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

THE State Administration Council hereby enacts this law under Section 419 of the Constitution of the Republic of the Union of Myanmar.

Chapter I

Name, enforcement and judiciary

1. This law shall be called the Cybersecurity Law.

2. This law shall come into force on the date prescribed, by notification, by the President.

3. (a) Every person who commits any offence under the law shall be liable to punishment: -

(1) Offences committed in the country or vehicles and aircraft registered in accord with any existing law of the country

(2) Offences committed within the national cyberspace, or other cyberspaces connecting with national cyberspace

(b) Myanmar citizens residing in foreign countries shall be liable to punishment under this law if they commit any offence under the law.

Chapter II

Definition

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

(a) State means the Republic of the Union of Myanmar.

(b) Central Committee means Central Committee on Cybersecurity formed by the Union Government.

(c) Steering Committee means Steering Committee on Cybersecurity formed by the Central Committee.

(d) Ministry means a ministry that implements the provisions of this law.

(e) Relevant ministries and organizations refer to Union ministries or Union-level organizations deemed by the Union Government to be related to cybersecurity issues, including the Ministry of Defence, Ministry of Home Affairs, and Central Bank of Myanmar.

(f) Department means a department assigned duties by a ministry that implements the provisions of this law.

(g) Investigation Unit refers to a task force established by the Steering Committee with the approval of the Central Committee to conduct investigations.

(h) Cybersecurity refers to the prevention of actions such as destroying, disclosing, accessing, sending, distributing, using, disturbing, transforming, and impeding information, cyber resources, or electronic information without approval. It also includes preventing unauthorized use, disturbance, transformation, and impediment to critical information infrastructures, as well as attempts to do so.

(i) Cybersecurity service means an industry that offers cybersecurity services using cyber resources or similar technology and equipment. The word contains the services recognized by the ministry.

(j) Cybersecurity provider refers to any individual or organization authorized to provide cybersecurity services in the country.

(k) Digital Platform Service is a service that can allow users to express, send, distribute or use data information by using cyber resources and similar systems or equipment.

(l) Digital Platform Service Provider means any individual or any entity providing digital platform services in the country.

(m) Information means data, database, voice, text, image, appearance, code, sign, signal, video, software or application.

(n) Electronic information means information created, sent, received or stored by electronic technology, electromagnetic wave technology or any other specific technology including fax and email.

(o) Data refers to the data which can be stored in various forms in a network or a computer system.

(p) Cyber resources refer to computers, computer systems, software programmes, networks, network utilities, databases, technological advancements and related accessories.

(q) Computer refers to a device capable of acquiring, storing, transmitting, processing, and retrieving information as needed, as well as performing tasks systematically according to mathematical and logical methods by applying electronic technology, electromagnetic wave technology, or other forms of technology.

(r) Computer programme or simply a programme refers to a set of instructions or descriptions that guide a computer system to perform specific tasks or functions during its operation.

(s) A computer system refers to a system of devices that can automatically process and operate data through a programme which comprises a system of a single device or interconnected and related devices that communicate and function together. This term encompasses systems involving storage devices (Removable Storage Medium) used in connection with the computer system for storing data.

(t) A network refers to a collection of connections established to mutually link and utilize cyber resources or related technologies and associated devices through communication technology.

(u) A virtual private network refers to a specific system as a back-up network in the original network with the use of a technology in order to ensure safety of linking networks each other.

(v) A network utility refers to either a physical component of the basic infrastructure used in network operations or the integration of such components.

(w) Data analysis refers to the act of gathering, examining, analyzing, or investigating specific information or data – whether entirely or partially – using cyber resources or similar technology-related tools for the purpose of cybersecurity.

(x) Malware refers to malicious code that disrupts or poses a threat to cyber resources.

(y) A cyberspace refers to exchanging, communicating, distributing or accepting the electronic information with the use of a cyber resource or a similar related technological accessory in a network or among networks.

(z) A cyberattack refers to any act conducted within the cyber domain using cyber resources or related technologies to harm, disrupt, halt or degrade the governance, financial systems, economy, rule of law, national security, public safety, or the lives and property of individuals, aimed at interfering with, distorting, suspending, or damaging information and communication systems in any way.

(aa)Cybercrime refers to committing, attempting to commit, aiding, abetting, or encouraging an offence either specified under this law or punishable under any existing law, using cyber resources or related technologies within the cyber domain.

(bb)Cybersecurity threats refer to actions taken within the cyber domain, using cyber resources or similar technologies and related tools, to compromise cybersecurity in some way.

(cc) A digital forensics laboratory is a technology-assisted lab that enables the discovery, retrieval, management, analysis, and reporting of data stored through electronic systems.

(dd)Online Gambling System refers to a system where various cyber resources or related technologies are used as gambling tools, whether or not they involve betting on chance or skill-based games, involving the use of money, or any valuable item that can be exchanged or agreed upon as having a monetary value, for gambling purposes, whether it is for financial gain or loss, allowing the participation in gambling activities with a mutually agreed-upon value, whether it be in terms of money or something else that holds similar value.

(ee)Cybersecurity team refers to a group authorized by the steering committee to operate without profit for the nation’s cybersecurity activities, in accordance with the guidelines set by the committee.

Chapter III

Objective

5. Objectives of this law are as follows: -

(a) To safely use cyber resources, critical information infrastructure, and electronic data

(b) To protect and safeguard the sovereignty and stability of the nation from being harmed by cyber threats, cyberattacks, or cyber misuse through the application of electronic technologies

(c) To systematically develop cybersecurity services

(d) To effectively investigate and take action against cyber crimes

(e) To contribute to a digital economic system based on cyber resources

Chapter IV

Formation of Central Committee, Responsibilities and Authority

6. The Union government –

(a) shall form the Central Cybersecurity Committee with a Vice-President as Chairperson, the Union Minister of the ministry as Vice-Chairperson, relevant Union Ministers and chairs from relevant Union-level organizations as members to implement the objectives of this law.

(b) shall assign a secretary and a joint secretary at the central committee.

(c) shall amend formation of the central committee in accord with the criteria under Sub-Section (a), if necessary.

7. Responsibilities and authority of the Central Committee are as follows: -

(a) Adopting cybersecurity policies, strategies, or operational plans for the emergence of a secure and robust national cyber domain

(b) Guiding, overseeing, and coordinating the implementation of cybersecurity policies, strategies, or action plans, as well as to facilitate collaboration with international and regional countries and organizations,

(c) Developing human resources concerning cybersecurity

(d) Enhancing necessary infrastructures to prevent cybersecurity breaches and cybercrimes

(e) Coordinating and guiding relevant government departments and organizations in order to contribute to cybersecurity, prevention of cybercrimes, the rule of law and judicial measures

(f) Providing guidance to collaborate on cybersecurity services for critical information infrastructure in accordance with the cybersecurity plan

(g) Defining the storage of information for critical data infrastructure within the national cyber domain that the public is actively engaging with

(h) Allowing establishment and authorization of the National Digital Laboratory and digital laboratories in accordance with the set standards

(i) Providing guidance to the relevant ministry or organization for issuing policies, rules, regulations, orders, or directives related to online payment services as necessary

(j) Carrying out the tasks related to cybersecurity, which are assigned from time to time, by the Union government.

8. The Central Committee

(a) shall form the Steering Committee with the Union Minister from the ministry as Chairperson and deputy ministers or permanent secretaries from relevant ministries, vice-chairpersons from relevant Union-level organizations or permanent secretaries, cybersecurity experts, and representatives from non-governmental organizations as members and the director-general from the department as the secretary in order to carry out and supervise cybersecurity measures mentioned in this law.

(b) shall amend formation of the Steering Committee in accord with the criteria under Sub-Section (a), if necessary.

(c) shall permit allowances and cash awards set by the Union government for Steering Committee members who are not in service.

9. The Responsibilities and Authority of the Steering Committee are as follows: - (a) Implementation of cybersecurity policies, strategies, or action plans set in line with the guidelines adopted by the Central Committee

(b) Carrying out human resources development activities related to cybersecurity

(c) Setting a timely response system if an event of a cyberattack occurs

(d) Coordinating with relevant ministries or organizations to ensure safety of the national cyber arena

(e) Studying and presenting to the central committee whether it is appropriate for the country to participate as a member state in conventions, agreements, and memoranda of understanding related to cybersecurity or cyber incidents.

(f) Implementation and collaboration in accordance with cybersecurity or cybercrime-related conventions, agreements, and memoranda of understanding in which the country participates as a member state

(g) The exchange of information related to cybersecurity threats, cyberattacks, cyber exploitation, or cybercrimes, along with investigations, responses, and actions, in collaboration with international organizations, regional organizations, and neighbouring countries.

(h) Releasing press on cybersecurity recommendations, announcements, and the reporting of cyberattacks, cyber threat incidents, as well as their prevention and early mitigation

(i) Coordinating and collaborating with emergency monitoring and response teams for cybersecurity breaches in critical information infrastructure protection activities

(j) Verification, supervision, and guidance regarding the storage of critical information of the infrastructure in accordance with the standards and criteria

(k) Granting authorization for the cybersecurity team under verification, establishing and issuing regulations that these teams must adhere to, and taking action to verify groups that were formed without permission for cybersecurity matters

(l) Determining the licence fees, registration fees, fines, or other charges to be collected under this law

(m) Formulating policies and setting standards related to cyber resources produced domestically and abroad, installed, or imported from foreign countries

(n) Formation of an investigation team with setting duties and powers in accord with the approval of the Central Committee in carrying out the activities under this law, if an investigation is necessary

(o) Submitting working reports and other necessary reports to the central committee at least once a year

(p) Serving cybersecurity-related tasks as assigned by the Central Committee from time to time

10. The Steering Committee shall form and assign duties to relevant work committees in accord with the approval of the Central Committee as follows: -

(a) Cybersecurity Work Committee

(b) Cybercrime Operation Work Committee

(c) Cyber Protection Work Committee

(d) Other necessary work committees

Chapter VI

Responsibilities and authority of the department

11. The department shall take responsibility for office works as the secretariat of the central committee and the steering committee.

12. The department shall allow expenses and allowances for members of the steering committee who are not in-service.

13. The department

(a) can contact, coordinate and cooperate with international and regional cybersecurity organizations in accord with the directive of the ministry in implementing the cybersecurity cooperation measures internationally and regionally.

(b) can issue recognition certificates by examining qualification of cybersecurity and skills or holding competitions in line with the international standards.

(c) shall initiate sector-wise cybersecurity cooperation in the country under the directive of the ministry.

(d) shall set disciplines for cybersecurity service and registration disciplines for digital platform service in accord with the approval of the ministry.

(e) shall levy licence fees, registration fees, fine or other charges in line with the restrictions under this law.

(f) shall take responsibilities for the implementation of cybersecurity policies, strategies, action plans and work guidelines adopted by the central committee.

Chapter VII

Protection of critical information infrastructure

14. The critical information infrastructures are as follows: -

(a) Electronic information infrastructures for defence and security of the State

(b) e-government service infrastructure

(c) e-financial information infrastructure

(d) e-transport information infrastructure

(e) e-communications information infrastructure

(f) e-health information infrastructure

(g) e-electric power and energy information infrastructure

(h) Electronic information infrastructures set by the Central Committee from time to time in accord with the approval of the Union government

15. The Central Committee shall instruct the relevant government departments and organizations to designate, revise and manage critical information structures to carry out the tasks of planning and maintaining critical information infrastructure.

16. Relevant governments and organizations shall conduct measures for critical information infrastructures as follows: -

(a) Scheming cybersecurity plans under relevant criteria

(b) Formation of an Emergency Cybersecurity Incident Monitoring and Response Team (c) Assigning an appropriate person as an official to manage the critical information infrastructure

(d) submission of a cybersecurity report to the Steering Committee at least once for every calendar year

17. The official who is responsible for managing the critical information infrastructure

(a) shall keep the data related to the critical information infrastructure in accordance with the standards depending on the standards of information.

(b) shall manage publishing, releasing, sending, accepting and storing the data related to critical information infrastructures in accordance with the standards.

(c) shall submit the report of critical information infrastructures to the ministry via relevant government departments and organizations at least once every calendar year.

18. The ministry shall oversee and inspect whether those responsible for managing critical information infrastructure have implemented cybersecurity readiness in accordance with the standards set by the steering committee.

Chapter VIII

Issuance of licence and registration

19. The department can determine the validity period of licences for cybersecurity services and the registration period for digital platform services for a minimum of three years and a maximum of ten years.

20. A cybersecurity service provider must be a company registered under the Myanmar Companies Law and must also apply for a business licence from the relevant department in accordance with the prescribed regulations.

21. The department shall verify applications under the criteria in accord with Section 20 and conduct them as follows: -

(a) if application is aligned with criteria, it needs to issue licence to applicant with paying licence fee

(b) if application is not aligned with criteria, it needs to amend application or refuse to issue licence.

22. The cybersecurity service provider must apply for a licence extension to the relevant authority at least six months before the expiration of the licence if they wish to continue their operations.

23. The department

(a) can allow the application for renewal of licence with verification in accord with the criteria or refuse it.

(b) refuses to extend the licence, it shall not affect the remaining licence term.

24. A digital platform service provider with over 100,000 users within the country must be a registered company under the Myanmar Companies Law, and in line with the registration criteria, an application must be submitted to the relevant department for approval.

25. The department must review the application in accordance with the criteria set forth in Section 24 and proceed as follows: -

(a) issuing the registration to an applicant with payment of registration fee if the application is aligned with relevant criteria

(b) otherwise, it must allow the applicant to amend the application or refuse to issue the registration

26. The digital platform service provider must apply for an extension of the registration before the expiration of the registration term, at least six months in advance, as per the specified conditions, if they wish to continue operating the business.

27. The department –

(a) can verify renewal of registration term in compliance with the relevant criteria and allow or refuse it.

(b) refuse renewal of registration term, it shall not affect the remaining registration term.

28. The cybersecurity team must obtain the approval of the steering committee in line with the criteria, to carry out cybersecurity activities within the country without making a profit.