This draft 'Cyber Law' was prepared by Singapore based consultancy TRPC (TRPC.biz) in January 2019 in response to ToRs provided by the Myanmar's Ministry of Transport and Communications (MoTC) and with World Bank technical assistance. It was discussed at a meeting of ministries and other interested stakeholders on 25 January 2019, which Myanmar Centre for Responsible Business (MCRB) attended, at which there was consistent feedback that the scope of the draft law was too wide, and that it should be divided into individual laws on issues such as Cybercrime, Data Protection etc. It was also pointed out that the E-Commerce provisions should be covered in a unified law, and that Ministry of Commerce was currently preparing this.

Planned public consultations in Q1 2019 were not held, and the WB/TRPC assistance came to an end without further extension.

In 2020 the MoTC developed an internal 'zero draft' 'Cybersecurity Law' which took a different approach to this draft. This zero draft was updated following the assumption of power by the 1 Feb 2021 military government. The new draft was sent to Ministry and business stakeholders in February 2021 with a short deadline for comment.

MCRB has decided to make this January 2019 draft available to improve transparency and address some confusion which has arisen over the origins of the Feb 2021 draft Cybersecurity Law.

Myanmar Cyber Law (Draft)
Pyidaungsu Hluttaw Law No.[ ], 2019)

([], 1380 M.E.])

([], 2019)

Table of Contents

[Note: Table of contents will be populated prior to final version.]

First Draft of the Cyber Law

The Cyber Law is designed to address the objectives set out in the Terms of Reference (Legal Advisory for Elaboration of Cyber Legal and Policy Framework).

There are eight parts in the Cyber Law. Of the eight parts, the key substantive provisions, for the purposes of addressing the items set out in the Terms of Reference, can be found in dedicated parts on E-Government, E-Commerce, Cybersecurity, Data Protection and Cybercrime.

The eight parts, and a summary of the contents of those parts, are as follows:

Part (I): Preliminary

- *Part (I) sets out preliminary matters including the name of the law (The Cyber Law) and the commencement date (the date of notification determined by the President of the Union).*
- *This Part also sets out the definitions used in the Cyber Law, including definitions of "personal data" and "cybersecurity", that align with international good practices.*

Part (II): Objectives

Part (II) sets out the objectives of the Cyber Law, which frames the parts that follow. It summarises the objectives of the Cyber Law, based on the Terms of Reference, as follows:

- *to provide an enabling legislative framework to support the modernisation and development of the nation through information technology;*
- *to enable and support the modernisation and development of electronic government;*
- *to enable and support the modernisation and development of electronic commerce, including by increasing consumer and business trust in electronic commerce;*
- *to lay the legislative foundations for the development and execution of a comprehensive national strategy for cybersecurity;*
- *to lay the legislative foundations for the enhancement of personal data protection by establishing a new Privacy and Data Protection Commission and establishing key principles applicable to the collection, use and processing of personal data, and the cross-border transformation of personal data by electronic means;*
- *to lay the legislative foundations for the enhancement of protections in respect of computer misuse and cybercrime by establishing a Cybercrime Working Committee and setting out legislative and other measures for development to, inter alia, protect the integrity of computer systems and the confidentiality, integrity and availability of data, and, where applicable, to enable alignment with the Budapest Convention; and*
- *to provide the relevant public sector bodies with the necessary statutory authority, powers and responsibilities to give effect to the objectives above and to execute Government policies in relation to matters that are the subject of the Law.*

Part (III): E-Government

Part (III) addresses E-Government, in line with paragraph 6(a) of the Terms of Reference. This Part enables and supports the modernisation and development of electronic government by:

a. *providing the E-Government Steering Committee with a defined statutory remit and clear organisational structure and powers;*
b. *encouraging enhanced productivity, efficiency and effectiveness in public services via the use of technology, online services and electronic information;*
c. *providing for electronic information management governance in the public sector and encouraging the interoperability of information systems and datasets via, inter alia, standardisation and open government data;*
d. *encouraging human resource development in the field of electronic government;*
e. *encouraging enhancements in the security and reliability of electronic government systems;*
f. *addressing related matters in respect of open source software, cloud services, artificial intelligence and intellectual property rights; and*
g. *encouraging the building of appropriate information infrastructure to further these objectives.*

Part (IV): E-Commerce

Part (IV) addresses E-Commerce, in line with paragraph 6(b) of the Terms of Reference. This Part enables and supports the modernisation and development of electronic commerce by:

a. *increasing consumer and business trust in electronic commerce transactions;*
b. *updating certain provisions of the Electronic Transactions Law and the Evidence Act by further aligning the Electronic Transactions Law and the Evidence Act with the UNCITRAL Model Law on Electronic Commerce and the UNCITRAL Model Law on Electronic Signatures in order to encourage the use of electronic transactions, electronic signatures, electronic settlement, paperless trading and online trade as a component part of electronic commerce;*
c. *developing and promoting policy initiatives to facilitate the advancement of electronic commerce;*
d. *protecting the rights and interests of consumers and enhancing market confidence by confirming the basis on which the Consumer Protection Law is applicable to electronic commerce; and*
e. *establishing the roles, functions and powers of the relevant public sector bodies, including the Consumer Protection Central Committee, in executing consumer protection objectives in relation to electronic commerce.*

Provisions relating to the cross-border transfer of information by electronic means (referred to in paragraph 6(b) of the Terms of Reference), while being relevant to e-commerce, are dealt with more comprehensively in Part (VI) on Personal Data Protection.

Part (V): Cybersecurity

Part (V) addresses Cybersecurity, in line with paragraph 6(c) of the Terms of Reference. Certain components of paragraph 6(c) of the Terms of Reference are dealt with in other Chapters of the Cyber Law: namely, "Electronic Authentication and Electronic Signatures" are dealt with under Part (IV) (Electronic Commerce); "exposure to…Cybercrime" is dealt with in Part (VII) (Computer Misuse and Cybercrime); and "Privacy and Data Protection" is dealt with in Part (VI) (Personal Data Protection). Therefore, this Part (V) focuses only on cybersecurity specifically.

This Part lays the legislative foundations for the development and execution of a national strategy for cybersecurity by:

a. *promoting the cybersecurity of networks and information systems in the Republic of the Union of Myanmar;*
b. *specifying the principles and process for the development and execution of the national strategy for cybersecurity;*
c. *providing for the development of comprehensive regulations for the designation of critical information infrastructure;*
d. *providing for the development of comprehensive regulations for the protection of critical information infrastructure; and*
e. *establishing the roles, functions and powers of the relevant public sector bodies (namely ITCSD, National Cyber Security Centre and mmCERT) in executing these objectives.*

Part (VI): Personal Data Protection

Part (VI) addresses privacy and personal data protection, being one of the component items in paragraph 6(c) of the Terms of Reference. This Part lays the legislative foundations for the enhancement of personal data protection by:

a. *establishing a new Personal Data Protection Commission and providing it with appropriate statutory functions and powers;*
b. *introducing appropriate definitions based on international good practices, including a definition of "personal data" designed to encourage an appropriate degree of alignment with GDPR;*
c. *establishing key principles to regulate the processing of personal data based on international good practices, including a series of "Personal Data Protection Principles" designed to encourage an appropriate degree of alignment with GDPR;*
d. *addressing spam control; and*
e. *recognising the right of privacy of individuals with respect to their personal data and the need of organisations to process personal data for purposes that a reasonable person would consider appropriate in the circumstances, including provisions applicable to the cross-border transfer of personal data by electronic means.*

Part (VII): Computer Misuse and Cybercrime

Part (VII) addresses computer misuse and cybercrime, being a component part of paragraph 6(c) of the Terms of Reference.

Part (VII) also takes into account paragraph 9(b) of the Terms of Reference by laying a legislative framework designed to help enable adherence to the Budapest Convention.

Specifically, Part (VII) lays the legislative foundations for the enhancement of protections in respect of computer misuse and cybercrime by:

a. *establishing a Cybercrime Working Committee; and*
b. *setting out legislative and other measures for development to, inter alia, protect the integrity of computer systems and the confidentiality, integrity and availability of data, and, where applicable, to enable alignment with the Budapest Convention.*

Part (VIII): Miscellaneous

This Part will contain legislative boilerplate on matters such as saving and transitional provisions, and other miscellaneous provisions.

The Pyidaungsu Hluttaw hereby enacts the following Law:

PART (I)

PRELIMINARY

Chapter (1)
Citation and Commencement of this Law

1. This Law shall be called the Myanmar Cyber Law.

2. This Law commences on the date determined by the President of the Union in a notification.

Chapter (2)
Definitions

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

   a. **Budapest Convention** means The Convention on Cybercrime of the Council of Europe (CETS No.185);

   b. **cybersecurity** means the state in which a computer or computer system is protected from unauthorised access or attack, and because of that state: (a) the computer or computer system continues to be available and operational; (b) the integrity of the computer or computer system is maintained; and (c) the integrity and confidentiality of information stored in, processed by or transmitted through the computer or computer system is maintained;

   c. **computer** means an electronic, magnetic, optical, electrochemical, or other data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but does not include such device as the Minister may by prescribe by notification;

   d. **computer system** means an arrangement of interconnected computers that is designed to perform one or more specific functions, and includes: (a) an information technology system; and (b) an operational technology system such as an industrial control system, a programmable logic controller, a supervisory control and data acquisition system, or a distributed control system;

   e. **Consumer Protection Law** means the Consumer Protection Law (Pyidaungsu Hluttaw Law No.10/2014) as amended or replaced;

   f. **controller** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data;

g. **Copyright Law** means [*official citation of new copyright law to be inserted once confirmed*] as amended or replaced;

h. **electronic commerce** means a commercial service provided at a distance by electronic means and at the individual request of a recipient of the service. For the purposes of this definition: (a) "at a distance" means that the service is provided without the parties being simultaneously present, (b) "by electronic means" means that the service is sent initially and received at its destination by means of electronic equipment for the processing (including digital compression) and storage of data, and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means, and (c) "at the individual request of a recipient of services" means that the service is provided through the transmission of data on individual request;

i. **essential service** means any service essential to the national security, defence, foreign relations, economy, public health, public safety or public order of the Republic of the Union of Myanmar;

j. **Electronic Transactions Law** means the Electronic Transactions Law (State Peace and Development Council Law No. 5/2004) as amended or replaced;

k. **Evidence Act** means the Evidence Act, 1872 (India Act I, 1872) as amended or replaced;

l. **ITCSD** means the Information Technology and Cyber Security Department of the Ministry of Transport and Communications;

m. **Law** means this law;

n. **personal data** means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

o. **personal data breach** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

p. **processor** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

q. **processing** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

r. **UNCITRAL Model Law on Electronic Commerce** means the UNCITRAL Model Law on Electronic Commerce (1996, with additional article 5 bis as adopted in 1998); and

s. **UNCITRAL Model Law on Electronic Signatures** means the UNCITRAL Model Law on Electronic Signatures (2001).

PART (II)

OBJECTIVES

Chapter (3)
Objectives of the Myanmar Cyber Law

4. The objectives of this Law are as follows:

   a. to provide an enabling legislative framework to support the modernisation and development of the nation through information technology;
   b. to enable and support the modernisation and development of electronic government;
   c. to enable and support the modernisation and development of electronic commerce, including by increasing consumer and business trust in electronic commerce;
   d. to lay the legislative foundations for the development and execution of a comprehensive national strategy for cybersecurity;
   e. to lay the legislative foundations for the enhancement of personal data protection by establishing a new Privacy and Data Protection Commission and establishing key principles applicable to the collection, use and processing of personal data, and the cross-border transformation of personal data by electronic means;
   f. to lay the legislative foundations for the enhancement of protections in respect of computer misuse and cybercrime by establishing a cybercrime working committee and setting out legislative and other measures for development to, inter alia, protect the integrity of computer systems and the confidentiality, integrity and availability of data, and, where applicable, to enable alignment with the Budapest Convention; and
   g. to provide the relevant public sector bodies with the necessary statutory authority, powers and responsibilities to give effect to these objectives and to execute Government policies in relation to matters that are the subject of this Law.

PART (III)

E-GOVERNMENT

Chapter (4)
Objectives of this Part

5. The objective of this Part is to enable and support the modernisation and development of electronic government by:
   a. encouraging enhanced productivity, efficiency and effectiveness in public services via the use of technology, online services and electronic information;
   b. providing for electronic information management governance in the public sector and encouraging the interoperability of information systems and datasets via, inter alia, standardisation and open government data;
   c. encouraging human resource development in the field of electronic government;
   d. encouraging enhancements in the security and reliability of electronic government systems;
   e. addressing related matters in respect of open source software, cloud services, artificial intelligence and intellectual property rights;
   f. encouraging the building of appropriate information infrastructure to further the objectives described in this Part; and
   g. establishing the roles, functions and powers of the relevant public sector bodies in executing these objectives.

Chapter (5)
Role and functions of the E-Government Steering Committee

6. *[This section will incorporate the text of President's Office Notification No. 14/2018 in order to set out the formation, structure and funding of the E-Government Steering Committee within the scope of this Cyber Law.]*

7. The E-Government Steering Committee formed prior to the commencement date of this Law shall remain in office until a new E-Government Steering Committee is formed.

8. The E-Government Steering Committee shall have the following functions:

   a. to act as a lead agency in the public sector in respect of the functions specified in paragraphs b to w;
   b. to develop and execute policies for the successful implementation of electronic government systems;
   c. to provide guidance on prioritised electronic government systems based on best practices of countries having successfully implemented electronic government systems;
   d. to provide guidance on the continuous implementation of the E-Governance Master Plan;
   e. to supervise and support the E-Government Implementation Working Committee in the exercise of its functions in accordance with this Law, including reviewing and, where

applicable, approving projects and budgets submitted by the E-Government Implementation Working Committee;

f. to supervise and support the e-ID Working Committee in the exercise of its functions in accordance with this Law, including reviewing and, where applicable, approving projects and budgets submitted by the e-ID Working Committee;
g. to advise and make recommendations to the Government on public sector needs and policies in relation to technology, online services and electronic information;
h. to ensure the security and reliability of technology and online services in the public sector;
i. to provide, develop, implement or operate, or direct or facilitate the provision, development, implementation, operation or procurement, of technology and online services in the public sector, including, without limitation, encouraging the building of appropriate information infrastructure;
j. to promote the development and use of specific categories of software and services including cloud computing services, open source software and artificial intelligence, where such categories of software and services are conducive to achieving the objectives set out in this Law;
k. to undertake the procurement of technology and online services for public sector bodies, where authorised by the applicable Ministers on behalf of those public sector bodies;
l. to develop measures to prevent duplicative investment in technology and online services in the public sector and improving the interoperability of technology systems and datasets in the public sector via, inter alia, standardisation and open government data, including encouraging public sector bodies to make available, to the maximum extent possible, documents, information and data, in open and machine-readable format, together with metadata;
m. to work with each public sector body to minimise the formulation, receipt, circulation and storage of paper documents by digitising administrative affairs, including, without limitation, formulating plans to continuously reduce paper documents in each public sector body;
n. to provide to the public sector consultancy, project management and other services, manpower and facilities for technology, online services and electronic information;
o. to promote and develop competencies and professional standards in the public sector in relation to technology, online services and electronic information and to promote human resource development in these fields;
p. to take steps to encourage the widest possible range of public services and information to be made available online, in a widely-accessible format, taking into account accessibility for citizens with disabilities, including vision or hearing impairments;
q. to promote or undertake research into and development of matters relating to technology, online services and electronic information in the public sector;
r. to promote and facilitate public and private sector participation in the development of technology, online services and electronic information for the benefit of the nation;
s. to promote and facilitate international cooperation in the development of technology, online services and electronic information in the public sector;
t. to encourage the widespread use of the official ".gov.mm" domain at all times in connection with the performance of public sector functions;
u. to perform such other functions as may be conferred on the E-Government Steering Committee by any other written law or the Union Government;

v. to collaborate, in the performance of its functions, with other public sector bodies that have similar or related functions; and
w. to develop the necessary capabilities to support the delivery of such activities.

9. Nothing in this Chapter imposes on the members of the E-Government Steering Committee, directly or indirectly, any form of duty or liability enforceable by proceedings before any court to which the members of the E-Government Steering Committee would not otherwise be subject.

Chapter (6)
Powers of the E-Government Steering Committee

10. Subject to this Law and any other applicable law, the E-Government Steering Committee has the power to do all things necessary to be done for, or in connection with, the performance of its functions.

11. Without limiting the generality of section 10, the powers of the E-Government Steering Committee include power:

a. to develop and issue codes of practice and guidelines on standards and standardisation applicable to the public sector, including technical, data protection and cybersecurity standards for the public sector in respect of the use of technology, online services and electronic information, leveraging internationally-recognised standards where appropriate;
b. to develop and issue codes of practice and guidelines on data classification for the public sector to facilitate and encourage the adoption of technology, online services and electronic information, leveraging internationally-recognised standards where appropriate;
c. to collaborate with other persons (in or outside of the Republic of the Union of Myanmar), in respect of matters relating to the use of technology, online services and electronic information for the benefit of the public sector;
d. to organise, provide for or collaborate with any person on training programmes, assessments and certifications of, and scholarships for, persons in relation to technology, online services and electronic information for the public sector;
e. to enter into agreements and arrangements for the purposes of performing its functions in accordance with this Law;
f. to execute and manage agreements on behalf of the public sector for the procurement of technology and online services in accordance with its functions in Chapter (5) of this Part;
g. to form or participate in the formation of a body corporate, unincorporated association or trust, or enter into a joint venture with any person in compliance with all applicable procedures;
h. to charge for the provision of goods or services, or the performance of work, by or on behalf of the E-Government Steering Committee in accordance with its functions in Chapter (5) of this Part;
i. to accept grants, gifts, donations or contributions from any source, or raise funds, in each case by all lawful means and in compliance with all applicable procedures;

j. to provide financial support, grant, aid or assistance to any person in connection with any function of the E-Government Steering Committee in compliance with all applicable procedures; and
k. to issue notifications, orders, directives and procedures.

Chapter (7)
Security and reliability of electronic government systems

12. Without limiting sections 9 and 10, but subject to section 13**,** the E-Government Steering Committee has the power:

a. to develop and issue notifications, directives, codes, standards or guidelines for the public sector to enhance the security and reliability of electronic government systems;
b. to carry out, or authorise any person to carry out, an audit of the architecture or use of any technology or online service in the public sector:
    i. for the purpose of assessing any weaknesses or vulnerabilities that may affect the security or reliability of the relevant technology or online service; or
    ii. otherwise upon the request of the relevant public sector body;
c. to report on the results of any audit carried out pursuant to section 12b to the relevant public sector body;
d. to request that the relevant public sector body grant access, or make the necessary arrangements for access to be granted, to the E-Government Steering Committee or any other person authorised by the E-Government Steering Committee in respect of:
    i. any technology, online service, information or document relating to electronic government;
    ii. any premises containing that technology, online service, information or document; and
e. to work with the [ITCSD, the National Cyber Security Centre and mmCERT] to implement such security, mitigation or recovery measures as the E-Government Steering Committee considers necessary to enhance the cybersecurity and reliability of electronic government systems, including, without limitation, to address any weaknesses or vulnerabilities identified:
    i. as part of the audit carried out pursuant to section 12b; and
    ii. as part of a review of technology, information or documents made available pursuant to section 12d.

13. The E-Government Steering Committee's powers under section 12 are subject to any other law that prohibits or restricts the disclosure of information or access to technology or online services.

Chapter (8)
Role and functions of the E-Government Implementation Working Committee

14. *[This section will incorporate the text of President's Office Notification No. 14/2018 in order to set out the formation, structure, functions and funding of the E-Government Implementation Working Committee.]*

15. The E-Government Implementation Working Committee shall operate under the supervision and delegated authority of the E-Government Steering Committee.

Chapter (9)
Role and functions of the e-ID Working Committee

16. *[This section will incorporate the text of E-Government Steering Committee Notification No. 1/2018 in order to set out the formation, structure, functions and funding of the e-ID Working Committee.]*

17. The e-ID Working Committee shall operate under the supervision and delegated authority of the E-Government Steering Committee in accordance with this Law.

Chapter (10)
Responsibilities of other public sector bodies in respect of electronic government

18. Subject to this Law and any other applicable law, all public sector bodies have the responsibility to do all things necessary to be done:

    a. for, and in connection with, the advancement of the objectives set out in this Part, working with the E-Government Steering Committee as the primary responsible agency in accordance with its functions and powers set out in this Part; and
    b. to facilitate the performance by the E-Government Steering Committee, including its sub-committees and working groups, of its roles and functions, and the exercise of its powers, as set out in this Part.

PART (IV)

E-COMMERCE

Chapter (11)
Objectives of this Part

19. The objective of this Part is to enable and support the modernisation and development of electronic commerce by:

    a. increasing consumer and business trust in electronic commerce transactions;
    b. updating certain provisions of the Electronic Transactions Law and the Evidence Act by further aligning the Electronic Transactions Law and the Evidence Act with the UNCITRAL Model Law on Electronic Commerce and the UNCITRAL Model Law on Electronic Signatures, in order to encourage the use of electronic transactions, electronic signatures, electronic settlement, paperless trading and online trade as a component part of electronic commerce;
    c. developing and promoting policy initiatives to facilitate the advancement of electronic commerce;
    d. protecting the rights and interests of consumers and enhancing market confidence by confirming the basis on which the Consumer Protection Law is applicable to electronic commerce; and
    e. establishing the roles, functions and powers of the relevant public sector bodies in executing these objectives.

Chapter (12)
Definitions

20. Unless otherwise defined in this Law, terms used in this Part have the meanings given to them in the Consumer Protection Law, the Electronic Transactions Law and the Evidence Act respectively.

Chapter (13)
Provisions in respect of the Electronic Transactions Law

21. A new section is inserted in Chapter VIII of the Electronic Transactions Law to align with Article 10 of the UNCITRAL Model Law on Electronic Commerce, as follows:

    [Subject to the Ministry's feedback, the new section will provide that a document is deemed to be validly retained if the information in the document is: (a) accessible/usable for subsequent reference; (b) retained in a format in which it was generated, sent or received or is an accurate representation of such information; and (c) retained in a manner which enables the identification of the origin/destination of the electronic record and the date and time when it was sent or received.]

22. A new section is inserted in Chapter VIII of the Electronic Transactions Law to align with Article 18 of the UNCITRAL Model Law on Electronic Commerce, as follows:

[Subject to the Ministry's feedback, the new section will provide that an electronic record would be deemed as "original" if: (a) there exists a reliable assurance as to the integrity of the information from the time when it was first generated in its final form; and (b) where required to be presented, that information is capable of being displayed.]

23. Section 23 of the Electronic Transactions Law is amended to align with Article 4 of the UNCITRAL Model Law on Electronic Commerce, as follows:

[Subject to the Ministry's feedback, this section will provide that the addressee cannot assume that a message is attributable to the sender if the addressee: (a) has received noticed from the originator that the data message is not that of the originator; or (b) knew or should have known that the electronic message was not that of the originator.]

24. Section 25(b) the Electronic Transactions Law is amended to align with Article 14(4)(b) of the UNCITRAL Model Law on Electronic Commerce, as follows:

[Subject to the Ministry's feedback, this section will provide the originator with the express right to treat the message as though it had never been sent (or exercise any other rights it may have), where the originator has not stated that the electronic message is conditional on receipt of acknowledgement but subsequently gives notice to the addressee that no acknowledgement has been received and specifies a reasonable time by which the acknowledgement has been received.]

25. Section 14 of the Electronic Transactions Law is amended to align with Article 9 of the UNCITRAL Model Law on Electronic Signatures, as follows:

[Subject to the Ministry's feedback, this section will align with the obligations of the certification authority set out in Article 9 of the UNCITRAL Model Law on e-Signatures. At present, only s 14(ii) of the Electronic Transaction Law corresponds with Art 9(a) of the UNCITRAL Model Law on Electronic Signatures.]

26. Chapter VI of the Electronic Transactions Law is amended to align with Articles 12(2) and 12(3) of the UNCITRAL Model Law on Electronic Signatures, as follows:

[Subject to the Ministry's feedback, this section will provide that electronic signatures and/or electronic signature certificates created/issued outside Myanmar should have the same legal effect within Myanmar if it offers a substantially equivalent level of reliability. At the moment, recognition of foreign certification authorities is only granted on a case-by-case basis by the Electronic Transactions Control Board.]

Chapter (14)
Provisions in respect of the Evidence Act

27. Section 67a of the Evidence Act is amended to incorporate the test for reliability set out in Article 6(3) of the UNCITRAL Model Law on Electronic Signatures, as follows:

[This section will include a provision which deems an electronic signature to be "reliable" where: (a) the electronic signature is unique to the person using it; (b) the electronic

signature is created in a manner or using means under the sole control of the person using it; (c) alterations to the electronic signature is detectable; and (d) where the purpose of the legal requirement for a signature is to provide assurance as to the integrity of the information to which it relates, any alteration made to that information after the time of signing is detectable.]

Chapter (15)
Formation of the E-Commerce Steering Committee

28. The Union Government shall establish the E-Commerce Steering Committee.

29. *[To be discussed which ministry shall be the lead ministry – Ministry of Commerce?].*

30. *[Formation, structure and funding of the E-Commerce Steering Committee to be discussed and set out here.]*

Chapter (16)
Role and functions of the E-Commerce Steering Committee

31. The E-Commerce Steering Committee shall have primary responsibility for developing and promoting policy initiatives for the advancement of electronic commerce. For these purposes, the E-Commerce Steering Committee shall have the following functions:

    a. to act as the lead agency in the public sector in respect of the functions specified in paragraphs b to j;
    b. to develop and execute policies for the promotion of electronic commerce and related industry infrastructure;
    c. to provide guidance on electronic commerce based on international norms relevant to electronic commerce;
    d. to develop measures to ensure the safety and reliability of electronic commerce;
    e. to provide, develop, standardise, implement or operate, or direct or facilitate the provision, development, standardisation, implementation or operation of technologies relevant to electronic commerce;
    f. to support the Consumer Protection Central Committee in the exercise of its functions in relation to the application of the Consumer Protection Law to electronic commerce pursuant to the Consumer Protection Law and section 36 of this Law;
    g. to promote and undertake research into barriers to the adoption of electronic commerce;
    h. to minimise barriers to the adoption of electronic commerce;
    i. to collaborate, in the performance of its functions, with other public sector bodies that have similar or related functions; and
    j. to develop the necessary capabilities to support the delivery of such activities.

32. Nothing in this Part imposes on the members of the E-Commerce Steering Committee, directly or indirectly, any form of duty or liability enforceable by proceedings before any court to which the members of the E-Commerce Steering Committee would not otherwise be subject.

Chapter (17)

Powers of the E-Commerce Steering Committee

33. Subject to this Law and any other applicable law, the E-Commerce Steering Committee has the power to do all things necessary to be done for, or in connection with, the performance of its functions.

34. Without limiting the generality of section 33, the powers of the E-Commerce Steering Committee include power:

    a. to develop and issue codes of practice, guidelines and standards applicable to electronic commerce in accordance with Chapter 16;
    b. to work with any public sector body to minimise barriers to the adoption of electronic commerce;
    c. to collaborate with other persons (in or outside of the Republic of the Union of Myanmar) in respect of the advancement of electronic commerce;
    d. to organise, provide for or collaborate with any person on training programmes, assessments and certifications of, and scholarships for, persons in relation to the advancement of electronic commerce;
    e. to enter into agreements and arrangements for the purposes of performing its functions in accordance with this Law;
    f. to form or participate in the formation of a body corporate, unincorporated association or trust, or enter into a joint venture with any person in compliance with all applicable procedures;
    g. to accept grants, gifts, donations or contributions from any source, or raise funds, in each case by all lawful means and in compliance with all applicable procedures;
    h. to provide financial support, grant, aid or assistance to any person in connection with any function of the E-Commerce Steering Committee in compliance with all applicable procedures; and
    i. to issue notifications, orders, directives and procedures.

Chapter (18)
Application of the Consumer Protection Law to electronic commerce

35. The provisions of the Consumer Protection Law are applicable to electronic commerce and shall be construed and interpreted accordingly.

36. Without limiting the generality of section 35, the following principles shall be applicable to electronic commerce specifically, and the relevant provisions of the Consumer Protection Law shall be construed and interpreted accordingly:

    a. entrepreneurs shall, prior to a consumer completing a transaction via electronic commerce, provide the consumer with all information reasonably necessary, in a clear, comprehensible and intelligible manner, for the consumer to understand:
        i. their rights under the Consumer Protection Law;
        ii. the total amount payable by the consumer for the applicable products or services, inclusive of all applicable taxes, delivery charges, processing fees and other applicable amounts, in a manner that enables the consumer to understand the total amount payable;

iii. the technical steps necessary for the consumer to complete the relevant transaction via electronic commerce;
iv. the process for the consumer to return the applicable products or reject the applicable services to the extent that the consumer has the right to do so under the Consumer Protection Law; and
v. the existence of a complaints procedure (if any), including contact details to facilitate communications by the consumer to the entrepreneur in respect of the consumer's rights under the Consumer Protection Law;

b. unless the parties have agreed other terms in relation to delivery, the entrepreneur shall deliver goods that are the subject of the electronic commerce transaction by transferring the physical possession or control of the goods to the consumer without undue delay; and
c. entrepreneurs and consumers shall comply with such additional regulations in relation to electronic commerce as are developed by the Consumer Protection Central Committee in accordance with Chapter (20) of this Part.

Chapter (19)
Functions and responsibilities of the Consumer Protection Central Committee in relation to electronic commerce

37. The Consumer Protection Central Committee shall have primary responsibility for the application of the Consumer Law to electronic commerce.

38. In relation to electronic commerce, the Consumer Protection Central Committee shall have all of the functions and responsibilities applicable to it under the Consumer Protection Law. In addition, the Consumer Protection Central Committee shall have the following functions and responsibilities:

a. to act as the lead agency in the public sector in respect of the functions specified in paragraphs b to f;
b. to develop and specify policies to enhance consumer protection in relation to electronic commerce;
c. to promote and undertake research into matters of consumer protection in relation to electronic commerce;
d. to consult with the private sector and consumer groups in relation to measures that may give effect to the enhancement of consumer protection in relation to electronic commerce, including appropriate voluntary measures and self-regulatory frameworks;
e. to supervise and support the Consumer Dispute Settlement Bodies in relation to the exercise of their functions in relation to electronic commerce matters pursuant to the Consumer Protection Law and section 44 of this Law; and
f. to develop the necessary capabilities to support the delivery of such activities.

39. Nothing in this Part imposes on the members of the Consumer Protection Central Committee and the members of the E-Commerce Steering Committee, directly or indirectly, any form of duty or liability enforceable by proceedings before any court to which the members of the Consumer Protection Central Committee or the members of the E-Commerce Steering Committee would not otherwise be subject.

Chapter (20)
Development of comprehensive consumer protection regulations in relation to electronic commerce

40. The Consumer Protection Central Committee shall, within [twelve (12) months] of the date of this Law, introduce comprehensive regulations to enhance consumer protections in relation to electronic commerce, including:

    a. comprehensive details of the nature and format of information to be provided by entrepreneurs to consumers in relation to electronic commerce transactions;
    b. a mandatory right of withdrawal for consumers in relation to identified categories of electronic commerce transactions;
    c. obligations of entrepreneurs in relation to exercise by consumers of their rights under the regulations; and
    d. effective, proportionate and dissuasive sanctions or measures for non-compliance.

41. If any provision in the regulations to be developed pursuant to section 40 is inconsistent with this Law or the Consumer Protection Law, such provision, to the extent of the inconsistency, does not have effect.

Chapter (21)
Powers of the Consumer Protection Central Committee in respect of electronic commerce

42. Subject to this Law, the Consumer Protection Law and any other applicable law, the Consumer Protection Central Committee has the power to do all things necessary to be done for, or in connection with, the performance of its functions as they relate to electronic commerce.

43. Without limiting the generality of section 42, the powers of the Consumer Protection Central Committee in relation to electronic commerce include the power to develop, issue and enforce the regulations to be developed by it pursuant to section 40 of this Law through notifications, orders, directives and procedures.

Chapter (22)
Functions and responsibilities of the Consumer Dispute Settlement Bodies in relation to electronic commerce

44. In relation to electronic commerce, the Consumer Dispute Settlement Bodies shall have all of the functions and responsibilities applicable to them under the Consumer Protection Law. In addition, the Consumer Dispute Settlement Bodies shall be responsible for developing the necessary capabilities to support the investigation and enforcement of the Consumer Protection Law, and the regulations to be developed pursuant to section 40 of this Law, in the context of electronic commerce.

45. Nothing in this Part imposes on the members of the Consumer Protection Dispute Settlement Bodies, directly or indirectly, any form of duty or liability enforceable by proceedings before any court to which the members of the Consumer Protection Dispute Settlement Bodies would not otherwise be subject.

Chapter (23)
Powers of the Consumer Dispute Settlement Bodies in relation to electronic commerce

46. Subject to this Law, the Consumer Protection Law and any other applicable law, the Consumer Dispute Settlement Bodies have the power to do all things necessary to be done for, or in connection with, the performance of their functions as they relate to electronic commerce.

Chapter (24)
Advisory Committees

48. The Consumer Protection Central Committee may appoint one or more advisory committees to provide advice to the Consumer Protection Central Committee with regard to electronic commerce in connection with the performance of any of its functions under this Part.

49. The Consumer Protection Central Committee may consult such advisory committees in relation to the performance of its functions and duties and the exercise of its powers under this Part but shall not be bound by such consultation.

Chapter (25)
Ability of entrepreneurs to offer additional contractual protections

50. Nothing in this Part or the Consumer Protection Law shall prevent entrepreneurs from offering to consumers contractual arrangements in relation to electronic commerce which go beyond the protection provided for in this Part and the Consumer Protection Law.

Chapter (26)
Effect of this Part on national general contract law

51. This Part shall not affect national general contract law such as the rules on the validity, formation or effect of a contract.

Chapter (27)
Responsibilities of other public sector bodies in respect of electronic commerce

52. Subject to this Law and any other applicable law, all public sector bodies have the responsibility to do all things necessary to be done to facilitate the performance by the E-Commerce Steering Committee and the Consumer Protection Central Committee of its roles and functions, and the exercise of its powers, as set out in this Part.

PART (V)

CYBERSECURITY

Chapter (28)
Objectives of this Part

53. The objective of this Part is to lay the legislative foundations for the development and execution of a national strategy for cybersecurity by:

    a. promoting the cybersecurity of networks and information systems in the Republic of the Union of Myanmar;
    b. specifying the principles and process for the development and execution of the national strategy for cybersecurity;
    c. providing for the development of comprehensive regulations for the designation of critical information infrastructure;
    d. providing for the development of comprehensive regulations for the protection of critical information infrastructure; and
    e. establishing the roles, functions and powers of the relevant public sector bodies in executing these objectives.

Chapter (29)
Role and functions of the ITCSD

54. The ITCSD *[to be discussed with the Ministry – alternatively, one could replace "ITCSD" with "Ministry of Transport and Communications" throughout this Part]* shall have primary responsibility for the execution of the objectives set out in this Part. For these purposes, the ITCSD shall have the following functions:

    a. to act as lead agency in the public sector in respect of the functions specified in paragraphs b to r;
    b. to develop and execute a comprehensive national strategy for cybersecurity in accordance with Chapter (30) of this Part;
    c. to oversee and promote the cybersecurity of networks and information systems in the Republic of the Union of Myanmar;
    d. to advise and make recommendations to the Government on national needs and policies in relation to cybersecurity;
    e. to identify and designate critical information infrastructure in accordance with regulations to be developed pursuant to Chapter (31) of this Part;
    f. to regulate owners of critical information infrastructure with regard to the cybersecurity of the critical information infrastructure in accordance with regulations to be developed pursuant to Chapter (32) of this Part;
    g. to monitor exposure to cybersecurity threats, whether such cybersecurity threats occur in or outside the Republic of the Union of Myanmar;
    h. to manage the response to cybersecurity incidents that threaten the national security, defence, economy, foreign relations, public health, public order or public safety, or any essential services, of the Republic of the Union of Myanmar, whether such cybersecurity incidents occur in or outside the Republic of the Union of Myanmar;

i. to establish cybersecurity codes of practice and standards of performance for implementation by owners of critical information infrastructure;
j. to represent the Government on cybersecurity issues internationally;
k. to cooperate with computer emergency response teams (CERTs) of other countries or territories on cybersecurity incidents;
l. to promote, develop, maintain and improve competencies and professional standards of persons working in the field of cybersecurity, including human resource development in this field;
m. to support the advancement of technology, and research and development relating to cybersecurity;
n. to promote awareness of the need for and the importance of cybersecurity in the Republic of the Union of Myanmar;
o. to supervise and support the National Cyber Security Centre and mmCERT, including reviewing and, where applicable, approving projects and budgets submitted by the National Cyber Security Centre and mmCERT;
p. to collaborate, in the performance of its functions, with other public sector bodies that have similar or related functions, including, in relation to cybersecurity in the public sector, the E-Government Steering Committee;
q. to perform such other functions and discharge such other duties as may be conferred on the ITCSD under any other written law; and
r. to develop the necessary capabilities to support the delivery of such activities.

55. Nothing in this Part imposes on the public officers of the ITCSD, directly or indirectly, any form of duty or liability enforceable by proceedings before any court to which the public officers of the ITCSD would not otherwise be subject.

Chapter (30)
Development of a comprehensive national strategy for cybersecurity

56. The ITCSD shall, within [twelve (12) months] of the date of this Law, introduce a comprehensive national strategy to enhance cybersecurity, designed to address the objectives set out in this Part.

Chapter (31)
Development of comprehensive regulations for the designation of critical information infrastructure

57. The ITCSD shall, within [twelve (12) months] of the date of this Law, introduce comprehensive regulations for the designation of critical information infrastructure.

58. The regulations to be developed by the ITCSD pursuant to section 57 shall:

a. include a comprehensive definition of "critical information infrastructure", which shall be based on the principle that a computer or computer system may only constitute "critical information infrastructure" if:
    i. it is necessary for the continuous delivery of an essential service, and the loss or compromise of the computer or computer system would have a debilitating

effect on the availability of the essential service in the Republic of the Union of Myanmar; and

ii. the computer or computer system is located wholly or partly in the Republic of the Union of Myanmar;

b. set out a process by which the ITCSD may issue a written notice to the owner of a computer or computer system in order to designate that computer or computer system as a critical information infrastructure;

c. provide for a procedure under which the designated owner of a critical information infrastructure under section 58b may appeal against the designation;

d. specify the time period pursuant to which a designation under section 58b applies which, in any event, shall not exceed five (5) years from the date of the designation; and

e. specify a process for the withdrawal of a designation by the ITCSD under section 58b.

59. If any provision in the regulations to be developed pursuant to section 57 is inconsistent with this Law, such provision, to the extent of the inconsistency, does not have effect.

Chapter (32)
Development of comprehensive regulations for the protection of critical information infrastructure

60. The ITCSD shall, within [twelve (12) months] of the date of this Law, introduce comprehensive regulations for the protection of critical information infrastructure in accordance with this Law through orders or directives *[with the approval of the Ministry of Transport and Communications]*.

61. The regulations to be developed by the ITCSD pursuant to section 60 shall:

a. set out the technical or other standards relating to cybersecurity to be maintained in respect of a critical information infrastructure in accordance with this Part;

b. specify measures to be taken by designated owners of critical information infrastructure to ensure the cybersecurity of the critical information infrastructure in accordance with this Part, in particular, obligations for owners of critical information infrastructure to:

i. notify the [National Cyber Security Centre / mmCERT / ITCSD] of the occurrence of defined categories of cybersecurity incidents in respect of: (A) critical information infrastructure, or (B) any computer or computer system under the owner's control that is interconnected with or communicates with the critical information infrastructure;

ii. establish such mechanisms and processes for the purposes of detecting cybersecurity threats and incidents in respect of the critical information infrastructure as set out in any applicable code of practice issued by ITCSD in accordance with this Part;

iii. perform or have performed a cybersecurity audit and cybersecurity risk assessment in respect of the critical information infrastructure at a frequency to be specified in the regulations, and for the owner of the critical information infrastructure to provide copies of the audit and risk assessment to the [National Cyber Security Centre / mmCERT / ITCSD] within a reasonable timeframe to be specified in the regulations;

iv. take such reasonable and proportionate security, mitigation or recovery measures as are necessary to enhance the cybersecurity of the critical information infrastructure, including, without limitation, to address any weaknesses or vulnerabilities as part of the audit and/or risk assessment carried out pursuant to section 61a.iii; and

v. participate in notified cybersecurity exercises led by the [National Cyber Security Centre / mmCERT] for the purpose of enabling the [National Cyber Security Centre / mmCERT] to test the state of readiness of owners of different critical information infrastructure in responding to significant cybersecurity incidents;

c. contain measures and safeguards to protect the confidentiality of information, and the privacy of personal data, to which any person may have access in the performance of his functions or the exercise of his duties under the regulations; and

d. specify effective, proportionate and dissuasive sanctions or measures, including monetary sanctions, for non-compliance.

62. If any provision in the regulations to be developed pursuant to section 60 is inconsistent with this Law, such provision, to the extent of the inconsistency, does not have effect.

Chapter (33)
Powers of the ITCSD

63. Subject to this Law and any other applicable law, the ITCSD has the power to do all things necessary to be done for, or in connection with, the performance of its functions.

64. Without limiting the generality of section 63, the powers of the ITCSD include power:

a. to develop, issue and enforce the regulations to be developed by it pursuant to Chapters (31) and (32) of this Part;

b. to develop and issue codes of practice, guidelines and standards applicable to cybersecurity in accordance with this Part;

c. to collaborate with other persons (in or outside of the Republic of the Union of Myanmar) in respect of cybersecurity matters;

d. to organise, provide for or collaborate with any person on training programmes, assessments and certifications of, and scholarships for, persons in relation to cybersecurity;

e. to enter into agreements and arrangements for the purposes of performing its functions in accordance with this Law;

f. to form or participate in the formation of a body corporate, unincorporated association or trust, or enter into a joint venture with any person in compliance with all applicable procedures;

g. to accept grants, gifts, donations or contributions from any source, or raise funds, in each case by all lawful means and in compliance with all applicable procedures; and

h. to provide financial support, grant, aid or assistance to any person in connection with any function of the ITCSD in compliance with all applicable procedures.

65. The ITCSD shall ensure that the establishment, implementation and application of the powers provided for in this Part provide for the adequate protection of human rights and

liberties and shall incorporate the principle of proportionality. Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, inter alia, include grounds justifying application, and limitation of the scope and the duration of such power or procedure. To the extent that it is consistent with the public interest, in particular the sound administration of justice, the ITCSD shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.

Chapter (34)
Advisory Committees

67. The ITCSD may appoint one or more advisory committees to provide advice to the ITCSD with regard to the performance of any of its functions under this Part.

68. The ITCSD may consult such advisory committees in relation to the performance of its functions and duties and the exercise of its powers under this Part but shall not be bound by such consultation.

Chapter (35)
Functions and responsibilities of the National Cyber Security Centre

69. *[To be discussed whether this is sufficiently covered by the sections above (in relation to ITCSD) or whether a separate and defined remit for NCSC needs to be provided for.]*

Chapter (36)
Functions and responsibilities of mmCERT

70. *[To be discussed whether this is sufficiently covered by the sections above (in relation to ITCSD) or whether a separate and defined remit for mmCERT needs to be provided for. This could potentially include:*
    a. *Monitoring of incidents at a national level;*
    b. *Providing early warning, alerts, announcements and dissemination of information to relevant stakeholders about risks and incidents;*
    c. *Responding to incidents;*
    d. *Providing dynamic risk and incident analysis and situational awareness;*
    e. *Participating in a network of CERTs;*
    f. *Establishing cooperation arrangements with the private sector; and*
    g. *Promoting the adoption and use of common or standardised practices for incident and risk handling procedures and incident, risk and information classification schemes.]*

Chapter (37)
Responsibilities of other public sector bodies in respect of cybersecurity

71. Subject to this Law and any other applicable law, all public sector bodies have the responsibility to do all things necessary to be done to facilitate the performance by the ITCSD of its roles and functions, and the exercise of its powers, as set out in this Part.

PART (VI)

PERSONAL DATA PROTECTION

Chapter (38)
Objectives of this Part

72. The objective of this Part is to lay the legislative foundations for the enhancement of personal data protection by:
    a. establishing a new Personal Data Protection Commission and providing it with appropriate statutory functions and powers; and
    b. establishing key principles to regulate the processing of personal data in a manner that recognises the right of privacy of individuals with respect to their personal data and the need of organisations to process personal data for purposes that a reasonable person would consider appropriate in the circumstances, including provisions applicable to the cross-border transfer of personal data by electronic means.

Chapter (39)
Formation of the Personal Data Protection Commission

73. The Union Government shall establish the Personal Data Protection Commission.

74. *[To be discussed which ministry shall be the lead ministry – Ministry of Transport and Communications?]*

75. [*Formation, structure and funding of the Personal Data Protection Commission to be discussed and set out here.]*

Chapter (40)
Role and functions of the Personal Data Protection Commission

76. The Personal Data Protection Commission shall have primary responsibility for the execution of the objectives set out in this Part. For these purposes, the Personal Data Protection Commission shall have the following functions:

    a. to act as the lead agency in the public sector in respect of the functions specified in paragraphs b to n;
    b. to promote awareness of personal data protection in the Republic of the Union of Myanmar;
    c. to provide consultancy, advisory, technical, managerial or other specialist services relating to personal data protection;
    d. to work with and advise the Government and any other public sector body, including the [E-Government Steering Committee and the Ministry of Home Affairs], on national needs and policies in respect of personal data protection;
    e. to conduct research and studies on technical standards for the protection of personal data, including international best practices with applicability to the Republic of the Union of Myanmar;

f. to conduct research and studies and promote educational activities relating to personal data protection, including organising and conducting seminars and workshops relating to such activities, and supporting other organisations conducting such activities;
g. to manage technical co-operation and exchange in the area of personal data protection with other organisations, including foreign data protection authorities and international or inter-governmental organisations;
h. to develop and enforce comprehensive regulations for the enhancement of personal data protection in accordance with Chapter (41) of this Part;
i. to manage personal data breach incident reporting;
j. to consult with the private sector and consumer groups in relation to regulations and other measures that give effect to the objectives set out in this Part, including appropriate voluntary measures and self-regulatory frameworks where applicable;
k. to conduct research and studies on ethical frameworks for the processing of personal data in connection with new technologies, including artificial intelligence;
l. to represent the Government internationally on matters relating to personal data protection;
m. to carry out functions conferred on the Personal Data Protection Commission under any other written law; and
n. to develop the necessary capabilities to support the performance of these functions.

Chapter (41)
Development of comprehensive regulations for the protection of personal data

77. The Personal Data Protection Commission shall, within twelve (12) months of the date of this Law, introduce comprehensive regulations for the protection of personal data in accordance with this Law through notifications, orders, directives or procedures.

78. The regulations to be developed by the Personal Data Protection Commission pursuant to section 77 shall:

a. incorporate the definitions of "personal data", "controller", "processor", "data subject" and "processing" under this Law;
b. be aligned with, and elaborate on, the principles set out in Chapter (42) of this Part (such principles to be known as the "Personal Data Protection Principles");
c. to provide for appropriate and proportionate rights of data subjects;
d. impose appropriate and proportionate obligations on organisations to report specified categories of personal data breach incidents;
e. regulate the sending of unsolicited commercial electronic messages by organisations;
f. require controllers to be primarily responsible for, and able to demonstrate compliance with, paragraphs b to e of this section;
g. impose appropriate and proportionate obligations on processors; and
h. specify effective, proportionate and dissuasive sanctions or measures for non-compliance.

79. If any provision in the regulations to be developed pursuant to section 77 is inconsistent with this Law (including the Personal Data Protection Principles), such provision, to the extent of the inconsistency, does not have effect.

Chapter (42)
Personal data protection principles

80. The Personal Data Protection Principles referred to in section 78.b are as follows:

a. personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject;
b. personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
c. personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
d. personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
e. personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;
f. personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures; and
g. personal data may be transferred outside of the Republic of the Union of Myanmar provided that the organisation takes reasonable steps to ensure that the personal data transferred will be subject to a standard of protection that is comparable to those required by these Personal Data Protection Principles.

81. The following provisions shall be applicable in determining an organisation's responsibilities in connection with the Personal Data Protection Principles:
a. an organisation shall be responsible for personal data in its possession or under its control; and
b. an organisation shall be required to consider what a reasonable person would consider appropriate in the circumstances.

Chapter (43)
Powers of the Personal Data Protection Commission

82. Subject to this Law and any other applicable law, the Personal Data Protection Commission has the power to do all things necessary to be done for, or in connection with, the performance of its functions.

83. Without limiting the generality of section 82, the powers of the Personal Data Protection Commission include power:

a. to develop, issue and enforce the regulations to be developed by it pursuant to Chapter (41) of this Part;
b. to develop and issue codes of practice, guidelines and standards applicable to personal data protection in accordance with this Part;
c. to collaborate with other persons (in or outside the Republic of the Union of Myanmar), in respect of personal data protection matters;

d. to organise, provide for or collaborate with any person on training programmes, assessments and certifications of, and scholarships for, persons in relation to personal data protection;
e. to enter into agreements and arrangements for the purposes of performing its functions in accordance with this Law;
f. to form or participate in the formation of a body corporate, unincorporated association or trust, or enter into a joint venture with any person in compliance with all applicable procedures;
g. to accept grants, gifts, donations or contributions from any source, or raise funds, in each case by all lawful means and in compliance with all applicable procedures; and
h. to provide financial support, grant, aid or assistance to any person in connection with any function of the Personal Data Protection Commission in compliance with all applicable procedures.

Chapter (44)
Advisory Committees

85. The Personal Data Protection Commission may appoint one or more advisory committees to provide advice to the Personal Data Protection Commission with regard to the performance of any of its functions under this Part.

86. The Personal Data Protection Commission may consult such advisory committees in relation to the performance of its functions and duties and the exercise of its powers under this Part but shall not be bound by such consultation.

PART (VII)

COMPUTER MISUSE AND CYBERCRIME

Chapter (45)
Objectives of this Part

87. The objective of this Part is to lay the legislative foundations for the enhancement of protections in respect of computer misuse and cybercrime by:
    a. establishing a Cybercrime Working Committee; and
    b. setting out legislative and other measures for development to, inter alia, protect the integrity of computer systems and the confidentiality, integrity and availability of data, and, where applicable, to enable alignment with the Budapest Convention.

Chapter (46)
Definitions

88. In this Part, terms not defined elsewhere in this Law have the meanings given to them in the Budapest Convention.

Chapter (47)
Formation of the Cybercrime Working Committee

89. The Union Government hereby establishes the Cybercrime Working Committee.

90. *[Lead ministry to be discussed – Ministry of Transport and Communications?]*.

91. The Cybercrime Working Committee shall comprise the following persons : -

a.	[Union Minister, Ministry of Transport and Communications]	Chairman
b.	[Minister, Ministry of President's Office]	Vice-Chairman
c.	[Attorney General, Union Attorney General Office]	Member
d.	[Minister or Deputy Minister, Ministry of Defence Affairs]	Member
e.	[Minister or Deputy Minister, Ministry of Home Affairs]	Member
f.	[Chief of Police, Myanmar Police Force]	Member
g.	[Head of the National Cyber Security Centre]	Member
h.	[Head of the Myanmar Intellectual Property Office *(once it is established)]*	Member
i.	[Appropriate person as Secretary]	

92. *[Funding of the Working Committee on Cybercrime to be discussed and set out here.]*

Chapter (48)
Role and functions of the Cybercrime Working Committee

93. The Cybercrime Working Committee shall have primary responsibility for the execution of the objectives set out in this Part. For these purposes, the Cybercrime Working Committee shall have the following functions:

a. to act as the lead agency in the public sector in respect of the functions specified in paragraphs b to j;
b. to promote awareness of computer misuse and cybercrime threats and mitigation measures in the Republic of the Union of Myanmar;
c. to develop a common criminal policy aimed at the protection of society against computer misuse and cybercrime, including developing such legislative and other measures as are required to give effect to Chapters (49) to (62) of this Part;
d. to provide consultancy, advisory, technical, managerial or other specialist services relating to computer misuse and cybercrime threats and mitigation measures;
e. to work with and advise the Union Government and any other public sector body on all matters relating to computer misuse and cybercrime threats and mitigation measures, including national needs and policies;
f. to conduct research and studies and promote educational activities relating to computer misuse and cybercrime threats and mitigation measures, including organising and conducting seminars and workshops relating to such measures, and supporting other organisations conducting such activities;
g. to manage technical co-operation and exchange in the area of computer misuse and cybercrime with other organisations, including foreign computer misuse and cybercrime authorities and international or inter-governmental organisations;
h. to consult with the private sector in combating computer misuse and cybercrime, recognising the need to protect legitimate interests in the use and development of information technologies;
i. to carry out functions conferred on the Cybercrime Working Committee under any other written law or by the Union Government; and
j. to develop the necessary capabilities to support the performance of these functions.

Chapter (49)
Illegal access

94. The Cybercrime Working Committee shall develop such legislative and other measures as may be necessary to establish as a criminal offence, when committed intentionally, the access to the whole or any part of a computer system without right. The offence may be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

Chapter (50)
Illegal interception

95. The Cybercrime Working Committee shall develop such legislative and other measures as may be necessary to establish as a criminal offence, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. The offence may be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.

Chapter (51)
Data interference

96. The Cybercrime Working Committee shall develop such legislative and other measures as may be necessary to establish as criminal offences, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right, where the conduct results in serious harm.

Chapter (52)
System interference

97. The Cybercrime Working Committee shall develop such legislative and other measures as may be necessary to establish as criminal offences, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

Chapter (53)
Misuse of devices

98. The Cybercrime Working Committee shall develop such legislative and other measures as may be necessary to establish as criminal offences, when committed intentionally and without right:
    a. the production, sale, procurement for use, import, distribution or otherwise making available of:
        i. a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences to be established in accordance with sections 94 to 97;
        ii. a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed,

    with intent that it be used for the purpose of committing any of the offences established in sections 94 to 97; and
    b. the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in sections 94 to 97.

99. The legislative and other measures to be developed pursuant to this Chapter (53) shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in section 98 is not for the purpose of committing an offence to be established in accordance with sections 94 to 97, such as for the authorised testing or protection of a computer system.

Chapter (54)
Computer-related forgery

100. The Cybercrime Working Committee shall develop such legislative and other measures as may be necessary to establish as criminal offences, when committed intentionally, with intent to defraud, and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon

for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible.

Chapter (55)
Computer-related fraud

101. The Cybercrime Working Committee shall develop such legislative and other measures as may be necessary to establish as criminal offences, when committed intentionally and without right, the causing of a loss of property to another person by:
    a. any input, alteration, deletion or suppression of computer data,
    b. any interference with the functioning of a computer system,

    with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.

Chapter (56)
Child Pornography

102. The Cybercrime Working Committee shall develop such legislative and other measures as may be necessary to establish as criminal offences, when committed intentionally, the following conduct:
    a. producing child pornography for the purpose of its distribution through a computer system;
    b. offering or making available child pornography through a computer system;
    c. distributing or transmitting child pornography through a computer system;
    d. procuring child pornography through a computer system for oneself or for another person; and
    e. possessing child pornography in a computer system or on a computer-data storage medium.

103. For the purpose of section 102 above, the term "child pornography" shall include pornographic material that visually depicts:
    a. a minor engaged in sexually explicit conduct;
    b. a person appearing to be a minor engaged in sexually explicit conduct;
    c. realistic images representing a minor engaged in sexually explicit conduct.

104. For the purpose of section 103 above, the term "minor" shall include all persons under 18 years of age.

Chapter (57)
Attempt and aiding or abetting

105. The Cybercrime Working Committee shall develop such legislative and other measures as may be necessary to establish as criminal offences, when committed intentionally, aiding or abetting the commission of any of the offences to be established in accordance with sections 94 to **Error! Reference source not found.** with intent that such offence be committed.

106. The Cybercrime Working Committee shall develop such legislative and other measures as may be necessary to establish as criminal offences, when committed intentionally, an attempt

to commit any of the offences to be established in accordance with sections 95, 96, 97, 100, 101, 102.a and 102.c.

Chapter (58)
Corporate liability

107. The Cybercrime Working Committee shall develop such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offence to be established in accordance with this Part, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on:
    a. power of representation of the legal person;
    b. an authority to take decisions on behalf of the legal person;
    c. an authority to exercise control within the legal person.

108. In addition to the circumstances already provided for in section 107, the Cybercrime Working Committee shall develop such legislative and other measures as may be necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in section 107 has made possible the commission of a criminal offence to be established in accordance with this Part for the benefit of that legal person by a natural person acting under its authority.

109. The liability of a legal person under this Chapter (58) may be criminal, civil or administrative. Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.

Chapter (59)
Sanctions and measures

110. The Cybercrime Working Committee shall develop such legislative and other measures as may be necessary to ensure that the criminal offences to be established in accordance with sections 94 to 106 are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty.

111. The Cybercrime Working Committee shall develop such legislative and other measures as may be necessary to ensure that legal persons held liable in accordance with Chapter (58) shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions.

Chapter (60)
Procedural matters

112. The Cybercrime Working Committee shall develop such legislative and other measures as may be necessary to establish the powers and procedures provided for in this Part for the purpose of specific criminal investigations or proceedings.

113. Except as specifically provided otherwise in section 118, the powers and procedures referred to in section 112 shall apply to:

a. the criminal offences to be established in accordance with sections 94 to 106;
b. other criminal offences committed by means of a computer system; and
c. the collection of evidence in electronic form of a criminal offence.

114. The Cybercrime Working Committee shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Part provide for the adequate protection of human rights and liberties and shall incorporate the principle of proportionality. Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, inter alia, include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure. To the extent that it is consistent with the public interest, in particular the sound administration of justice, the Cybercrime Working Committee shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.

115. The Cybercrime Working Committee shall develop such legislative and other measures as may be necessary to enable competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification, by means of an order to a person to preserve specified stored computer data in the person's possession or control. Such measures shall oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. Such an order may subsequently be renewed. The Cybercrime Working Committee shall develop such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time in accordance with applicable confidentiality law. The powers and procedures referred to in this section shall be subject to sections 112 to 114.

116. The Cybercrime Working Committee shall develop, in respect of traffic data that is to be preserved under section 115, such legislative and other measures as may be necessary to:
    a. ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and
    b. ensure the expeditious disclosure to the competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the competent authority to identify the service providers and the path through which the communication was transmitted.

    The powers and procedures referred to in this section shall be subject to sections 112 to 114.

117. The Cybercrime Working Committee shall develop such legislative and other measures as may be necessary to empower competent authorities to:
    a. collect or record through the application of technical means in the territory of Republic of the Union of Myanmar, and
    b. compel a service provider, within its existing technical capability:
        i. to collect or record through the application of technical means in the territory of Republic of the Union of Myanmar; or

ii. to co-operate and assist the competent authorities in the collection or recording of,

traffic data, in real-time, associated with specified communications in the territory of the Republic of the Union of Myanmar transmitted by means of a computer system. The Cybercrime Working Committee shall develop such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this section and any information relating to it. The powers and procedures referred to in this section shall be subject to sections 112 to 114.

118. The Cybercrime Working Committee shall develop such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to:
    a. collect or record through the application of technical means in the territory of the Republic of the Union of Myanmar, and
    b. compel a service provider, within its existing technical capability:
        i. to collect or record through the application of technical means in the territory of the Republic of the Union of Myanmar, or
        ii. to co-operate and assist the competent authorities in the collection or recording of,

content data, in real-time, of specified communications in the territory of the Republic of the Union of Myanmar transmitted by means of a computer system. The Cybercrime Working Committee shall develop such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this section and any information relating to it. The powers and procedures referred to in this section shall be subject to sections 112 to 114.

Chapter (61)
Jurisdiction

119. The Cybercrime Working Committee shall develop such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with sections 94 to 106 when the offence is committed:
    a. in the territory of the Republic of the Union of Myanmar; or
    b. on board a ship flying the flag of the Republic of the Union of Myanmar; or
    c. on board an aircraft registered under the laws of the Republic of the Union of Myanmar; or
    d. by a national of the Republic of the Union of Myanmar, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.

120. The Cybercrime Working Committee shall develop such legislative and other measures as may be necessary to establish jurisdiction in relation to extraditable offences to the extent necessary to give effect to Chapter (62) of this Part, in accordance with Article 22.3 of the Budapest Convention.

Chapter (62)
International Cooperation

121. The Cybercrime Working Committee shall develop such legislative and other measures (including relevant international instruments on international cooperation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation and domestic laws) as may be necessary to give effect to the provisions of Chapter (III) (International Cooperation) of the Budapest Convention.

Chapter (63)
Powers of the Cybercrime Working Committee

122. Subject to this Law and any other applicable law, the Cybercrime Working Committee has the power to do all things necessary to be done for, or in connection with, the performance of its functions.

123. Without limiting the generality of section 122, the powers of the Cybercrime Working Committee include power:
    a. to develop the legislative and other measures to be developed by it in accordance with Chapters (49) to (62) of this Part and submit them to Parliament through the appropriate channels;
    b. to develop and issue codes of practice, guidelines and standards applicable to computer misuse and cybercrime prevention and mitigation;
    c. to collaborate with other persons (in or outside the Republic of the Union of Myanmar), in respect of computer misuse and cybercrime;
    d. to organise, provide for or collaborate with any person on training programmes, assessments and certifications of, and scholarships for, persons in relation to computer misuse and cybercrime prevention and mitigation;
    e. to enter into agreements and arrangements for the purposes of performing its functions in accordance with this Law;
    f. to form or participate in the formation of a body corporate, unincorporated association or trust, or enter into a joint venture with any person in compliance with all applicable procedures;
    g. to accept grants, gifts, donations or contributions from any source, or raise funds, in each case by all lawful means and in compliance with all applicable procedures;
    h. to provide financial support, grant, aid or assistance to any person in connection with any function of the Cybercrime Working Committee in compliance with all applicable procedures; and
    i. issue notifications, orders, directives and procedures.

Chapter (64)
Advisory Committees

124. The Cybercrime Working Committee may appoint one or more advisory committees to provide advice to the Cybercrime Working Committee with regard to the performance of any of its functions under this Part.

125. The Cybercrime Working Committee may consult such advisory committees in relation to the performance of its functions and duties and the exercise of its powers under this Part but shall not be bound by such consultation.

PART (VIII)

MISCELLANEOUS

Chapter (65)
Saving and transitional provisions

Chapter (66)
Other miscellaneous provisions

I hereby signed under the Constitution of the Republic of the Union of Myanmar.

Sd/

Win Myint
President
Republic of the Union of Myanmar