPTER (14)
Online Gambling

55. Regarding online gambling, no one shall, without permission: -

(a) claim or collect stakes for gambling;
(b) gamble, encourage or assist someone to gamble, gather or solicit people to gamble; and
(c) through any cyber sources, organise lucky draws or play a game, with or without tolls, that involves an element of skill with the intent of winning money or any property that is worth like money or that have been agreed to be exchanged into money.

CHAPTER (15)
Offences and Penalties

56. If a person responsible to manage personal data is convicted of failure to manage personal data in accord with the provisions under this law, he or she shall be punishable by an imprisonment for a term not exceeding 3 years or a fine not exceeding 100 lakhs or both.

57. Any person, if convicted of obtaining, disclosing, using, destroying, modifying, disseminating or sending personal data of a person to another without approval, shall be punishable by an imprisonment for a term not exceeding 3 years or a fine not exceeding 100 lakhs or both.

58. If a person responsible to manage critical information infrastructure is convicted of failure to perform his or her duties under Section 20, he or she shall be punishable by an imprisonment for a term not exceeding 3 years or a fine not exceeding 100 lakhs or both.

59. Any person who is convicted of interfering, destroying, stealing, harming, illegally sending, modifying or changing electronic information, shall be punishable by an imprisonment for a term not exceeding 3 years or a fine not exceeding 100 lakhs or both.

60. Any person who is convicted of interrupting a communication within a network or using a data contained in a communication or disclosing a data to another person, without the approvals from the original sender and receiver, shall be punishable by an imprisonment for a term not exceeding 3 years or a fine not exceeding 100 lakhs or both.

61. Online service provider who is convicted of failure to comply with provisions prescribed in this law shall be punishable by an imprisonment for a term not exceeding 3 years or a fine not exceeding 100 lakhs or both.

62. Any person who commits any of the following acts in bad faith or dishonesty shall be punishable by an imprisonment for a term not exceeding 3 years or a fine not exceeding 100 lakhs or both.

(A) Dishonest attempt to access cyber source without permission;

(B) Extracting, copying, downloading or destroying any data stored on any removable storage medium or any information from cyber source;

(C) Infecting a cyber source with or inserting malwares and other elements that can compromise computer functions;

(D) Interrupting a cyber source;

(E) Preventing access of any authorized person to access a cyber source;

(F) Encouraging or assisting access to cyber source in violation of the regulations prescribed by the law;

(G) Interfering a person by using a cyber source of another person by paying or in any other ways;

(H) Destroying, removing or modifying information in a cyber source; or compromising its usefulness or effects for any reasons;

(I) Stealing, preventing ability to use, destroying or modifying the source codes from a computer with an intent to destroy it (or) asking someone to do so;

(J) Deceiving through the use of cyber source;

64. Any person who is convicted of creating misinformation and disinformation with the intent of causing public panic, loss of trust or social division on a cyber space, shall be punishable by an imprisonment for a term not exceeding 3 years or a fine not exceeding 100 lakhs or both.

65. Any person who is convicted of creating fake account, website and web portal with the intent of causing public panic, loss of trust or social division on a cyber space, shall be punishable by an imprisonment for a term not exceeding 3 years or a fine not exceeding 100 lakhs or both.

66. Any person who is convicted of providing online financial service without being legally registered in Myanmar shall be punishable by an imprisonment for a term not exceeding 3 years or a fine not exceeding 100 lakhs or both.

67. Any person who is convicted of buying and selling illegal currency such as digital currency, cryptocurrency on cyber space shall be punishable by an imprisonment for a term not exceeding 3 years or a fine not exceeding 100 lakhs or both.

68. Any person who is convicted of electronically sharing and disseminating sexually explicit speech, image, audio file, video, sentence, sign, symbol and other expressions shall be punishable by an imprisonment for a term not exceeding 3 years or a fine not exceeding 100 lakhs or both.

69. Any person who is convicted of creating, collecting, searching, downloading, announcing, promoting, changing or disseminating obscene, inappropriate and explicit child image, audio file, video, words, sign, symbol and other expressions for sexual purposes shall be charged in accord with the Child Rights Law.

70. Any person who is convicted of cyber violence acts such as preventing access to cyber source or making it difficult; attempting to hack into a cyber source without permission; using more than permitted; and inserting or installing dangerous malware with the intent to hurt someone; with an intent to threaten or disturb national sovereignty, security, peace and stability, rule of law and national solidarity, shall be charged with the Anti-violence Law.

71. Any person who commits acts of cyber-attack such as attempts of unauthorized access to and hacking cyber sources which are kept confidential for nationally, internationally or multilaterally implemented security reasons; and using more than permitted; with the intent

of deteriorating the relationship between the country and other foreign countries or for the interests of other foreign country, shall be charged with the Anti-violence Law.

72. The Department, with the approval of Steering Committee, shall take any of the following actions against a violator who is convicted of failure to comply with Section 44 and 48.

(a) Warning;
(b) Sentencing a fine;
(c) Temporary suspension of service provision within Myanmar for a particular term, or temporary suspension of the business license for a particular term;
(d) Banning service provision within Myanmar or revoking the business license.

73. Anyone who is convicted of violating the prohibitions prescribed under the rules, regulations, notifications, orders, instructions, and procedures this law shall be punishable by imprisonment for a term not exceeding one year or a fine not exceeding two hundred and fifty thousand kyats or both.

74. Anyone who attempts or conspires or abets any offences provided by this law, shall be liable to punishments provided by this law.

75. Anyone who commits online gambling without permission shall be charged with the Gambling Law.

Chapter (16)
Appeal

76. Anyone bearing grievances against the rejection of a business license, or rejection of an application for license extension, or an administrative action by the Department can file an appeal to the Central Committee within 30 days from the date on which such order was issued.

77. The Central Committee may validate or amend the decision of the Department related to the appeal submitted in accord with the Section (76) of this law. The decision of the Central Committee shall be conclusive and final.

Chapter (17)
Miscellaneous

78. Existing and ongoing Electronic Identification Permit License (Digital Signature) Services, Online Services and Cyber Security related Services before the enforcement of this law shall register and apply for the license in accordance with this law within one year from the date this law was enacted.

79. Matters not in compliance with the provision of this law are to be adjusted for public interest and in order to be in compliance with the provisions in this law, necessary adjustments are to be completed in the said period mentioned in Section 78.

80. Announcements, Orders and Directives issued relating to the provisions in this law prior to the enactment of this law shall be applicable unless otherwise contradicting to the provision in this law.

81. A member of the central committee or supervision committee or working committee or investigation committee who are not a civil servant while carrying out their activities in this law shall be deemed as such as mentioned in the penal code Section 21.

82. Outstanding fees and fines in this law shall be collected and it cannot be levied in the income tax and considered as outstanding balance.

83. When matters in Section 39, 40 and 41 are carried out by the permission of an existing law, it shall not be deemed as illegal activities.

84. An individual or organization assigned to carry out duties and responsibilities in accordance with this law in good faith shall not be prosecuted.

85. The offenses in this law recognized as cognizable offenses and can be charged by the Myanmar Police Force.

86. Any provision from all existing laws that are not in accord with this law or contrary to this law shall be overruled by the provisions of this law.

87. Should an explanation of any technological terms or technical terms in this law be required, the Ministry can issue a notification to explain such lexicons with the agreement from the State Administration Council.

88. In implementation of this law;

(a) the Ministry, the Ministry of Home Affairs, and the Ministry of Defense can issue rules and regulations with the agreement of the State Administration Council.

(b) the Ministry, the Ministry of Home Affairs, the Ministry of Defence, and related ministries can issue notifications, orders, directives, and procedures.

(c) the Central Committee, the Executive Committee and related working committees can issue notifications, orders, directives, and procedures.

89. The Electronic Transactions Law (State Peace and Development Council Law No. 5/2004) is repealed by this law.

I hereby sign this law in accord with the Constitution of the Union of Myanmar.

Sign:
Chairman, State Administration Council
The Republic of the Union of Myanmar