1. As the work we do frequently involves access to sensitive information about our clients, ensuring that the information we work with is protected is a crucial part of our job. This policy describes the measures we must take to secure information in our care.

၁။ ကျွန်ုပ်တို့ ဆောင်ရွက်နေသော လုပ်ငန်းများသည် ကျွန်ုပ်တို့၏ လုပ်ငန်းအပ်နှံသူများနှင့် ပတ်သတ်သည့် အရေးကြီးသော သတင်းအချက်အလက်များကို မကြာခဏဝင်ရောက် ကြည့်ရှုရသည် ဖြစ်သော ကြောင့် ကျွန်ုပ်တို့ ဆောင်ရွက်နေသော သတင်းအချက် အလက်များ ကို ထိန်းသိမ်းကာကွယ်ခြင်းသည် ကျွန်ုပ်တို့အလုပ်၏ အရေးပါသော အစိတ်အပိုင်း တစ်ရပ်ဖြစ်သည်။ ဤမူဝါဒတွင် သတင်းအချက် အလက်များကို ထိန်းသိမ်း ကာကွယ်ရာ၌ လုံခြုံ စိတ်ချမှု ရှိစေရန် ကျွန်ုပ်တို့ ဆောင်ရွက်မည့် အချက်များကို ဖော်ပြထားပါသည်။

Protected Information

2. As security professionals, we should always careful about protecting our information. The list below of examples of protected information is not exclusive. If you are uncertain whether other information should also be considered protected, assume that it should be. Examples of protected information include details regarding:

ထိန်းသိမ်းစောင့်ရှောက်ရမည့် သတင်းအချက်အလက်များ

၂။ လုံခြုံရေးဆိုင်ရာ ကျွမ်းကျင်သူများဖြစ်သော ကျွန်ုပ်တို့ အနေဖြင့် သတင်းအချက်အလက်များကို ထိန်းသိမ်း ကာကွယ်ရာတွင် အမြဲတစေ သတိရှိရမည်။ ဤစာရင်းတွင် ထိန်းသိမ်း ကာကွယ်ရမည့် သတင်းအချက်အလက် အောက်ပါ ဥပမာများ ပါဝင်ပါသည်။ အကယ်၍ ဥပမာတွင် ဖော်ပြမထားသည့် အခြားသော သတင်းအချက် အလက်များကိုထိန်းသိမ်း ကာကွယ်ရန် လိုအပ်ခြင်းရှိ/မရှိ သင့်အနေဖြင့် မသေချာလျှင် ထိုသတင်း အချက် အလက်များကို ထိန်းသိမ်းကာကွယ်သင့်သည်ဟု မှတ်ယူရမည်။ ထိန်းသိမ်း ကာကွယ် ရမည့် သတင်းအချက်အလက် ဥပမာများတွင် အောက်ဖော်ပြပါတို့နှင့် စပ်လျဉ်း၍ အသေးစိတ် အချက်အလက်များ ပါဝင်ပါသည်။

a. Exera's contracts with clients, including prices, contract duration, and scope of supply;

(က) ဈေးနှုန်းများ၊ စာချုပ်သက်တမ်းနှင့် လုပ်ငန်း ပမာဏ ပါဝင်သော Exera ၏လုပ်ငန်းအပ်နှံမှု ကန်ထရိုက် စာချုပ်များ

b. Client and Exera sites, including locations, vulnerabilities, security measures in place and daily routines;

(ခ) လုပ်ငန်းခွင် တည်နေရာများနှင့် အားနည်းချက်များ၊ လုပ်ငန်းခွင်နှင့် ပတ်သတ်သည့် လုံခြုံရေးဆိုင်ရာ ဆောင်ရွက်ချက်များ နှင့်နေ့စဉ် လုပ်ငန်းများ ပါဝင်သည့် Exera နှင့် လုပ်ငန်းအပ်နှံသူတို့၏ အလုပ်ခွင်များ။

c. Client and Exera employees and their family members, including names, home addresses, schools, contact information and common destinations; and

(ဂ) အမည်များ၊ အိမ်လိပ်စာများ၊ ကျောင်းများ၊ ဆက်သွယ် နိုင်မည့် သတင်းအချက် အလက်များနှင့် ပုံမှန် တည်ရှိရာနေရာများ ပါဝင်သော လုပ်ငန်းအပ်နှံသူနှင့် Exera တို့၏ ဝန်ထမ်းများ၊ မိသားစုဝင်များနှင့် သက်ဆိုင်သည့် သတင်း အချက်အလက်များ

d. Client and Exera operations, including suppliers, service providers, customers, and security arrangements.

(ဃ) ထောက်ပံ့သူများ (suppliers)၊ ဝန်ဆောင်မှု ပေးသူများ (service providers)၊ ဝန်ဆောင်မှု ရယူသူများ (customer) ၊ လုံခြုံရေးဆိုင်ရာ စီမံဆောင်ရွက်မှုများ ပါဝင်သည့် လုပ်ငန်း အပ်နှံသူနှင့် Exera ၏ လုပ်ငန်းဆောင်ရွက်ချက်များ။

Information Security Coordinator

3. A member of the executive team will be designated the Information Security Coordinator as a secondary duty. This person will control

သတင်းအချက်အလက် ထိန်းသိမ်းကာကွယ်သူ

၃။ ဒုတိယ တာဝန်အဖြစ် အမှုဆောင် အဖွဲ့ဝင် တစ်ဦးကို သတင်းအချက်အလက် ထိန်းသိမ်းကာကွယ်သူအဖြစ် ရွေးချယ်သတ်မှတ် လိမ့်မည်။ ထိုသူသည် သတင်းအချက်အလက် လုံခြုံရေးတည်တံ့ ခိုင်မြဲမှုကို ထိန်းသိမ်းရန် ကုမ္ပဏီရှိ ကွန်ပျူတာများ၊ စမတ်ဖုန်းများ၊ Tablets များ၏ အုပ်ချုပ်မှုပိုင်းဆိုင်ရာ

administrative accounts to company computers, smartphones and tablets to ensure that their information security integrity is maintained. They will also collect reports from Exera staff regarding suspicious emails, apparent computer viruses and discussions with non-authorized people, and make recommendations to the CEO as appropriate.

စာရင်းများ (accounts) ကို ထိန်းချုပ်လိမ့်မည်သာမက CEO ထံ သင့်လျော်သော အကြံပေးခြင်း၊ တရားဝင်ခွင့်ပြုထားခြင်း မရှိသောသူများနှင့် ဆွေးနွေးခြင်းများ၊ သိသာထင်ရှား သော ကွန်ပျူတာ ဗိုင်းရက်စ်များ၊ သံသယဖြစ်ဖွယ် အီးမေးလ်များ နှင့်စပ်လျဉ်း၍ Exera ဝန်ထမ်းများထံမှ အစီရင်ခံစာများ ကိုလည်း စုဆောင်း သိမ်းဆည်းလိမ့်မည်။

Secure Communication

4. Communication about protected information should only take place in *secure areas* using *secure means* and with *authorized people*.

လုံခြုံစိတ်ချရသော ဆက်သွယ်မှု

၄။ ထိန်းသိမ်းကာကွယ်ရမည့် သတင်းအချက် အလက်များနှင့် ပတ်သတ်၍ ဆက်သွယ် ပြောကြားမှုကို တရားဝင်ခွင့်ပြုထားသော သူများနှင့် လုံခြုံစိတ်ချရသည့် နည်းလမ်းများကို အသုံးပြုပြီး လုံခြုံ စိတ်ချရသည့် နေရာများတွင် သာလျှင် ဆက်သွယ် ပြောကြားရမည်။

a. *Secure areas* mean locations where the discussion is unlikely to be unintentionally or purposefully overhead or intercepted by non-authorized people;

(က) လုံခြုံစိတ်ချရသည့် နေရာဆိုသည်မှာ မသက်ဆိုင်သော/ တာဝန် မရှိသော သူများအနေဖြင့် မတော်တဆ ဖြစ်စေ၊ ရည်ရွယ်ချက်ရှိ၍ဖြစ်စေ ကြားခြင်း၊ ကြားဖြတ် ဝင်ရောက် ပြောဆိုခြင်း မပြုနိုင်သော နေရာကို ဆိုလိုသည်။

b. *Secure means* refers to a means of communication that can be reasonably supposed not to have been compromised. Such means include company-managed computers and telephones, or in-person discussions on client or company premises;

(ခ) လုံခြုံစိတ်ချရသည့် နည်းလမ်းဆိုသည်မှာ-ကြားဖြတ်ပြောဆိုခြင်း မပြုနိုင်သော ဆက်သွယ် ပြောကြားမှု နည်းလမ်းကို ဆိုလိုသည်။ ထိုနည်းလမ်းများတွင် ကုမ္ပဏီမှ စီမံထိန်းချုပ် ထားသော ကွန်ပျူတာများ၊ တယ်လီဖုန်းများ၊ လုပ်ငန်းအပ်နှံသူနှင့် လူကိုယ်တိုင် ဆွေးနွေးခြင်းများ (သို့) ကုမ္ပဏီ ပုရဝုဏ် စသည်တို့ဖြစ်သည်။

c. *Authorized people* means Exera or client staff, or designated client contractors, who have a legitimate requirement to know about and work with the protected information. Not all Exera or client employees will have a requirement to work with protected information, so they cannot all be assumed to be authorized people.

(ဂ) တရားဝင်ခွင့်ပြုထားသောသူများ ဆိုသည်မှာ ထိန်းသိမ်းကာကွယ်ရမည့် သတင်းအချက် အလက်များနှင့် ပတ်သက်၍ သိရှိနားလည်ပြီး တာဝန်ယူ ဆောင်ရွက်ရန် အတွက် တရားဝင် သတ်မှတ်ထား သော Exera ဝန်ထမ်းများ (သို့) လုပ်ငန်းအပ်နှံသူ၏ ဝန်ထမ်းများ (သို့) လုပ်ငန်းအပ်နှံသူ ကန်ထရိုက်တာ များကို ဆိုလိုခြင်းဖြစ်သည်။ Exera ဝန်ထမ်းများ (သို့) လုပ်ငန်းအပ်နှံသူ၏ ဝန်ထမ်းများ အားလုံးသည် ထိန်းသိမ်းကာကွယ်ရမည့် သတင်းအချက် အလက်များကို တာဝန်ယူ ဆောင်ရွက်လိမ့်မည် မဟုတ် သောကြောင့် ထိုသူတို့ကို တရားဝင် ခွင့်ပြုထားသော သူများ ဖြစ်သည်ဟု မမှတ်ယူသင့်ပါ။

5. Instances of non-authorized people trying to directly or indirectly

၅။ တရားဝင်ခွင့်ပြုမထားသူများသည် ထိန်းသိမ်း ကာကွယ်ရမည့် သတင်းအချက် အလက်များနှင့် ပတ်သတ်၍ သင့်ထံမှ တိုက်ရိုက် ဖြစ်စေ (သို့) သွယ်ဝိုက်၍ ဖြစ်စေ သိရှိရန် ကြိုးစား အားထုတ်သည့် ဖြစ်ရပ်များကို သံသယ

learn about protected information from you should be met with suspicion. Do not respond to questioning about protected information if you are not certain that a person is authorized to discuss it. Report instances like this to the Information Security Coordinator.

ရှိသည်ဟု မှတ်ယူရမည်။ ထိုပုဂ္ဂိုလ်သည် သတင်းအချက်အလက်များကို ဆွေးနွေးရန် တရားဝင် ခွင့်ပြုထား သောသူ ဟုတ်/မဟုတ် သင့်အနေဖြင့် မသေချာလျှင် ထိန်းသိမ်း ကာကွယ်ရမည့် သတင်းအချက် အလက်များ နှင့် ပတ်သတ်သော မေးခွန်းများကို ဖြေကြ ဖြေကြားခြင်းမပြုပါနှင့်။ ထိုကဲ့သို့သော ဖြစ်ရပ်များကို သတင်း အချက်အလက် ထိန်းသိမ်း ကာကွယ်သူထံ သတင်း ပေးပို့ရမည်။

Secure Workspaces

6. Exera's office is considered a *secure area*, however to ensure protected information is not compromised, keep your personal workspace secure by:

လုံခြုံစိတ်ချရသော လုပ်ငန်းခွင် နေရာများ

၆။ Exera ရုံးသည် လုံခြုံစိတ်ချရသော နေရာတွင် တည်ရှိပါသည်။ သို့သော်လည်း ထိန်းသိမ်းကာကွယ်ရမည့် သတင်းအချက် အလက်များကို အပေးအယူလုပ်ခြင်း မရှိစေရန် သင်၏ ကိုယ်ပိုင် လုပ်ငန်းခွင်နေရာကို အောက်ဖော်ပြပါ အချက်များကို ပြုလုပ်ခြင်းဖြင့် လုံခြုံစိတ်ချစွာ ထားရှိရမည်။

a. *Clearing* your desk of papers and working material at the end of the work day, or when leaving your desk for an extended period of time;

(က) တစ်နေ့တာ လုပ်ငန်းပြီးဆုံးလျှင်(သို့) လုပ်ငန်းခွင်၌ သင်မရှိလျှင် သင်၏စားပွဲပေါ်ရှိ စာရွက်များ၊ လုပ်ငန်းခွင်သုံး ပစ္စည်းများကို ရှင်းလင်း ထားရှိခြင်း။

b. *Storing* working documents only in lockable drawers or filing cabinets that you control access to; and

(ခ) သော့ခတ်၍ရသော အံဆွဲများနှင့် ဗီရိုများ တွင်သာလျှင် လုပ်ငန်းခွင်နှင့် ပတ်သတ်သော စာရွက်စာတမ်းများကို သိမ်းဆည်းခြင်း။

c. *Shredding* documents that are no longer required. Shredders are located next to each printer in the office. Drawers and filing cabinets should be periodically cleared and old material that is not needed for historical record keeping shredded.

(ဂ) မလိုအပ်သော စာရွက်စာတမ်းများကို ဖျက်ဆီးခြင်း။ ရုံးတွင် စက္ကူဖြတ်စက်များကို Printer ဘေးတွင် ထားရှိပါသည်။ အံဆွဲများနှင့် ဗီရိုများကို ပုံမှန် ရှင်းလင်း ထားရှိရမည် ဖြစ်ပြီး ရှေးဟောင်း မှတ်တမ်းအနေဖြင့် သိမ်းဆည်းထားရန် မလိုအပ်သော စုဆောင်းထားသည့် အချက် အလက်များကို ဖျက်ဆီးရမည်။

7. In order to keep Exera's office secure, access to the office is control by an RFID swipe card system on the main door. All other doors to the office (fire escapes, etc) should be kept closed and locked except in emergencies. If other doors need to be used for specific purposes, they should be guarded continuously while unlocked and immediately locked again once no longer in use.

၇။ Exera ရုံးကို လုံခြုံစိတ်ချမှုရှိစေရန် အလို့ငှာ ပင်မ တံခါးတွင် RFID swipe card စနစ်ဖြင့် ရုံး၏ဝင်ပေါက်ကို ထိန်းချုပ်ထားပါသည်။ အရေးပေါ် လှေခါးအစရှိသည့် ရုံးသို့ ဝင်ရောက်နိုင်သော တံခါးပေါက်အားလုံးကို အရေးပေါ် အခြေအနေမှ လွဲ၍ သော့ခတ် ပိတ်ထားရမည်။ အခြား တံခါးပေါက်များကို သတ်မှတ်ထားသော အကြောင်းရင်း ကိစ္စများအတွက် အသုံးပြုရန် လိုအပ်လျှင် တံခါးဖွင့်ထားစဉ် အဆက်မပြတ် စောင့်ကြည့်ရမည်ဖြစ်ပြီး အသုံးမပြုလျှင် ချက်ချင်း သော သော့ခတ်ပိတ်ထားရမည်။

P.O. Box 967, 85 Hlaing Myint Moh 1st Street, Hlaing, Yangon 11181, Myanmar
Tel: +95 (0)1 514-001

Secure Devices

8. Company computers, smartphones, tablets and USB memory sticks are deemed to be *secure means* for communication of protected information, however to keep them secured:

a. Company computers must have an administrator account controlled only by the Information Security Coordinator (below), and a pre-configured, restricted-access user account with encrypted storage for daily use;

b. Company smartphones and tablets must have a restricted-access app installed to prevent the installation of non-authorized software, and the means to delete data remotely;

c. The company's Collab system alone should be used for work email and file storage/sharing. The use of non-"@exera.asia" accounts for work purposes is not permitted;

d. Attachments or links sent to your email by unknown people should not be opened. Speak to the Information Security Coordinator before responding to these emails or opening any such links or attachments;

e. Protected information copied onto USB memory sticks should be deleted as soon as it no longer needs to be stored there (i.e. after copying it to another computer). USB memory sticks with protected information on them should be kept securely locked when not in use, just like a hardcopy document; and

လုံခြုံစိတ်ချရသော ပစ္စည်းကိရိယာများ

၈။ ကုမ္ပဏီမှ ထုတ်ပေး ထားသော ကွန်ပျူတာများ၊ စမတ်ဖုန်းများ၊ Tablet များနှင့် USB memory stick များကို ထိန်းသိမ်း ကာကွယ်ရမည့် သတင်းအချက်အလက်များအား ပေးပို့ရာတွင် လုံခြုံစိတ်ချရသည့် နည်းလမ်းများဖြင့် ယူဆအသုံးပြုရမည်။

(က) ကုမ္ပဏီမှ ထုတ်ပေးထားသော ကွန်ပျူတာများတွင် သတင်းအချက်အလက် ထိန်းသိမ်း ကာကွယ်သူအနေဖြင့် သာလျှင် ထိန်းချုပ်ထားနိုင်သော အုပ်ချုပ်မှုပိုင်းဆိုင်ရာ စီမံခန့်ခွဲမှု အကောင့်တစ်ခု (administrator account)နှင့် နေ့စဉ် အသုံးပြုရန်အတွက် လျှို့ဝှက်ကုဒ်နံပါတ်နှင့်အတူ ဝင်ခွင့်ကို ကန့်သတ်ထားသော User account တစ်ခု ရှိပါသည်။

(ခ) ကုမ္ပဏီမှ ထုတ်ပေးထားသော စမတ် ဖုန်းများနှင့် tablets များတွင် ခွင့်ပြုမထား သော software များ ထည့်သွင်းခြင်းကို တားမြစ်ရန် ဝင်ရောက်ခွင့်ကို ကန့်သတ်ထားသော app နှင့် အချက်အလက်များကို ဖျက်ရန် နည်းလမ်းများကို ထည့်သွင်းထားပါသည်။

(ဂ) ကုမ္ပဏီ၏ Collab စနစ်ကို လုပ်ငန်းနှင့်ဆိုင်သော အီးမေးလ်များ၊ ဖိုင်များ သိမ်းထားခြင်း၊ ဝေမျှခြင်းအတွက်သာ အသုံးပြုရမည်။ "@exera.asia" မဟုတ်သော အီးမေးလ် အကောင့်များကို လုပ်ငန်းအတွက် အသုံးပြုရန် ခွင့်ပြုမည် မဟုတ်ပါ။

(ဃ) အမည်မသိသောသူများမှ သင်၏ အီးမေးလ် ထံပို့သော Attachments (သို့) links များကို ဖွင့်မကြည့်ရပါ။ ထိုကဲ့သို့သော Attachments (သို့) links များကို မဖွင့်မီ (သို့) အီးမေးလ်ပြန်မပို့မီ သတင်းအချက်အလက် ထိန်းသိမ်း ကာကွယ်သူကို ပြောကြားရမည်။

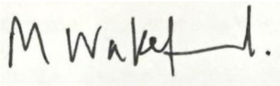
(င) USB memory stick ထဲသို့ ကူးယူသော ထိန်းသိမ်းကာကွယ်ရမည့် သတင်းအချက် အလက်များကို သိမ်းဆည်းထားရန် မလိုအပ်လျှင် ချက်ချင်း ဖျက်ရမည်။ (ဥပမာ- အခြားကွန်ပျူတာ ထဲသို့ သတင်းအချက်အလက်ကို ကူးယူပြီးလျှင်) ထိန်းသိမ်းကာကွယ်ရမည့် သတင်းအချက် အလက်များ ပါဝင်သော USB memory sticks ကို အသုံးမပြုလျှင် စာရွက်စာတမ်းများကို သိမ်းထား သကဲ့သို့ လုံခြုံစွာ သိမ်းထားရမည်။

f. If devices with protected information on them are lost or stolen, this must be reported to the Information Security Coordinator as soon as possible. A description of the material believed to have been lost should be provided.

(စ) ထိန်းသိမ်းကာကွယ်ရမည့် သတင်း အချက် အလက်များ ပါဝင်သော ပစ္စည်း ကိရိယာများ ပျောက်ဆုံးလျှင် (သို့) ခိုးယူခံရလျှင် သတင်း အချက် အလက် ထိန်းသိမ်း ကာကွယ်သူထံ ဖြစ်နိုင်သမျှ လျှင်မြန်စွာ သတင်းပေးပို့ရမည်။ ပျောက်ဆုံး သွားခဲ့သည်ဟု ယုံကြည် လက်ခံထားသည့် ပစ္စည်းအမျိုးအစားကို ပြန်လ ပြန်လည် ထုတ်ပေးလိမ့်မည်။

9. Individuals permitted to work with personal computers or personal smartphones at the office will consult with the Information Security Coordinator and follow their guidance on how to keep their computer and smartphone secure.

၉။ ရုံး၌ ကိုယ်ပိုင် ကွန်ပျူတာများ (သို့) စမတ်ဖုန်းများနှင့် လုပ်ငန်း ဆော ဆောင်ရွက်ရန် ခွင့်ပြုထားသောသူများသည် သတင်း အချက်အလက် ထိန်းသိမ်းကာကွယ်သူနှင့်ဆွေးနွေး တိုင်ပင်ပြီး ၎င်းတို့၏ ကွန်ပျူတာများ၊ စမတ်ဖုန်းများကို မည်ကဲ့သို့ လုံခြုံစိတ်ချစွာ ထားရှိနိုင်ရန် လမ်းညွှန်ချက်များအား လိုက်နာရမည်။



Mark Wakeford
Chief Executive Officer