CONVENIENCE TRANSLATION - ACCURACY NOT GUARANTEED

Republic of the Union of Myanmar
State Administration Council
Cybersecurity Law
(State Administration Council Law No. 1/2025)
1386, 3rd Waxing Day of Pyatho
(1 January 2025)

The State Administration Council hereby enacts this law according to article 419 Constitution of the Republic of the Union of Myanmar.

Chapter 1

Title, commencement and jurisdiction

1. This law shall be known as the Cybersecurity Law.

2. This law shall come into force on the date specified by the president by notification.

3. (a) Any person who commits any of the following offences punishable under this law shall be adjudicated according to this law:

   (1) Offences committed within the country or on board any vessel or aircraft registered under any law in force of the state;

   (2) offences committed within the national cyberspace or in any other cyberspace connected to the national cyberspace.

   (b) Any Myanmar citizen residing abroad who commits an offence punishable under this law shall be adjudicated according to this law.

Chapter 2
Definitions

4. The following expressions shall have the meanings given hereunder:

   (a) "**State**" means the Republic of the Union of Myanmar;

   (b) "**Central Committee**" means the Cybersecurity Central Committee established by the Union Government under this law.

No. 35 (D), Inya Myaing Road, Golden Valley, Bahan Township, Yangon Region
Phone: +95-9-262546284 (English) or +95-9-428372669 (Myanmar)
E-mail: info@lincolnmyanmar.com - Web: www.lincolnmyanmar.com

(c) "**Steering Committee**" means the Cybersecurity Steering Committee established by the Central Committee.

(d) "**Ministry**" means the ministry implementing the matters under this law.

(e) "**Relevant ministry or organisation**" means any Union ministry or Union-level organisation designated by the Union Government as being relevant to cybersecurity matters, including the Ministry of Defense, the Ministry of Home Affairs, and the Central Bank of Myanmar.

(f) "**Department**" means the department to which the Ministry assigned the duty of implementing the matters under this law.

(g) "**Investigation team**" means the team established by the Steering Committee with the consent of the Central Committee to conduct investigations according to the provisions of this law.

(h) "**Cybersecurity**" means the protection of information, cyber resources or electronic information from unauthorised access, disclosure, transmission, distribution, use, interference, modification or destruction, or of critical information infrastructure from unauthorised use, disruption, modification, destruction, and attempts to do so.

(i) "**Cybersecurity services**" means a business that provides cybersecurity services using cyber resources or similar technology and related equipment. This term also includes services determined by the Ministry from time to time.

(j) "**Cybersecurity service provider**" means a person or organisation licensed to provide cybersecurity services within the country.

(k) "**Digital platform services**" means a type of business that provides services that enables users to display, transmit, distribute or use information online using cyber resources or similar technology and related equipment.

(l) "**Digital platform service provider**" means a person or organisation that provides digital platform services that can be used within the country.

(m) "**Information**" means data, a database, sound, text, image, code, sign, signal, video, software or application.

(n) "**Electronic information**" means information created, transmitted, received or stored with electronic technology, including fax and e-mail, electromagnetic wave technology or any other technology.

No. 35 (D), Inya Myaing Road, Golden Valley, Bahan Township, Yangon Region
Phone: +95-9-262546284 (English) or +95-9-428372669 (Myanmar)
E-mail: info@lincolnmyanmar.com - Web: www.lincolnmyanmar.com

(o) "**Data**" means data that can be stored in various formats within a network or computer system.

(p) "**Cyber resources**" means a computer, computer system, computer programme or programme, network, network equipment, databases, or technology that has developed in connection with these elements and related equipment.

(q) "**Computer**" means a device that can be prompted by electronic technology, electromagnetic wave technology or any other technology to gather, store, transmit, process, and (when needed) retrieve and use information, and to use information using mathematical and logical methods.

(r) "**Computer programme or programme**" means a set of instructions or descriptions that refer to data and enable a computer system to perform a specific action during the operation of the computer system.

(s) "**Computer system**" means a system of various devices that can automatically process data using a programme, or a system of devices that consists of interconnected or related devices. This expression also includes a system of any type of removable storage media that is connected to and used with a computer system.

(t) "**Network**" means a set of connections created to interconnect and use, through telecommunication technology, cyber resources or similar technology and related equipment.

(u) "**VPN (virtual private network)**" means a system that is set up as a separate network within the original network using specific technology to ensure security when connecting to a network.

(v) "**Network equipment**" means any item of physical infrastructure used in the execution of network operations, or a combination of such items.

(w) "**Data analysis**" means the process of gathering, analysing and examining any piece of information or part of it for the purpose of cybersecurity using cyber resources or similar technology and related equipment.

(x) "**Malware**" means a malicious code that disrupts or harms cyber resources.

(y) "**Cyberspace**" means an environment where electronic information can be sent, communicated, distributed or received, either within a network or between interconnected networks, using cyber resources or similar technology and related equipment.

No. 35 (D), Inya Myaing Road, Golden Valley, Bahan Township, Yangon Region
Phone: +95-9-262546284 (English) or +95-9-428372669 (Myanmar)
E-mail: info@lincolnmyanmar.com - Web: www.lincolnmyanmar.com

(z) "**Cyberattack**" means any act that uses cyber resources or similar technology and related equipment in cyberspace to harm or damage the administration, finance, economy, law enforcement, national security and public safety of the state and life and property in the state, or to disrupt, distort, suspend or destroy the communication of information in any way.

(*ya*) "**Cybercrime**" means the act of committing, attempting to commit, aiding and abetting, inciting, or acting as an accomplice to any offence under this law or any offence punishable under any law in force, using cyber resources or similar technology and related equipment in cyberspace.

(*la*) "**Cybersecurity threat**" means any attempt to compromise cybersecurity using cyber resources or similar technology and related equipment in cyberspace.

(*wa*) "**Digital laboratory**" means a technology-assisted laboratory that can identify, retrieve, process, analyse and report data stored electronically.

(*tha*) "**Online gambling system**" means a system that uses cyber resources or similar technology and related equipment to enable gambling (whether for a prize or not) in games of chance and games of skill for money, or for something that has monetary value or that has been agreed to be transferred as money.

(ha) "**Cybersecurity group**" means a group that has been permitted by the Steering Committee as prescribed to carry out cybersecurity activities within the country without seeking profit.

Chapter 3
Objectives

5. The objectives of this law are as follows:

(a) Ensuring the safe and secure use of cyber resources, critical information infrastructure and electronic information;

(b) protecting and safeguarding the sovereignty and stability of the state from cybersecurity threats, cyberattacks or cyber abuse using electronic technologies;

(c) systematically developing cybersecurity services;

(d) effectively investigating and prosecuting cybercrimes;

(e) supporting a digital economy based on cyber resources.

No. 35 (D), Inya Myaing Road, Golden Valley, Bahan Township, Yangon Region
Phone: +95-9-262546284 (English) or +95-9-428372669 (Myanmar)
E-mail: info@lincolnmyanmar.com - Web: www.lincolnmyanmar.com

Chapter 4

Establishment, duties and powers of the Central Committee

6. The Union Government:

(a) Shall, to implement the objectives of this law, establish the Cybersecurity Central Committee with the Vice President as its chairperson, the Union minister of the Ministry as its vice chairperson, and Union ministers of relevant ministries and chairpersons of relevant Union-level organisations as its members.

(b) Shall appoint and assign responsibilities to the secretary and joint Secretary when establishing the Central Committee.

(c) May, if necessary, reorganise the Central Committee according to the provisions of subsection (a).

7. The duties and powers of the Central Committee are as follows:

(a) Creating cybersecurity policies, strategies or action plans for the development of a sound and secure national cyberspace in the country;

(b) providing guidance, supervision and coordination to implement cybersecurity policies, strategies or action plans, and to cooperate with countries in the region and elsewhere and with international and regional organisations;

(c) promoting the development of human resources in cybersecurity;

(d) promoting the development of infrastructure necessary for cybersecurity and cybercrime prevention;

(e) providing coordination and guidance between relevant government departments and organisations to support cybersecurity, cybercrime prevention, law enforcement, and justice;

(f) providing guidance to ensure that cybersecurity services for critical information infrastructures are coordinated according to the cybersecurity plan;

(g) determining the storage of information for critical information infrastructure within the national cyber space to which the public connects;

(h) permitting the establishment of a national digital laboratory and digital laboratories as prescribed;

No. 35 (D), Inya Myaing Road, Golden Valley, Bahan Township, Yangon Region
Phone: +95-9-262546284 (English) or +95-9-428372669 (Myanmar)
E-mail: info@lincolnmyanmar.com - Web: www.lincolnmyanmar.com

(i) providing guidance to the relevant ministry or organisation for the issuance, if necessary, of policies, regulations, terms, orders and directives for online financial services;

(j) carrying out cybersecurity-related duties assigned by the Union Government from time to time.

Chapter 5
Establishment, duties and powers of the Steering Committee

8. The Central Committee:

(a) Shall, to carry out and supervise the cybersecurity activities under this law, establish the Steering Committee with the Union minister of the Ministry as chairperson, deputy ministers or permanent secretaries of relevant ministries, deputy chairpersons or permanent secretaries of relevant Union-level organisations, cybersecurity experts, and representatives of non-governmental organisations as members, and the director general of the Department as secretary.

(b) May, if necessary, reorganise the Steering Committee according to the provisions of subsection (a).

(c) allow members of the Steering Committee who are not civil servants to receive allowances and honoraria determined by the Union Government.

9. The duties and powers of the Steering Committee are as follows:

(a) Implementing according to the guidelines the cybersecurity policies, strategies or action plans created by the Central Committee;

(b) conducting human resource development activities related to cybersecurity;

(c) taking steps to ensure that a timely response and protection system is in place in the event of a cyberattack;

(d) coordinating with relevant ministries or organisations to ensure safety of the national cyberspace;

(e) studying and submitting the matter to the Central Committee as to whether the state should participate as a member in conventions, treaties and agreements on cybersecurity or cybercrime.

No. 35 (D), Inya Myaing Road, Golden Valley, Bahan Township, Yangon Region
Phone: +95-9-262546284 (English) or +95-9-428372669 (Myanmar)
E-mail: info@lincolnmyanmar.com - Web: www.lincolnmyanmar.com

(f) implementing and cooperating according to conventions, treaties and agreements on cybersecurity or cybercrime in which the state participates as a member;

(g) cooperating with international organisations, regional organisations and neighbouring countries in relation to information exchange, investigation, and action related to cybersecurity threats, cyberattacks, cyber abuse or cybercrimes;

(h) publishing and announcing information on cybersecurity recommendations to raise public awareness, and reporting, announcing and preventing cyberattacks and cyber threats;

(i) coordinating activities with the cybersecurity incident response teams to protect critical infrastructure;

(j) inspecting, supervising and providing guidance on whether information on critical information infrastructure is stored as prescribed;

(k) permitting the examination of cybersecurity groups, issuing terms that these groups must follow, and taking action against cybersecurity groups established without permission;

(l) determining the license fees, registration fees, fines or other fees to be collected under this law;

(m) establishing policies and standards regarding cyber resources that are manufactured in the country or abroad, installed, or imported from abroad;

(n) when implementing this law, establishing an investigation team and determining its duties and powers with the consent of the Central Committee if an investigation is necessary;

(o) submitting activity reports and other necessary reports to the Central Committee at least once a year;

(p) carrying out cybersecurity-related duties assigned by the Central Committee from time to time.

10. The Steering Committee may, with the consent of the Central Committee, establish and assign duties to the following working committees:

(a) Cybersecurity Working Committee;

(b) Cybercrime Working Committee;

(c) Cyberdefence Working Committee;

No. 35 (D), Inya Myaing Road, Golden Valley, Bahan Township, Yangon Region
Phone: +95-9-262546284 (English) or +95-9-428372669 (Myanmar)
E-mail: info@lincolnmyanmar.com - Web: www.lincolnmyanmar.com

(d) other working committees as necessary.

Chapter 6
Duties and powers of the Department

11. The Department shall be responsible for carrying out office functions as the secretariat team of the Central Committee and the Steering Committee.

12. The Department shall pay the allowances and honoraria of the members of the Steering Committee who are not civil servants.

13. The Department:

(a) May, when implementing international and regional cybersecurity cooperation initiatives, communicate, coordinate and cooperate with international cybersecurity organisations and regional cybersecurity organisations according to the Ministry's guidelines.

(b) May conduct competency tests or competitions in cybersecurity technology and skills according to international standards and issue certificates.

(c) Shall sector-wise implement cybersecurity cooperation activities within the country in accordance with the Ministry's guidelines.

(d) Shall, with the approval of the Ministry, determine the terms for licensing cybersecurity services and the terms for registering digital platform services.

(e) Shall collect as prescribed the license fees, registration fees, fines or other fees to be collected according to this law.

(f) Shall be responsible for implementing the cybersecurity policies, strategies, action plans and guidelines created by the Central Committee.

Chapter 7
Protecting critical information infrastructure

14. The following infrastructures are considered to be critical information infrastructures:

(a) Electronic information infrastructure for national defence and security;

(b) Infrastructure for the electronic government (e-Government) service system;

(c) electronic information infrastructure for finance;

No. 35 (D), Inya Myaing Road, Golden Valley, Bahan Township, Yangon Region
Phone: +95-9-262546284 (English) or +95-9-428372669 (Myanmar)
E-mail: info@lincolnmyanmar.com - Web: www.lincolnmyanmar.com

(d) electronic information infrastructure for transportation;

(e) electronic information infrastructure for telecommunication;

(f) electronic information infrastructure for health;

(g) electronic information infrastructure for electricity and energy;

(h) electronic information infrastructure as determined from time to time by the Central Committee with the consent of the Union Government.

15. The Central Committee shall direct the relevant government departments and government organisations to identify, modify and maintain critical information infrastructures.

16. Relevant government departments and organisations shall act as follows with regard to critical information infrastructure:

(a) Developing cybersecurity plans as prescribed;

(b) establishing cybersecurity incident response teams;

(c) appointing a suitable person as person responsible for the management and maintenance of critical information infrastructure;

(d) submitting a cybersecurity report to the Steering Committee at least once per calendar year.

17. The person responsible for the management and maintenance of critical information infrastructure:

(a) Shall store as prescribed information related to critical information infrastructure based on the level *[of classification]* of the data.

(b) Shall distribute, publish, send, receive and store information related to critical information infrastructure as prescribed.

(c) Shall submit a cybersecurity report on the critical information infrastructure to the Ministry through the relevant government department or government organisation at least once per calendar year.

18. Supervised by the Steering Committee, the Ministry shall supervise and inspect whether the person responsible for the management and maintenance of critical information infrastructure has carried out cybersecurity readiness measures as prescribed.

No. 35 (D), Inya Myaing Road, Golden Valley, Bahan Township, Yangon Region
Phone: +95-9-262546284 (English) or +95-9-428372669 (Myanmar)
E-mail: info@lincolnmyanmar.com - Web: www.lincolnmyanmar.com

Chapter 8
Issuance of licenses and registration

19. The Department may set the cybersecurity service license term and the digital platform registration term from a minimum of 3 years to a maximum of 10 years.

20. A cybersecurity service provider must be a company registered according to the Myanmar Companies Law and shall apply to the Department as prescribed to obtain a business license.

21. The Department shall review the application filed according to section 20 as to whether it is as prescribed and act as follows:

    (a) Shall cause the applicant to pay the license fee and issue the license if the application is as prescribed.

    (b) Shall request the applicant to amend the application or reject the issuance of the license if the application is not as prescribed.

22. If a cybersecurity service provider wishes to continue operating, it must apply as prescribed to the Department for license renewal 6 months prior to the expiration of the license.

23. The Department:

    (a) May review whether the application for license renewal is as prescribed and approve or reject it.

    (b) If the Department rejects the renewal of the license, such rejection shall not affect the remaining term of the license.

24. A digital platform service provider with 100,000 or more users within the country must be a company registered in accordance with the Myanmar Companies Law and shall apply as prescribed to the Department to be allowed registration.

25. The Department shall review the application filed according to section 24 as to whether it is as prescribed and act as follows:

    (a) Shall cause the applicant to pay the registration fee and issue a registration certificate if the application is as prescribed.

No. 35 (D), Inya Myaing Road, Golden Valley, Bahan Township, Yangon Region
Phone: +95-9-262546284 (English) or +95-9-428372669 (Myanmar)
E-mail: info@lincolnmyanmar.com - Web: www.lincolnmyanmar.com

(b) Shall request the applicant to amend the application or reject the issuance of a registration certificate if the application is not as prescribed.

26. If a digital platform service provider wishes to continue operating, it must apply as prescribed to the Department for renewal of the registration period 6 months prior to the expiration of the registration period.

27. The Department:

(a) May review whether the application for renewal of the registration is as prescribed and approve or reject it.

(b) If the Department rejects the renewal of the registration, such rejection shall not affect the remaining term of the registration.

28. A cybersecurity group shall obtain permission from as prescribed the Central Committee to carry out cybersecurity activities within the country without seeking profit.

Chapter 9
Duties of a service provider

29. A cybersecurity service provider shall comply with the following:

(a) Obtaining necessary permits or documentation according to relevant laws for the business or sector in which the cybersecurity service provider wishes to be active;

(b) establishing and implementing cybersecurity prevention plans to assist the Department and the cybersecurity incident response teams;

(c) advising on potential cybersecurity threats and preventive measures;

(d) developing emergency response plans and solutions for malware or cyberattacks;

(e) in the event of a malware or cyberattack, promptly implementing an appropriate emergency response plan, addressing and resolving *[the issue]*, and notifying the relevant stakeholders;

(f) applying cybersecurity technology and necessary international standards;

(g) preventing leakage, damage to, or loss of information of users accessing the service;

(h) immediately notifying the Department if an exceptional cybersecurity incident occurs;

No. 35 (D), Inya Myaing Road, Golden Valley, Bahan Township, Yangon Region
Phone: +95-9-262546284 (English) or +95-9-428372669 (Myanmar)
E-mail: info@lincolnmyanmar.com - Web: www.lincolnmyanmar.com

(i) complying with the terms of the license;

(j) compiling and submitting a cybersecurity work report to the Department as prescribed.

30. A digital platform service provider shall comply with the following:

(a) Obtaining necessary permits or documentation according to relevant laws for the business or sector in which the digital platform service provider wishes to be active;

(b) maintaining the data storage device as prescribed depending on the level *[of classification]* of the data of the user accessing the service;

(c) If the digital platform service provider wishes to conduct any related business or profit-generating business through the digital platform service, it shall do so according to the relevant laws.

(d) complying with the terms in the registration certificate.

31. A digital platform service provider shall have adequate measures in place to identify the relevant information and cyber resource in the event that any of the following occurs on the service platform:

(a) Information occurs that incites hatred, disrupts unity, or disrupts peace and order;

(b) false news or rumors occur;

(c) information is displayed that is not suitable for public viewing;

(d) adisplay of pornographic pictures or pornographic videos, texts or symbols of children that are sexually explicit;

(e) display of information that is contrary to any law in force or performance of an illegal act;

(f) a complaint occurs regarding information intended to cause social or economic harm to an individual;

(g) a complaint occurs regarding the infringement of an intellectual property right;

(h) inciting to commit, committing, attempting, and aiding or abetting acts of terrorism.

32. If a digital platform service provider becomes aware in any way that any of the acts set forth in section 31 occurred or is notified to this effect by the Department, it must prevent, remove, destroy or suspend the act in a timely manner as prescribed.

No. 35 (D), Inya Myaing Road, Golden Valley, Bahan Township, Yangon Region
Phone: +95-9-262546284 (English) or +95-9-428372669 (Myanmar)
E-mail: info@lincolnmyanmar.com - Web: www.lincolnmyanmar.com

33. A digital platform service provider shall retain the following data regarding a user of the service for 3 years:

(a) Personal information of the user accessing the service;

(b) usage records of the user accessing the service;

(c) data specified by the Department from time to time.

34. If a person or organisation authorised under any law in force requests in writing any or all of the data in section 33, the digital platform service provider shall provide it as prescribed.

35. A cybersecurity service provider or digital platform service provider shall cooperate with the relevant working committee in dealing with any cybersecurity threat, cyberattack or cyber abuse incident.

Chapter 10
Cyber abuse

36. Unless otherwise provided in any law in force, any of the following acts, done without permission from the authorised person, to harm a cyber resource or the performance of a computer system is considered cyber abuse:

(a) Altering, modifying or deleting with dishonest intention any computer programme or programme or information, or its condition or quality;

(b) selling a computer programme or programme or information, or moving, transferring or copying it with dishonest intention from its original location to another location, to another cyber resource or to any storage device;

(c) obtaining, operating or using with dishonest intention a computer programme or programme or electronic information;

(d) modifying, adding to, destroying or altering a computer programme or programme or electronic information, or impairing its performance, or altering its original state in any way;

(e) controlling or remotely controlling a computer system, computer programme or programme or electronic information;

(f) analysing with dishonest intention data from a computer programme or programme or information.

No. 35 (D), Inya Myaing Road, Golden Valley, Bahan Township, Yangon Region
Phone: +95-9-262546284 (English) or +95-9-428372669 (Myanmar)
E-mail: info@lincolnmyanmar.com - Web: www.lincolnmyanmar.com

Chapter 11
Detecting cybercrimes and preventing cyberattacks

37. The working committees established by the Steering Committee according to this law shall, under the supervision of the Steering Committee, do the following:

    (a) Preventing cybersecurity threats, cyberattacks or cyber abuse from occurring;

    (b) assisting relevant law enforcement groups in investigating cybercrimes and assessing the risk of cybercrimes;

    (c) taking preventive measures to avoid potential secondary risks from cybersecurity threats, cyberattacks or cyber abuse;

    (d) assessing the likelihood of a cybersecurity threat, cyberattack, or cyber abuse incident occurring and the potential impact if it occurs;

    (e) monitoring and evaluating the strengths and weaknesses of cybersecurity levels in relevant sectors and making recommendations to relevant government departments and organisations to improve cybersecurity;

    (f) identifying, investigating and taking action against cybersecurity threats, cyberattacks or cyber abuse;

    (g) evaluating the services of cybersecurity service providers or digital platform service providers;

    (h) providing technical assistance to the national digital laboratory and digital laboratories.

38. The relevant working committee may as prescribed seize and analyse cyber resources from any of the following individuals who are believed to be implicated in any cybersecurity threat, cyberattack or cyber abuse incident:

    (a) a person who has used or is suspected of having used a cyber resource that is believed to be implied in a cyber security threat, cyberattack or cyber abuse incident;

    (b) a person associated with any person in sub-section (a).

39. The relevant working committee shall, after it analysed the data in the cyber resource and dispatched the cyber resource to a digital laboratory for examination, return the cyber resource as prescribed to the person who provided it.

No. 35 (D), Inya Myaing Road, Golden Valley, Bahan Township, Yangon Region
Phone: +95-9-262546284 (English) or +95-9-428372669 (Myanmar)
E-mail: info@lincolnmyanmar.com - Web: www.lincolnmyanmar.com

40. The Ministry may, with the consent of the Union Government, assign a relevant person or organisation for conducting data analyses and dispatches to a digital laboratory for examination, to identify in advance cyber security threats or cyberattacks in the national cyberspace so that they may be prevented and controlled.

41. The Ministry shall provide support as necessary to companies and organisations providing telecommunications services according to the Telecommunications Law for conducting data analyses and dispatches to a digital laboratory for examination according to section 40.

42. The Ministry may, for national defense and security matters, in the interest of the public, or in consultation with the relevant government department or government organisation pursuant to any law, enter cyber security service businesses or digital platform service businesses to inspect and control them, if necessary.

43. The Ministry may, with the consent of the Union Government, do the following if necessary for the public interest:

    (a) Temporarily suspending digital platform services or electronic information;

    (b) temporarily control of materials related to digital platform services;

    (c) closing digital platform services or declaring them unfit for public use.

44. Anyone wishing to establish a VPN or provide VPN services within the national cyberspace shall obtain permission as prescribed from the Ministry.

Section 12

Seizure of evidence and submission of expert testimony

45. The investigation team may seize as prescribed electronic evidence according to the provisions of this law and any law in force to investigate cybersecurity or cybercrime matters.

46. When investigating a cybercrime, the investigation team may seize as prescribed cyber resources or similar technology and related equipment that are believed to be related to the matter under investigation, and conduct data analyses and dispatches to a digital laboratory for examination.

47. The relevant government department or government organisation may, with the approval of the Central Committee, establish a national digital laboratory or digital laboratories to identify, obtain, process, analyse and report according to the provisions of this law and any law in force on electronic evidence stored electronically.

No. 35 (D), Inya Myaing Road, Golden Valley, Bahan Township, Yangon Region
Phone: +95-9-262546284 (English) or +95-9-428372669 (Myanmar)
E-mail: info@lincolnmyanmar.com - Web: www.lincolnmyanmar.com

48. The Steering Committee shall assist in providing the necessary human resources and technical assistance for the national digital laboratory and the digital laboratories established with the approval of the Central Committee.

49. The investigation team may send electronic evidence stored electronically to the national digital laboratory or a digital laboratory for data discovery, gathering, management and analysis, and submit as prescribed the resulting findings, report and opinion to the Steering Committee or relevant court as expert testimony.

50. (a) If any dispute arises regarding the submission of evidence as an electronic document, the matter shall be sent to the national digital laboratory for examination.

(b) The national digital laboratory's report and opinion on the result of the examination shall be final.

Chapter 13
Administrative action

51. The Department may impose any of the following administrative orders on a cyber security service provider who fails to comply with any provision of section 29 or 35:

(a) Warning;

(b) imposition of a fine;

(c) temporary suspension of the license for a limited period;

(d) revocation of the license.

52. The Department may impose any of the following administrative orders on a digital platform service provider who fails to comply with any provision of section 30, 31, 32, 33, 34 or 35:

(a) Warning;

(b) imposition of a fine;

(c) temporary suspension of the registration certificate for a limited period;

(d) revocation of the registration certificate and blacklisting.

53. The Steering Committee may dissolve a cybersecurity group that was established without permission or that does not comply with the terms, and may confiscate the funds of the group,

No. 35 (D), Inya Myaing Road, Golden Valley, Bahan Township, Yangon Region
Phone: +95-9-262546284 (English) or +95-9-428372669 (Myanmar)
E-mail: info@lincolnmyanmar.com - Web: www.lincolnmyanmar.com

including the money and movable or immovable property owned by the group, as property of the state.

Chapter 14
Appeal

54. Any person dissatisfied with the Department's rejection to issue a license according to section 21, rejection to renew a license according to section 23, rejection to register according to section 25 or rejection to renew a registration according to section 27 may appeal to the Ministry as prescribed within 30 days from the date on which such decision or order was made.

55. Any person dissatisfied with any administrative action taken according to section 51 or 52 may appeal to the Ministry as prescribed within 30 days from the date on which such decision or order was made.

56. The Ministry may confirm, modify or cancel the relevant decision or order in relation to an appeal according to section 54 or 55.

57. Any person dissatisfied with a decision or order made by the Ministry according to section 56 may appeal to the Central Committee as prescribed within 60 days from the date on which such decision or order was made.

58. The Central Committee may confirm, modify or cancel the relevant decision or order in relation to an appeal according to section 57.

59. The decision of the Central Committee is final and conclusive.

Chapter 15
Offences and penalties

60. If a person responsible for the management and maintenance of critical information infrastructure, who is not a civil servant, is convicted of having failed to comply with the provisions of section 17 (a) or (b), he shall be punished with imprisonment for a term of not less than 1 month but not more than 6 months, or to a fine of not less than MMK 1,000,000 but not more than MMK 10,000,000, or with both.

61. Any person convicted of having committed or attempted to commit an act of unauthorised interference, destruction, theft, damage, unlawful transmission, use, distribution, disclosure, modification or alteration of electronic information pertaining to a critical information infrastructure shall be punished with imprisonment for a term of not less than 6 months but not

No. 35 (D), Inya Myaing Road, Golden Valley, Bahan Township, Yangon Region
Phone: +95-9-262546284 (English) or +95-9-428372669 (Myanmar)
E-mail: info@lincolnmyanmar.com - Web: www.lincolnmyanmar.com

more than 3 years, or with a fine of not less than MMK 5,000,000 but not more than MMK 20,000,000, or with both.

62. If any person is convicted of having provided cyber security services without a license:

(a) Such person shall be punished with imprisonment for a term of not less than 1 month but not more than 6 months, or with a fine of not less than MMK 1,000,000 but not more than one MMK 10,000,000, or with both, and the evidence relating to the case shall be confiscated as property of the state.

(b) If the offender is a company or organisation, such company or organisation shall be punished with a fine of not less than MMK 10,000,000, and the evidence relating to the case shall be confiscated as property of the state.

63. Any person convicted of having continued to provide cybersecurity services without renewing his license shall be punished with a fine of not less than MMK 1,000,000 and not more than MMK 5,000,000.

64. If a person operating digital platform services with 100,000 or more users in the country is convicted of having operated without registration, he shall be punished with a fine of at least MMK 100,000,000, and the evidence related to the case shall be confiscated as property of the state.

65. Any person convicted of having continued to operate digital platform services without renewing his registration shall be punished with a fine of not less than MMK 50,000,000.

66. Any person convicted of any of the cyber-abuse offences in section 36 (a), (b), (c) or (d) shall be punished with imprisonment for a term of not less than 6 months but not exceeding2 years, or with a fine of not less than MMK 1,000,000 but not more than MMK 10,000,000, or with both.

67. Any person convicted of any of the cyber-abuse offences in section 36 (e) or (f) shall be punished with imprisonment for a term of not less than 1 year but not more than 3 years, or with a fine of not less than MMK 5,000,000 but not more than MMK 20,000,000, or with both.

68. Any person convicted of having with dishonest intention committed or having with dishonest intention caused another person to commit any of the following acts shall be punished with imprisonment for a term of not less than 1 year and not more than 2 years, or with a fine of not less than MMK 5,000,000 and not more than MMK 20,000,000, or with both:

(a) Performing acts that may damage cyber resources or install malware or cause malware to enter;

No. 35 (D), Inya Myaing Road, Golden Valley, Bahan Township, Yangon Region
Phone: +95-9-262546284 (English) or +95-9-428372669 (Myanmar)
E-mail: info@lincolnmyanmar.com - Web: www.lincolnmyanmar.com

(b) preventing a person authorised to access a cyber resource from accessing the system;

(c) destroying, removing, altering or otherwise impairing the usefulness or effectiveness of information contained in a cyber resource;

(d) stealing, disabling, destroying or altering source code on a computer with the intent of damaging it;

(e) cheating using cyber resources;

(f) electronically creating, modifying or altering information to harm another person or degrade his reputation, or electronically distributing such data;

(g) using a network to send unwanted or unsolicited text messages, e-mails or information.

69. Any person convicted of having with dishonest intention used a cyber resource to steal or destroy any online financial assets of another person, or having with dishonest intention caused another person to do so, shall be punished with imprisonment for a term of not less than 2 years and not more than 7 years, and may also be fined.

70. If any person is convicted of having established a VPN or having provided VPN services without permission from the Ministry:

(a) Such person shall be punished with imprisonment for a term of not less than 1 month but not more than 6 months, or with a fine of not less than MMK 1,000,000 but not more than MMK 10,000,000, or with both, and the evidence relating to the case shall be confiscated as property of the state.

(b) If the offender is a company or organisation, such company or organisation shall be punished with a fine of not less than MMK 10,000,000, and the evidence relating to the case shall be confiscated as property of the state.

71. If any person is convicted of having established an online gambling system without permission:

(a) Such person shall be punished with imprisonment for a term of not less than 6 months but not more than 1 year, or to a fine of not less than MMK 5,000,000 but not more than MMK 20,000,000, or with both, and the property related to the case shall be confiscated as property of the state.

(b) (b) If the offender is a company or organisation, such company or organisation shall be punished with a fine of not less than MMK 20,000,000, and the evidence relating to the case shall be confiscated as property of the state.

No. 35 (D), Inya Myaing Road, Golden Valley, Bahan Township, Yangon Region
Phone: +95-9-262546284 (English) or +95-9-428372669 (Myanmar)
E-mail: info@lincolnmyanmar.com - Web: www.lincolnmyanmar.com

72. Any person convicted of having electronically distributed, transmitted, sent, copied or sold information that is not suitable to be viewed by the public shall be punished with imprisonment for a term of not less than 1 month but not more than 6 months, or with a fine of not less than MMK 1,000,000 but not more than MMK 10,000,000, or with both.

73. If any person is convicted of having violated any of the rules, regulations, terms, notifications, orders, directives and procedures issued under this law:

(a) Such person shall be punished with imprisonment for a term of not less than 1 month but not more than 3 months, or with a fine of not less than MMK 1,000,000 but not more than MMK 10,000, or with both, and the evidence relating to the case shall be confiscated as property of the state.

(b) If the offender is a company or organisation, such company or organisation shall be punished with a fine of not less than MMK 10,000,000, and the evidence relating to the case shall be confiscated as property of the state.

74. Any person convicted of having attempted or conspired to commit any offence under this law, or of having aided and abetted in the commission of an offence under this law shall be subject to the punishment prescribed for that offense under this law.

Chapter 16
Miscellaneous

75. If the evidence relating to an offence prosecuted under this law is difficult to produce before the court, the investigation team may submit to the relevant court a report and documentary evidence on how the evidence has been preserved. Such submission shall be treated as if the evidence had been produced before the court and may be handled by the relevant court according to the law.

76. A cybersecurity group established before this law came into force shall obtain permission within 6 months from the date on which this law comes into force.

77. The Department shall collect the fees and fines due under this law as prescribed as if they were tax arrears.

78. (a) If international cooperation is required in matters under this law, this shall be done according to the Mutual Assistance in Criminal Matters Law.

(b) If the perpetrator of an offense under this law is a foreigner who committed it abroad, the Extradition Law shall be complied with.

No. 35 (D), Inya Myaing Road, Golden Valley, Bahan Township, Yangon Region
Phone: +95-9-262546284 (English) or +95-9-428372669 (Myanmar)
E-mail: info@lincolnmyanmar.com - Web: www.lincolnmyanmar.com

79. If the person responsible for the management and maintenance of critical information infrastructure is a civil servant, and it is found that he has failed to comply with section 17 (a) or (b), action shall be taken against him according to the Civil Services Personnel Law.

80. Any member of the Steering Committee or a working Committee or an investigation team who is not a civil servant shall, while performing duties under this law, be deemed to be a public servant according to section 21 Penal Code.

81. No person or organisation having been assigned responsibilities and duties to act under this law shall be prosecuted for acting in good faith.

82. Prior permission from the Ministry shall be obtained for prosecution under this law.

83. Violations of offences under this law shall be prosecuted under this law only.

84. Offences under sections 60, 62, 64, 66, 68, 71 and 72 are cognizable offences.

85. Administrative action or criminal prosecution under this law shall not be deemed to relieve the person subject to the administrative action or the offender from his liability if he is liable to make good for public losses arising from the matter.

86. The Central Committee or the Steering Committee:

(a) May, with the consent of the Union Government, exempt for the public benefit any government department, government organisation or individual from a permission, license or registration and from the payment of fees that would otherwise be compulsory according to this law.

(b) May, in cases related to a national emergency, to national defense and security or to a natural disaster act on its own and without the prior consent of the Union Government grant an exemption from a permission or license and from the payment of fees that would otherwise be compulsory according to this law.

(c) shall report back to the Union Government the matters according to subsection (b).

87. If the Ministry needs to clarify the meaning of any technical expression or specialised expression in this law, it may, with the approval of the Central Committee, issue a notification to provide such clarification.

88. When implementing the provisions of this law:

No. 35 (D), Inya Myaing Road, Golden Valley, Bahan Township, Yangon Region
Phone: +95-9-262546284 (English) or +95-9-428372669 (Myanmar)
E-mail: info@lincolnmyanmar.com - Web: www.lincolnmyanmar.com

(a) The Ministry may issue rules, regulations and terms with the approval of the Union Government.

(b) The Central Committee, the Steering Committee, the working committees and the Department may issue notifications, orders, directives and procedures.

I hereby sign according to article 419 Constitution of the Republic of the Union of Myanmar.

(Signature) Min Aung Hlaing
Senior General
Chairman
State Administration Council

About Lincoln Legal Services (Myanmar) Limited

Lincoln Legal Services (Myanmar) Limited provides the full range of legal and tax advisory and compliance work required by investors. We pride ourselves in offering result-oriented work, high dependability and a fast response time at very competitive prices. Please do not hesitate to contact us:

Sebastian Pawlita, Managing Director
E-Mail: sebastian@lincolnmyanmar.com

Phone: +95-9-262546284 (English) or +95-9-428372669 (Myanmar)

Office address: No. 35 (D), Inya Myaing Road, Golden Valley, Bahan Township, Yangon Region

Web: www.lincolnmyanmar.com