

## အီလက်ထရောနစ် ဆက်သွယ်ဆောင်ရွက်ရေးဥပဒေကို ပြင်ဆင်သည့် ဥပဒေပြဋ္ဌာန်း

ပြည်ထောင်စုသမ္မတမြန်မာနိုင်ငံတော်

နိုင်ငံတော်စီမံအုပ်ချုပ်ရေးကောင်စီ

နိုင်ငံတော်စီမံအုပ်ချုပ်ရေးကောင်စီ ဥပဒေအမှတ်(၇/၂၀၂၁)

အီလက်ထရောနစ်ဆက်သွယ်ဆောင်ရွက်ရေးဥပဒေကို ပြင်ဆင်သည့် ဥပဒေ

၁၃၈၂ခုနှစ်၊ တပို့တွဲလဆန်း ၄ရက်

၂၀၂၁ခုနှစ်၊ ဖေဖော်ဝါရီလ ၁၅ရက်

## Legislation amending the Electronic Transactions Law<sup>1</sup>

The Republic of the Union of Myanmar

State Administrative Council

State Administrative Council Law No. (7/2021)

Law Amending the Electronic Transactions Law

4th day of the first lunar month, 1382

February 15, 2021

၁။ နိုင်ငံတော်စီမံအုပ်ချုပ်ရေးကောင်စီသည် ပြည်ထောင်စုသမ္မတမြန်မာနိုင်ငံတော် ဖွဲ့စည်းပုံအခြေခံဥပဒေပုဒ်မ ၄၁၉ အရ ဤဥပဒေကို ပြဋ္ဌာန်းလိုက်သည်။

1. The State Administrative Council enacts this Law in accordance with Article 419 of the Constitution of the Republic of the Union of Myanmar.

၂။ ဤဥပဒေကို အီလက်ထရောနစ်ဆက်သွယ်ဆောင်ရွက်ရေးဥပဒေကို ပြင်ဆင်သည့် ဥပဒေဟု ခေါ်တွင်စေရမည်။

2. This Law shall be called the Law Amending the Electronic Transactions Law.

၃။ အီလက်ထရောနစ် ဆက်သွယ်ဆောင်ရွက်ရေး ဥပဒေပုဒ်မ ၂ ပုဒ်မခွဲ (က) ကို အောက်ပါအတိုင်း အစားထိုးရမည်။

3. Article 2 subsection (a) of the Electronic Transactions Law shall be substituted as follows:

(က) သတင်းအချက်အလက်ဆိုသည်မှာ အချက်အလက် (Data)၊ မူရင်းစာ (Text)၊ ပုံရိပ်သဏ္ဍာန် (Image)၊ အသံ (Voice)၊ ဗီဒီယို (Video)၊ သင်္ကေတ (Code)၊ ဆော့ဖ်ဝဲ (Software)၊ အပလီကေးရှင်း (Application) နှင့် အချက်အလက်အစုအဝေး (Database) တို့ကိုဆိုလိုသည်။

(A) “Information” means data, text, images, audio, video, Code Software, Application, and Database

၄။ အီလက်ထရောနစ်ဆက်သွယ်ဆောင်ရွက်ရေး ဥပဒေ ပုဒ်မ ၂

4. Article 2 of the Electronic Transactions Law, subsection (k) will be followed by subsection (l), subsection (m), subsection (n), subsection (o), subsection (p), subsection (q) and subsection (r) shall be supplemented as follows:

ပုဒ်မခွဲ (ဋ) ၏ နောက်တွင် ပုဒ်မခွဲ (ဌ)၊ ပုဒ်မခွဲ (ဍ)၊ ပုဒ်မခွဲ (ဎ)၊ ပုဒ်မခွဲ (ဏ)၊ ပုဒ်မခွဲ (တ)၊ ပုဒ်မခွဲ (ထ) နှင့် ပုဒ်မခွဲ (ဒ) တို့အဖြစ် အောက်ပါအတိုင်း ဖြည့်စွက်ရမည်။

(l) “Personal information” means any information which has been verified or verified as a person associated with a person.

(ဌ) ကိုယ်ရေးဆိုင်ရာအချက်အလက်ဆိုသည်မှာ လူတစ်ဦးတစ်ယောက်နှင့် ဆက်သွယ်သည့် မည်သူ့မည်ဝါအဖြစ် အတည်ပြုပြီးသော သို့မဟုတ် အတည်ပြုနိုင်သော မည်သည့် အချက်အလက်ကိုမဆို ဆိုသည်။

(m) “Person responsible for the management of personal information” means the person under any existing law or the provisions of this Law; It means the person and its staff assigned by a government department or organization that has the authority to collect, store, and use personal information.

(ဍ) ကိုယ်ရေးဆိုင်ရာ အချက်အလက်ကို စီမံထိန်းသိမ်းရန် တာဝန်ရှိသူ ဆိုသည်မှာ တည်ဆဲဥပဒေ တစ်ရပ်ရပ်အရဖြစ်စေ၊ ဤဥပဒေပါ ပြဋ္ဌာန်းချက်အရဖြစ်စေ၊ ကိုယ်ရေးဆိုင်ရာအချက်အလက်ကို ကောက်ခံခြင်း၊ စုဆောင်းသိမ်းဆည်းခြင်းနှင့် အသုံးပြုခြင်းတို့အား ဆောင်ရွက်နိုင်သည့် အခွင့်အရေးအာဏာရှိသော အစိုးရဌာန၊ အဖွဲ့အစည်း တစ်ခုခုဖြစ်စေ တာဝန်ပေးအပ်ခြင်းခံရသော ပုဂ္ဂိုလ်နှင့် ယင်း၏ ဝန်ထမ်းများကို ဆိုလိုသည်။

(ပ)စီမံခန့်ခွဲခြင်းဆိုသည်မှာ ကိုယ်ရေးဆိုင်ရာအချက်အလက်ကို ကောက်ယူခြင်း၊ ရယူခြင်း၊ လွှဲပြောင်းခြင်း၊ ဖြန့်ဝေခြင်း၊ တွဲဖက်ဆောင်ရွက်ခြင်း၊ တားမြစ်ခြင်း၊ ဖျက်ဆီးခြင်း၊ မှတ်တမ်းတင်ခြင်း၊ ထိန်းသိမ်းခြင်း၊ သိမ်းဆည်းခြင်း၊ ပြောင်းလဲခြင်း၊ သိမ်းဆည်းထားသည်များကို ပြန်လည်ကောက်ယူခြင်း၊ အကြံပြုခြင်း၊ အသုံးပြုခြင်း သို့မဟုတ် ထုတ်ဖော်ခြင်းကို ဆိုလိုသည်။

(ဏ) ဆိုက်ဘာအရင်းအမြစ် ဆိုသည်မှာ ကွန်ပျူတာ၊ ကွန်ပျူတာစနစ်၊ ကွန်ပျူတာ ပရိုဂရမ် သို့မဟုတ် ပရိုဂရမ်၊ ကွန်ယက်၊ ဆက်သွယ်ရေးပစ္စည်းနှင့် အချက်အလက်တို့ကို ဆိုသည်။

(တ) မောလ်ဝဲရ် (Malware) ဆိုသည်မှာ ဆိုက်ဘာအရင်းအမြစ်အား အနှောင့်အယှက် ဖြစ်စေသော သို့မဟုတ် အန္တရာယ်ဖြစ်စေသော အဖျက်အမှောင့် ကုဒ် ( Malicious Code ) ကို ဆိုသည်။

(ထ) ဆိုက်ဘာနယ်ပယ် ( Cyber Space) ဆိုသည်မှာ သတင်းအချက်အလက်နည်းပညာအခြေခံကွန်ရက်စနစ်တွင် ဆိုက်ဘာအရင်းအမြစ်များကို အသုံးပြု၍ သတင်းအချက်အလက်၊ အချက်အလက်အစုအဝေး၊ အီလက်ထရောနစ် သတင်းအချက်အလက်၊ ကွန်ပျူတာပရိုဂရမ်၊ ဆော့ဖ်ဝဲ ( Software ) ၊ အပလီကေးရှင်း ( Application ) တစ်ခုခုကို အသုံးပြုပြီး အီလက်ထရောနစ် သတင်းအချက်အလက်များအား ကွန်ရက်တစ်ခုအတွင်းဖြစ်စေ၊ ကွန်ရက်အချင်းချင်းချိတ်ဆက်၍ဖြစ်စေ အပြန်အလှန်အားဖြင့် ပေးပို့ခြင်း၊ ဆက်သွယ်ခြင်း၊ ဖြန့်ဝေခြင်း သို့မဟုတ် လက်ခံရယူခြင်း ဆောင်ရွက်နိုင်သည့် ဝန်းကျင်နယ်ပယ်ကို ဆိုသည်။

(ဒ) ဆိုက်ဘာတိုက်ခိုက်မှု ဆိုသည်မှာ ဆိုက်ဘာနယ်ပယ်အတွင်း ဆိုက်ဘာအရင်းအမြစ် တစ်ရပ်ရပ်ကို အသုံးပြု၍ နိုင်ငံတော်၏ အုပ်ချုပ်ရေး၊ ဘဏ္ဍာရေး၊ စီးပွားရေး၊ တရားဥပဒေ စိုးမိုးရေး၊ အမျိုးသားလုံခြုံရေး သို့မဟုတ် အများပြည်သူ၏ လုံခြုံရေးနှင့် အသက်အိုးအိမ်စည်းစိမ် ထိခိုက်ပျက်စီးစေရေးတို့ကို ရည်ရွယ်သည့် တိုက်ခိုက်မှု တစ်ရပ်ရပ်ကို ဖောက်ဖျက်ကျူးလွန်ခြင်း၊ ကျူးလွန်ရန် အားထုတ်ခြင်း၊ အားပေးကူညီခြင်း၊ လှုံ့ဆော်ခြင်း သို့မဟုတ် ကြိရာပါအဖြစ် ဆောင်ရွက်ခြင်းတို့ကို ဆိုသည်။

(n) “Management” means the collection of personal information; Acquisition Transfer Distribution; Collaboration; Prohibition Destruction; Recording; Maintenance; Storage; Change Retrieval, advice, and retrieval of archives Use or disclosure.

(o) “Cyber resources” means computers, Computer system; Computer program or program; Network, communication equipment and data.

(p) “Malware” means malicious code that disrupts or endangers a cyber source.

(q) “Cyberspace” means the use of cyber resources in information technology-based networks. Data collection; Electronic information; Computer programs; Software Use electronic applications to access electronic information over a network or network. An environment in which you can send, communicate, distribute, or receive networked or reciprocal networks.

(r) “Cyber-attack” means the use of any cyber resource in the field of cyber’s administrative, financial, economic, Rule of law; Committing an offence against an attack aimed at national security or public safety and property; Attempt to commit; Encouragement; Incitement or conspiracy. (Editor’s note: the corresponding provision in the CSL also referred to provisions which have been removed.)

၅။ အီလက်ထရောနစ်ဆက်သွယ်ဆောင်ရွက်ရေးဥပဒေပုဒ်မ ၂ ပုဒ်မခွဲ (၄)၊ ပုဒ်မခွဲ (၃) နှင့် ပုဒ်မခွဲ (ပ) တို့ကို ပုဒ်မခွဲ (၈)၊ ပုဒ်မခွဲ (န) နှင့် ပုဒ်မခွဲ (ပ) တို့အဖြစ် ပြန်လည်အမှတ်စဉ်ရမည်။

5. Article 2 of Electronic Transaction Law subsection (l), subsection (m) shall be reclassified as subsection (s), subsection (t), subsection (u).

၆။ အီလက်ထရောနစ်ဆက်သွယ်ဆောင်ရွက်ရေးဥပဒေပုဒ်မ ၃ ပုဒ်မခွဲ (င) ၏ နောက်တွင် ပုဒ်မခွဲ (စ) အဖြစ် အောက်ပါအတိုင်း ဖြည့်စွက်ရမည် -  
  
(စ) အများပြည်သူတို့၏ ကိုယ်ရေးဆိုင်ရာ အချက်အလက်များကို ဥပဒေနှင့် အညီအကာအကွယ်ပေးနိုင်ရန်။

6. After Article 3 subsection (e), subsection (f) shall be added as follows:  
  
(F) To protect the personal information of the public in accordance with the law.

၇။ အီလက်ထရောနစ်ဆက်သွယ်ဆောင်ရွက်ရေးဥပဒေ အခန်း (၁၀) ကို အောက်ပါအတိုင်း ဖြည့်စွက်ရမည်။  
  
အခန်း (၁၀)  
  
ကိုယ်ရေးဆိုင်ရာ အချက်အလက်ကာကွယ်ခြင်း  
  
၂၇-က ။ ကိုယ်ရေးဆိုင်ရာ အချက်အလက်ကို စီမံထိန်းသိမ်းရန် တာဝန်ရှိသူသည်-

7. Chapter 10 of the Electronic Transactions Law shall be supplemented as follows:  
  
Chapter (10)  
  
Protection of personal information  
  
27.a. The person responsible for managing and keeping the personal information shall: (Editor’s note: this provision is

(၁) မိမိတာဝန်ခံဆောင်ရွက်ရသည့် ကိုယ်ရေးဆိုင်ရာအချက်အလက်ကို အမျိုးအစား၊ လုံခြုံမှုအဆင့်အတန်းအလိုက် ဥပဒေနှင့် အညီ စနစ်တကျ ထိန်းသိမ်းခြင်း၊ ကာကွယ်ခြင်း နှင့် စီမံခန့်ခွဲခြင်းတို့ကို ဆောင်ရွက်ရမည်။

(၂) တည်ဆဲဥပဒေ တစ်ရပ်ရပ်ပါ ပြဋ္ဌာန်းချက်အရ ခွင့်ပြုချက် သို့မဟုတ် ကိုယ်ရေးဆိုင်ရာ အချက်အလက်ပိုင်ရှင်၏ ခွင့်ပြုချက်အရမှ အပ မိမိ၏ စီမံခန့်ခွဲမှုအောက်ရှိ ကိုယ်ရေးဆိုင်ရာ အချက်အလက်ကို အခြားသူတစ်ဦးတစ်ယောက် သို့မဟုတ် အဖွဲ့အစည်းတစ်ခုခုသို့ ကိုယ်ရေးဆိုင်ရာ အချက်အလက် တစ်စုံတစ်ရာအား စီစစ်ရန် ခွင့်ပြုခြင်း၊ ဖွင့်ချခြင်း၊ အသိပေးခြင်း၊ ဖြန့်ဝေခြင်း၊ ပေးပို့ခြင်း၊ ပြုပြင်ပြောင်းလဲခြင်း၊ ဖျက်ဆီးခြင်း၊ မိတ္တူကူးပွားခြင်း သို့မဟုတ် သက်သေခံအဖြစ် တင်သွင်းခြင်း မပြုရ။

(၃) ဦးတည်ချက်နှင့် ကိုက်ညီမှန်ကန်မှုမရှိသည့် စီမံခန့်ခွဲခြင်းကိစ္စရပ်များအတွက် ကိုယ်ရေးဆိုင်ရာအချက်အလက်တို့ကို သုံးစွဲခြင်းမပြုရ။

(၄) အချိန်ကာလ အကန့်အသတ်ဖြင့် အသုံးပြုရန် ရည်ရွယ်ထားသော ကိုယ်ရေးဆိုင်ရာ အချက်အလက်ကို သတ်မှတ်အချိန်ကာလ ကျော်လွန်ပါက စနစ်တကျ ဖျက်ဆီးရမည်။

၂၇-ခ။ တည်ဆဲဥပဒေတစ်ရပ်ရပ်အရ ကိုယ်ရေးဆိုင်ရာအချက်အလက်အပါအဝင် သတင်းအချက်အလက်ကို လက်ခံရရှိသည့် စုံစမ်းစစ်ဆေးရေးအဖွဲ့တစ်ခုခုသည် လည်ကောင်း၊ ယင်း၏ ကိုယ်စား တာဝန်လွှဲအပ်ခြင်းခံရသော သို့မဟုတ် ညွှန်ကြားမှုအောက်တွင်ရှိသော ပုဂ္ဂိုလ်သည်လည်ကောင်း မိမိရရှိထားသည့် သတင်းအချက်အလက်များကို ဥပဒေအရထုတ်ဖော်ပြောဆိုရန် တာဝန်ရှိမှုမတစ်ပါး လျှို့ဝှက်ထားရမည်။

၂၇-ဂ။ ကိုယ်ရေးဆိုင်ရာအချက်အလက် စီမံခန့်ခွဲခြင်းကိစ္စရပ်များတွင် အောက်ပါကိစ္စရပ်များ သက်ဆိုင်ခြင်းမရှိစေရ-

(၁) ဗဟိုအဖွဲ့က တာဝန်ပေးအပ်သော အစိုးရဌာန၊ စုံစမ်းစစ်ဆေးရေးအဖွဲ့ သို့မဟုတ် တရားဥပဒေစိုးမိုးရေးအဖွဲ့က ဆိုက်ဘာလုံခြုံရေး၊ ဆိုက်ဘာတိုက်ခိုက်ခြင်း၊ ဆိုက်ဘာ အလွဲအသုံးပြုခြင်း၊ ဆိုက်ဘာမတော်တဆမှုများ ဖြစ်ပွားခြင်း သို့မဟုတ် ဆိုက်ဘာမှခင်းနှင့် သက်ဆိုင်၍ ဟန့်တားကာကွယ်ခြင်း၊ ရှာဖွေထောက်လှမ်းခြင်း၊ စုံစမ်းစစ်ဆေးခြင်း၊ တရားရုံးတစ်ခုခုတွင် သက်သေခံအဖြစ် တင်သွင်းခြင်း။

(၂) ဗဟိုအဖွဲ့က တာဝန်ပေးအပ်သော အစိုးရဌာန၊ စုံစမ်းစစ်ဆေးရေးအဖွဲ့ သို့မဟုတ် တရားဥပဒေစိုးမိုးရေးအဖွဲ့က ပြစ်မှုဆိုင်ရာကိစ္စရပ်များ အလိုက် စီမံဆောင်ရွက်ခွင့် အာဏာအရ ဆောင်ရွက်သည့် ရှာဖွေထောက်လှမ်းခြင်း၊ စုံစမ်းစစ်ဆေးခြင်း၊ သတင်းရယူစုစည်းခြင်း၊ တရားစွဲဆိုတင်ပို့ခြင်းနှင့် တရားရုံးတစ်ခုခုတွင် သက်သေခံအဖြစ် တင်သွင်းခြင်း။

(၃) ဆိုက်ဘာလုံခြုံရေးနှင့် ဆိုက်ဘာမှခင်းဆိုင်ရာ ကိစ္စရပ်များသည် နိုင်ငံတော်အချုပ်အခြာအာဏာ တည်တံ့ခိုင်မြဲရေး၊ တည်ငြိမ်အေးချမ်းရေး၊ အမျိုးသားလုံခြုံရေး ကိစ္စရပ်များနှင့် သက်ဆိုင်သော စီမံဆောင်ရွက်ပိုင်ခွင့်အာဏာအရ ဆောင်ရွက်သည့် ရှာဖွေထောက်လှမ်းခြင်း၊ စုံစမ်းစစ်ဆေးခြင်း၊ သတင်းရယူစုစည်းခြင်း၊ သတင်းပေါင်းစပ်ညှိနှိုင်းဆောင်ရွက်ခြင်း။

(၄) ပုဒ်မခွဲ (၃)ပါ ကိစ္စရပ်များအား စီမံဆောင်ရွက်ရာတွင် ဗဟိုအဖွဲ့ကဖြစ်စေ၊ ဗဟိုအဖွဲ့ကတာဝန်ပေးအပ်သော ဌာန သို့မဟုတ် အဖွဲ့အစည်းကဖြစ်စေ စီမံပိုင်ခွင့် အာဏာခွဲခြားသတ်မှတ်ခြင်းနှင့် ယင်းသတ်မှတ်ချက်များနှင့်အညီ စီမံဆောင်ရွက်ခြင်း။

*copied from the draft CSL. Art. 13)*

(1) systematically keep, protect and manage the personal information based on its types, security levels in accordance with the law

(2) not allow, disclose, inform, distribute, dispatch, modify, destroy, copy and submit as evidence of the personal information of an individual without the consent or the permission in provisions included in an existing law to any individual or organization.

(3) not utilize personal information for managing issues that are not in compliance with the objectives

(4) systematically destroy the personal information that is collected to be used for a period of time after a certain period

27.b. The investigation team who receives information that includes personal information in accordance with the existing laws or the person mandated or instructed on their behalf shall keep the information confidential except disclosing the information in hand in accordance with the law. *(Editor's note: this provision is copied from the draft CSL. Art. 14)*

27.c. Personal Information Management shall not include the following: *(Editor's note: this provision is copied from the draft CSL. Art. 15)*

1) prevention, search and enquiry, investigation, submission of evidence in regard to cybersecurity, cyber-attacks, cyber terrorism, cyber misuse and cyber accident, cyber-crimes in a court by the government agency, investigation team or rule of law team assigned by the Central Committee

2) search and enquiry, investigation, collecting information, prosecution and submission of evidence in a court, carried out under the authority of respective criminal case by the government agency, investigation team or rule of law team assigned by the Central Committee.

3) enquiry, investigation, collecting information, coordinating information carried out in accordance with the authority on each relevant issue of stability of state sovereignty, public order, national security [when] the cybersecurity and cybercrime [fall under those aforementioned issues]

4) when carrying out activities in subsection (3),

	<p>identification of the management and managing in line with those identifications undertaken by either the central committee or department or organisation assigned by the central committee</p>
<p>၈။ အီလက်ထရောနစ်ဆက်သွယ်ဆောင်ရွက်ရေးဥပဒေ အခန်း(၁၀)(၁၁)(၁၂)နှင့်(၁၃)တို့ကို အခန်း(၁၁)(၁၂)(၁၃)နှင့် (၁၄)တို့အဖြစ်ပြန်လည်အမှတ်စဉ်ရမည်။</p>	<p>8. Chapters (10), (11), (12) and (13) of the Electronic Transactions Law shall be reclassified as Chapters (11), (12), (13) and (14).</p>
<p>၉။ အီလက်ထရောနစ်ဆက်သွယ်ဆောင်ရွက်ရေးဥပဒေပုဒ်မ ၃၈၏နောက်တွင် ပုဒ်မ ၃၈-က၊ ၃၈-ခ၊ ၃၈-ဂ၊ ၃၈-ဃနှင့် ၃၈-င တို့အဖြစ် အောက်ပါအတိုင်းဖြည့်စွက်ရမည်။</p> <p>၃၈-က။ ကိုယ်ရေးဆိုင်ရာအချက်အလက်များအား စီမံထိန်းသိမ်းရန်တာဝန်ရှိသူသည် ကိုယ်ရေးဆိုင်ရာအချက်အလက်ကို တျီဥပဒေပါ ပြဋ္ဌာန်းချက်များနှင့် အညီ စီမံခန့်ခွဲခြင်းမပြုကြောင်း ပြစ်မှုထင်ရှားစီရင်ခြင်းခံရလျှင် ထိုသူကို အနည်းဆုံး တစ်နှစ်မှ အများဆုံးသုံးနှစ်အထိ ထောင်ဒဏ်ဖြစ်စေ၊ ကျပ်သိန်းတစ်ရာထက်မပိုသော ငွေဒဏ်ဖြစ်စေ၊ ဒဏ်နှစ်ရပ်လုံးဖြစ်စေ ချမှတ်ရမည်။</p> <p>၃၈-ခ။ မည်သူမဆိုသက်ဆိုင်ရာပုဂ္ဂိုလ်၏ခွင့်ပြုချက်မရှိဘဲ လူပုဂ္ဂိုလ်တစ်ဦးတစ်ယောက်၏ ကိုယ်ရေးဆိုင်ရာ အချက်အလက်ကို ရယူခြင်း၊ဖွင့်ချခြင်း၊အသုံးပြုခြင်း၊ ဖျက်ဆီးခြင်း၊ ပြုပြင်ပြောင်းလဲခြင်း၊ ဖြန့်ဝေခြင်း၊ တစ်ဦးတစ်ယောက်ထံသို့ ပေးပို့ခြင်း သို့မဟုတ် အလွဲသုံးပြုခြင်းဖြစ်ကြောင်း ပြစ်မှုထင်ရှားစီရင်ခြင်းခံရလျှင် ထိုသူကို အနည်းဆုံး ထောင်ဒဏ်တစ်နှစ်မှ အများဆုံး သုံးနှစ်အထိ ထောင်ဒဏ်ဖြစ်စေ၊ ကျပ်သိန်းငါးဆယ်ထက်မပိုသော ငွေဒဏ်ဖြစ်စေ၊ ဒဏ်နှစ်ရပ်လုံးဖြစ်စေ ချမှတ်ရမည်။</p> <p>၃၈-ဂ။ မည်သူမဆို ဆိုက်ဘာနယ်ပယ်တွင် အများပြည်သူအထိတ်တလန့် ဖြစ်စေရန်၊ အယုံအကြည်ပျက်စေရန်၊ အကြည်ညိုပျက်စေရန် သို့မဟုတ်၊ အသင်းအဖွဲ့ကွဲစေရန် ရည်ရွယ်၍ သတင်းတု သို့မဟုတ် သတင်းမှား ပြုလုပ်ဖန်တီးခြင်းကို ကျူးလွန်ကြောင်း ပြစ်မှုထင်ရှားစီရင်ခြင်း ခံရလျှင် ထိုသူကို အနည်းဆုံး တစ်နှစ်မှ အများဆုံး သုံးနှစ်အထိ ထောင်ဒဏ်ဖြစ်စေ၊ ကျပ်သိန်းငါးဆယ်ထက်မပိုသော ငွေဒဏ်ဖြစ်စေ၊ ဒဏ်နှစ်ရပ်လုံးဖြစ်စေ ချမှတ်ရမည်။</p> <p>၃၈-ဃ။ မည်သူမဆို နိုင်ငံတော်၏ အချုပ်အခြာအာဏာ၊ လုံခြုံရေး။ တည်ငြိမ်အေးချမ်းရေး၊ တရားဥပဒေစိုးမိုးရေး သို့မဟုတ် တိုင်းရင်းသားစည်းလုံးညီညွတ်ရေးကို ခြိမ်းခြောက်နှောင့်ယှက်ဖျက်ဆီးရန် ရည်ရွယ်ချက်ဖြင့် ဆိုက်ဘာအရင်းအမြစ်ကို ရယူပိုင်ခွင့်မရှိအောင် တားဆီးခြင်း၊ ခက်ခဲအောင်ပြုလုပ်ခြင်း သို့မဟုတ် ခွင့်ပြုချက်မရှိဘဲ ဆိုက်ဘာအရင်းအမြစ်ကို ထိုးဖောက်ဝင်ရောက်ရန် ကြိုးစားခြင်း၊ ခွင့်ပြုထားသည်ထက်ပို၍ အသုံးပြုခြင်း၊ တစ်စုံတစ်ယောက်ကို ထိခိုက်စေရန် ရည်ရွယ်ချက်ဖြင့် ကွန်ပျူတာတွင် မောလ်ဝဲရပ်တည်သွင်းခြင်းဖြင့် ဆိုက်ဘာတိုက်ခိုက်မှုကို ကျူးလွန်ကြောင်း ပြစ်မှုထင်ရှား စီရင်ခြင်းခံရလျှင် ထိုသူကို အနည်းဆုံးနှစ်နှစ်မှ အများဆုံး ငါးနှစ်အထိ ထောင်ဒဏ်ဖြစ်စေ၊ ကျပ်သိန်းသုံးရာထက်မပိုသော ငွေဒဏ်ဖြစ်စေ၊ ဒဏ်နှစ်ရပ်လုံးဖြစ်စေ ချမှတ်ရမည်။</p> <p>၃၈-င။ မည်သူမဆို နိုင်ငံတော်နှင့် အခြားနိုင်ငံတို့၏ ရင်းနှီးသောဆက်ဆံရေးကို ထိခိုက်ပျက်ပြားစေနိုင်သည့် ရည်ရွယ်ချက်ဖြင့်လည်းကောင်း၊ အခြားနိုင်ငံတစ်ခုခု၏ အကျိုးစီးပွားအလို့ငှာလည်းကောင်း၊ နိုင်ငံတော်နှင့် အခြားနိုင်ငံများအကြား ပူးပေါင်းဆောင်ရွက်နေသော လုံခြုံရေးအရ လျှို့ဝှက်ထားသည့်</p>	<p>9. Article 38-A, 38-B, 38-C, 38-D and 38-E shall be added as follows after Article 38 of the Electronic Transactions Law as follows:</p> <p>38.a. If a person responsible for managing personal data is convicted of failure to manage personal data in accordance with the provisions under this law, he or she shall be punishable by imprisonment for a term of 1 to 3 years, or a fine not exceeding 100 lakhs, or both.</p> <p>38.b. Any person, if convicted of obtaining, disclosing, using, destroying, modifying, disseminating or sending personal data of a person to another without approval, shall be punishable by imprisonment for a term of 1 to 3 years, or a fine not exceeding 50 lakhs, or both.</p> <p>38.c. Any person who is convicted of creating misinformation and disinformation with the intent of causing public panic, loss of trust or social division on cyberspace, shall be punishable by imprisonment for a term of 1 to 3 years, or a fine not exceeding 50 lakhs, or both.</p> <p>38.d. Any person who is convicted of cyber violence acts such as preventing access to cyber resource or making it difficult; attempting to hack into a cyber source without permission; using more than permitted; and inserting or installing dangerous malware with the intent to hurt someone; with an intent to threaten or disturb national sovereignty, security, peace and stability, rule of law and national solidarity, shall be punished by imprisonment for a term of 2 to 5 years, or a fine not exceeding 300 lakhs, or both.</p> <p>38.e. Any person who commits acts of cyber-attack such as attempts of unauthorised access to and hacking cyber sources which are kept confidential for nationally, internationally or multilaterally implemented security reasons; and using more than permitted; with the intent of deteriorating the relationship between the country and other foreign countries</p>

<p>ဆိုက်ဘာအရင်းအမြစ်ကို ခွင့်ပြုချက်မရှိဘဲ ထိုးဖောက်ဝင်ရောက်ရန်ကြိုးစားခြင်း သို့မဟုတ် ခွင့်ပြုထားသည်ထက်ပို၍ အသုံးပြုခြင်းဖြင့် ဆိုက်ဘာတိုက်ခိုက်မှုကို ကျူးလွန်ကြောင်း ပြစ်မှုထင်ရှားစီရင်ခြင်းခံရလျှင် ထိုသူကို အနည်းဆုံး သုံးနှစ်မှ အများဆုံးခုနှစ်နှစ်အထိ ထောင်ဒဏ်ဖြစ်စေ၊ ကျပ်သိန်းငါးရာထက်မပိုသော ငွေဒဏ်ဖြစ်စေ၊ ဒဏ်နှစ်ရပ်လုံးဖြစ်စေ ချမှတ်ရမည်။</p>	<p>or for the interests of other foreign countries, shall be punished by imprisonment for a term of 3 to 7 years, or a fine not exceeding 700 lakhs, or both.</p>
<p>ဖွဲ့စည်းပုံအခြေခံဥပဒေပုဒ်မ ၄၁၉အရ ကျွန်ုပ် လက်မှတ်ရေးထိုးသည်- (ပုံ) မင်းအောင်လှိုင် ဗိုလ်ချုပ်မှူးကြီး ဥက္ကဋ္ဌ နိုင်ငံတော်စီမံအုပ်ချုပ်ရေးကောင်စီ</p>	<p>I sign under Article 419 of the Constitution: Min Aung Hlaing Senior General Chairman State Administrative Council</p>