ပြည်ထောင်စုသမ္မတမြန်မာနိုင်ငံတော်အစိုးရ

စီမံကိန်းနှင့်ဘဏ္ဍာရေးဝန်ကြီးဌာန

ပြည်တွင်းအခွန်များဦးစီးဌာန

အီလက်ထရောနစ် သတင်းအချက်အလက် လုံခြုံမှုရှိစေရေးနှင့် အချက်အလက်ပေါက်ကြားမှု မရှိစေရေးအတွက် လိုက်နာဆောင်ရွက်ရမည့် စံပြုလုပ်ငန်းစဉ်များ

Standard Operating Procedures(SOP)

အတည်ပြုသည့်ရက်စွဲ။ ၂၀၂၂ ခုနှစ် ဇွန်လ ၁၅ ရက်

မာတိကာ

စီမံကိန်းနှင့်ဘဏ္ဍာရေးဝန်ကြီးဌာန
ပြည်တွင်းအခွန်များဦးစီးဌာန

အီလက်ထရောနစ် သတင်းအချက်အလက် လုံခြုံမှုရှိစေရေးနှင့် အချက်အလက်ပေါက်ကြားမှု မရှိစေရေးအတွက် လိုက်နာဆောင်ရွက်ရမည့် စံပြုလုပ်ငန်းစဉ်များ

(Standard Operating Procedures – SOP)

နိဒါန်း

၁။ ပြည်တွင်းအခွန်များဦးစီးဌာနရှိ ဌာနခွဲများ၊ ရုံးဌာန၊ အဖွဲ့တို့တွင် သတင်းအချက်အလက်နည်းပညာကို အသုံးပြု၍ ရုံးလုပ်ငန်းများဆောင်ရွက်ခြင်း၊ အီလက်ထရောနစ်ဝန်ဆောင်မှု (e-Services) များကို ဆောင်ရွက်ပေးခြင်း၊ အီလက်ထရောနစ်နည်းဖြင့် ဆက်သွယ်ဆောင်ရွက်ခြင်း၊ ရုံးစာမှတ်စာတမ်းအချက်အလက်များ၊ အခွန်ထမ်းများ၏ အခွန်ပေးဆောင်မှုနှင့် အခွန်စည်းကြပ်မှုဆိုင်ရာ အချက်အလက်အထောက်အထားများကို အီလက်ထရောနစ်နည်းဖြင့် သိမ်းဆည်းခြင်းတို့ လုပ်ဆောင်ရာတွင် လုံခြုံရေးကျိုးပေါက်မှုမရှိစေရေးအတွက် ဤလုပ်ထုံးလုပ်နည်းကို ထုတ်ပြန်သတ်မှတ်ရခြင်းဖြစ်ပါသည်။

ရည်ရွယ်ချက်

၂။ ပြည်တွင်းအခွန်များဦးစီးဌာနရှိ ဌာနခွဲများ၊ ရုံးဌာန၊ အဖွဲ့တို့တွင် ကွန်ပျူတာ၊ အင်တာနက်၊ အီးမေးလ်နှင့် လူမှုကွန်ရက်များအသုံးပြုရာတွင် ဌာန၏လုံခြုံမှုအဆင့်အတန်း သတ်မှတ်ချက်ရှိသော အရေးကြီးသည့် သတင်းအချက်အလက်များကို ပြင်ပသို့ပေါက်ကြားမှု မရှိစေရေးအတွက် ဆောင်ရွက်ရမည့် လုပ်ငန်းစဉ်အဆင့်ဆင့်အား သိရှိလိုက်နာစေရန်နှင့် ပြည်တွင်းအခွန်များဦးစီးဌာနရှိ Data Center များ၏ အချက်အလက်များ လုံခြုံမှုရှိစေရေး၊ မလိုလားအပ်သော ပြဿနာများမဖြစ်ပေါ်စေရေးအတွက် ကြိုတင်ကာကွယ်နိုင်ရန် ရည်ရွယ်ပါသည်။

လိုက်နာရန် အကျုံးဝင်သူများ

၃။ ပြည်တွင်းအခွန်များဦးစီးဌာနရှိ ဝန်ထမ်းများအားလုံးသည် ရုံးလုပ်ငန်းများ ဆောင်ရွက်ရာ၌ ရုံးသုံးကွန်ပျူတာများနှင့် ကိုယ်ပိုင်ကွန်ပျူတာများ အသုံးပြုရာတွင် အီလက်ထရောနစ် သတင်းအချက်အလက် လုံခြုံရေးနှင့်ပေါက်ကြားမှုမရှိစေရေးအတွက် ဤစံပြုလုပ်ငန်းစဉ်များကို လိုက်နာရန် လိုအပ်ပါသည်။

တစ်ဦးချင်းလိုက်နာရမည့် တာဝန်များ

၄။ ပြည်တွင်းအခွန်များဦးစီးဌာနရှိ ဝန်ထမ်းများအားလုံးသည် ဤလုပ်ငန်းစဉ်များအား ထိရောက်စွာ လိုက်နာဆောင်ရွက်ရန်တာဝန်ရှိပြီး အရာထမ်းများသည် လက်အောက်ဝန်ထမ်းများအား ဤလုပ်ငန်းစဉ်များ လုပ်ဆောင်ရသည့်အကြောင်းအရင်း၊ လိုက်နာဆောင်ရွက်ရန် လိုအပ်ပုံနှင့် လိုက်နာရန်ပျက်ကွက်ပါက ဝန်ထမ်းစည်းမျဉ်းစည်းကမ်း၊ တည်ဆဲဥပဒေများနှင့်အညီ အရေးယူခံရမည့်အကြောင်းအား နားလည်အောင် သေချာစွာရှင်းပြရန်တာဝန်ရှိပါသည်။ ဝန်ထမ်းများအားလုံးသည်လည်း ဤလိုက်နာဆောင်ရွက်ရမည့် စံပြုလုပ်ငန်းစဉ်များကို သေချာစွာဖတ်ရှု၍ တိကျစွာလိုက်နာဆောင်ရွက်ရန် တာဝန်ရှိပါသည်။

လိုက်နာဆောင်ရွက်ရမည့် လုပ်ငန်းစဉ်များ

၅။ ရုံးဌာနအသီးသီးရှိ အရေးကြီးသတင်းအချက်အလက်အပါအဝင် လုံခြုံမှုအဆင့် သတ်မှတ်ထားသော သတင်းအချက်အလက်များ၊ မှတ်တမ်းများ ပြင်ပသို့ပေါက်ကြားခြင်း၊ ခိုးယူခံရခြင်း၊ မသက်ဆိုင်သူများသိရှိခြင်းစသည့် လုံခြုံမှုကျိုးပေါက်သည့်ဖြစ်ရပ်များ မဖြစ်ပေါ်စေရန်အတွက် လိုက်နာဆောင်ရွက်ရမည့် လုပ်ငန်းစဉ်များကို အောက်တွင်ဖော်ပြထားပါသည်-

(က) အင်တာနက် ချိတ်ဆက်ထားခြင်းမရှိသည့် ရုံးလုပ်ငန်းသုံး ကွန်ပျူတာများအတွက် လိုက်နာဆောင်ရွက်ရမည့်အချက်များ၊

(ခ) အင်တာနက်ချိတ်ဆက်ထားသည့် ကွန်ပျူတာများအတွက် လိုက်နာဆောင်ရွက်ရမည့် အချက်များ၊

(ဂ) e-Government ကွန်ရက်စနစ်သုံး ကွန်ပျူတာများအတွက် လိုက်နာဆောင်ရွက်ရမည့် အချက်များ၊

(ဃ) E-mail ပေးပို့/လက်ခံခြင်း ဆောင်ရွက်ရာတွင် လိုက်နာဆောင်ရွက်ရမည့် အချက်များ၊

(င) Wi-Fi စနစ်ထားရှိအသုံးပြုရာတွင် လိုက်နာဆောင်ရွက်ရမည့် အချက်များ၊

(စ) အင်တာနက်အသုံးပြုသူများ လိုက်နာဆောင်ရွက်ရမည့်အချက်များ၊

(ဆ) Password များသတ်မှတ်ထားရှိရာတွင် လိုက်နာဆောင်ရွက်ရမည့်အချက်များ၊

(ဇ) Removable Devices များအသုံးပြု၍ အချက်အလက်များကူးယူရာတွင် လိုက်နာဆောင်ရွက်ရမည့်အချက်များ၊

(ဈ) Data Center လုံခြုံမှုရှိစေရေးအတွက် လိုက်နာဆောင်ရွက်ရမည့်အချက်များ၊

(ည) အချက်အလက် Data Base များကိုင်တွယ်အသုံးပြုသူများ လိုက်နာဆောင်ရွက်ရမည့် အချက်များ၊

(ဋ) ဆိုရှယ်မီဒီယာအသုံးပြုသူဝန်ထမ်းများလိုက်နာရန်စည်းကမ်းချက်များ။

အင်တာနက်ချိတ်ဆက်ထားခြင်းမရှိသည့် ရုံးလုပ်ငန်းသုံးကွန်ပျူတာများအတွက် လိုက်နာဆောင်ရွက်ရမည့်အချက်များ

၆။ ဌာနအတွင်းရှိ အင်တာနက်နှင့် ချိတ်ဆက်အသုံးပြုခြင်းမရှိဘဲ ရုံးလုပ်ငန်းများ ဆောင်ရွက်ရန် ကွန်ပျူတာများကို Standalone အနေဖြင့် သီးခြားထားရှိအသုံးပြုရာတွင် လိုက်နာရမည့် လုပ်ငန်းစဉ်များမှာ အောက်ပါအတိုင်းဖြစ်ပါသည်-

(က) Anti-Virus Software များ ထည့်သွင်းထားရှိရမည်၊

(ခ) Anti-Virus Software Version များအသစ်ထွက်ရှိပါက Upgrade ပြုလုပ်ရမည်၊

(ဂ) မိမိ၏ကွန်ပျူတာကို Off-line အသုံးပြုနေပါက Anti-Virus Update ဖိုင်များကို အင်တာနက်ရရှိသည့် စက်များမှ Download ရယူ၍ Update ပြုလုပ်ရမည်၊

(ဃ) နေ့စဉ် Virus Scan ပုံမှန်ပြုလုပ်ရမည်၊

(င) Removable Devices (Memory Sticks, External Drives, CDs, DVDs) များကို ကွန်ပျူတာနှင့် ချိတ်ဆက်၍ အသုံးပြုရာတွင် ပထမဦးစွာ Virus Scan ပြုလုပ်ပြီးမှသာ ဆက်လက်အသုံးပြုရမည်၊

(စ) Scan ဖတ်ရာ၌ Virus များပါလာသည့်အခါ ဆက်လက်အသုံးမပြုတော့ဘဲ Virus များ ရှင်းလင်းပြီးမှသာ ဆက်၍အသုံးပြုရမည်၊

(ဆ) အရေးကြီးသည့်အချက်အလက်များ သိမ်းဆည်းထားသော Standalone ကွန်ပျူတာများကို User Name နှင့် Password များ ထားရှိအသုံးပြုရမည်၊

(ဇ) သတ်မှတ်ထားသည့် Password များကို မြင်သာထင်သာရှိသည့် နေရာများတွင် (ဥပမာ Stick Notes များတွင်ရေးသား၍ ကွန်ပျူတာမျက်နှာပြင်ထောင့် သို့မဟုတ် ခုံပေါ်တွင်) ကပ်ထားခြင်းများ မပြုလုပ်ဘဲ တာဝန်ရှိသူမှ စနစ်တကျ လုံခြုံစွာ သိမ်းဆည်းအသုံးပြုရမည်၊

(ဈ) ကွန်ပျူတာအသုံးပြုရာ၌ မည်သူ့ကို မည်သည့်လုပ်ငန်းစဉ်များ လုပ်ဆောင်ရမည်ဆိုသည့် Permission များ သတ်မှတ်ပေးရမည်၊

(ည) အသုံးပြုမည့် ဝန်ထမ်းများအတွက် Priority အဆင့်များ သတ်မှတ်ပေးရမည်၊

(ဋ) အချက်အလက်များကို သိမ်းဆည်းရာ၌ ကွန်ပျူတာ၏ OS တင်ထားသော Partition (ဥပမာ- Desktop, C:\) တို့တွင် သိမ်းဆည်းခြင်းမပြုလုပ်ဘဲ အခြား Partition (ဥပမာ- D:\, Z:\) တို့တွင်သာ သိမ်းဆည်းရမည်။

အင်တာနက်ချိတ်ဆက်ထားသည့် ကွန်ပျူတာများအတွက် လိုက်နာဆောင်ရွက်ရမည့်အချက်များ

၇။ ရုံးလုပ်ငန်းများဆောင်ရွက်နိုင်ရန် အင်တာနက်ချိတ်ဆက်ထားသည့် ကွန်ပျူတာများ အသုံးပြုရာတွင် လိုက်နာဆောင်ရွက်ရမည့် လုပ်ငန်းစဉ်များမှာ အောက်ပါအတိုင်း ဖြစ်ပါသည်-

(က) Anti-Virus Software များ ထည့်သွင်းထားရှိရမည်၊

(ခ) Anti-Virus Software Version များ အသစ်ထွက်ရှိပါက Upgrade ပြုလုပ်ရမည်၊

(ဂ) နေ့စဉ် Virus Scan ပုံမှန်ပြုလုပ်ရမည်၊

(ဃ) Removable Devices (Memory Sticks, External Drives, CDs, DVDs) များကို ကွန်ပျူတာနှင့်ချိတ်ဆက်၍ အသုံးပြုရာတွင် ပထမဦးစွာ Virus Scan ပြုလုပ်ပြီးမှသာ ဆက်လက်အသုံးပြုရမည်၊

(င) Scan ဖတ်ရာ၌ Virus များပါလာသည့်အခါ ဆက်လက်အသုံးမပြုတော့ဘဲ Virus များ ရှင်းလင်းပြီးမှသာ ဆက်၍အသုံးပြုရမည်၊

(စ) Windows Firewall အား Turn on ပြုလုပ်ထားရမည်၊

(ဆ) Licensed OS အသုံးပြုပါက Windows Update ပုံမှန် ပြုလုပ်ရမည်၊

(ဇ) ကွန်ပျူတာ၏ Network Discovery နှင့် File and Printer Sharing များကို Turn Off ပြုလုပ်ထားရမည်၊

(စျ) ရုံးလုပ်ငန်းနှင့် မသက်ဆိုင်သည့် Website များသို့ ဝင်ရောက်ကြည့်ရှု သုံးစွဲနိုင်သည့် Software များ အသုံးမပြုနိုင်စေရေး ကြပ်မတ်ဆောင်ရွက်ရမည်၊

(ည) ရုံးလုပ်ငန်းနှင့်မသက်ဆိုင်သည့် Website များ၊ Social Media များအသုံးပြုခြင်းနှင့် Download ပြုလုပ်ခြင်းများ ဆောင်ရွက်မှုမရှိစေရေး ကြပ်မတ်ဆောင်ရွက်ရမည်။

e-Government ကွန်ရက်စနစ်သုံး ကွန်ပျူတာများအတွက် လိုက်နာဆောင်ရွက်ရမည့်အချက်များ

၈။ ပြည်တွင်းအခွန်များဦးစီးဌာနအနေဖြင့် ပြည်ထောင်စုဝန်ကြီးရုံးနှင့် အခြားဦးစီးဌာနများသို့ အချင်းချင်း ချိတ်ဆက်ဆောင်ရွက်နေသည့် e-Government ကွန်ယက်စနစ်သုံး ကွန်ပျူတာများ အသုံးပြုရာတွင် လိုက်နာဆောင်ရွက်ရမည့် လုပ်ငန်းစဉ်များမှာ အောက်ပါအတိုင်းဖြစ်ပါသည်-

(က) Anti-Virus Software များ ထည့်သွင်းထားရှိရမည်၊

(ခ) Anti-Virus Software Version များ အသစ်ထွက်ရှိပါက Upgrade ပြုလုပ်ရမည်၊

(ဂ) နေ့စဉ် Virus Scan ပုံမှန်ပြုလုပ်ရမည်၊

(ဃ) Removable Devices (Memory Sticks, External Drives, CDs, DVDs) များကို ကွန်ပျူတာနှင့် ချိတ်ဆက်၍ အသုံးပြုရာတွင် ပထမဦးစွာ Virus Scan ပြုလုပ်ပြီးမှသာ ဆက်လက်အသုံးပြုရမည်၊

(င) Scan ဖတ်ရာ၌ Virus များပါလာသည့်အခါ ဆက်လက်အသုံးမပြုတော့ဘဲ Virus များ ရှင်းလင်းပြီးမှသာ ဆက်၍အသုံးပြုရမည်၊

(စ) အခြားသော ဝန်ကြီးဌာနများနှင့် ဦးစီးဌာနများသို့ ဝင်စာ/ ထွက်စာများ ပေးပို့/ လက်ခံ ဆောင်ရွက်ရာတွင် အသုံးပြုလျက်ရှိသော EDMS စနစ်ထည့်သွင်းထားသည့် ကွန်ပျူတာ အား Username နှင့် Password များ ထားရှိအသုံးပြုရမည်၊

(ဆ) e-Government ကွန်ရက်ချိတ်ဆက်ထားသောကွန်ပျူတာအား အခြားကွန်ယက်များနှင့် ချိတ်ဆက်အသုံးပြုခြင်းကို ရှောင်ကြဉ်ရမည်၊

(ဇ) e-Government လုပ်ငန်းများနှင့် သက်ဆိုင်မှုမရှိသည့် Social Media များနှင့် Website များကို ဝင်ရောက်ကြည့်ရှုခြင်းမရှိစေရန် အထူးကြပ်မတ် ဆောင်ရွက်ရမည်၊

(ဈ) Electronic Document Management System (EDMS) စနစ်ဖြင့် ပေးပို့လာသော စာများအား မှတ်ပုံတင်စာအုပ်များထားရှိ၍ သေချာစွာသိမ်းဆည်းထားရမည်ဖြစ်ပြီး Soft Copy များအား နေ့အလိုက် သီးခြား Folder များဆောက်၍ စနစ်တကျ သိမ်းဆည်း ထားရမည်။

E-mail ပေးပို့/လက်ခံခြင်း ဆောင်ရွက်ရာတွင် လိုက်နာဆောင်ရွက်ရမည့်အချက်များ

၉။ လုံခြုံမှုအဆင့်အတန်းမပါသည့် ဝန်ကြီးဌာနတွင်း စာပေး/ စာယူကိစ္စရပ်များကို E-mail စနစ်ဖြင့် ပေးပို့/လက်ခံဆောင်ရွက်လျက်ရှိရာတွင် လုံခြုံမှုကျိုးပေါက်သည့်ဖြစ်ရပ်များ မဖြစ်ပေါ်စေရန်အတွက် စီမံကိန်းနှင့်ဘဏ္ဍာရေးဝန်ကြီးဌာန၊ ပြည်ထောင်စုဝန်ကြီးရုံး ၏ ၃၀-၉-၂၀၂၁ ရက်စွဲပါစာအမှတ်၊ စဘ/ စီမံ-eGov/ ၃၆ (၇၀/၂၀၂၁) ဖြင့် ပေးပို့ညွှန်ကြားထားသော E-mail ပေးပို့/လက်ခံခြင်းလုပ်ငန်းလမ်းညွှန်ပါ အောက်ဖော်ပြပါအချက်များကို လိုက်နာဆောင်ရွက်ရမည်-

(က) E-mail ပေးပို့မည့် လိပ်စာ To နေရာတွင် ပေးပို့လိုသော ဌာန/ အဖွဲ့အစည်းများ၏ လိပ်စာများကို ထည့်သွင်းရမည်၊

(ခ) CC နေရာတွင် မိတ္တူပေးပို့လိုသော ဌာန/အဖွဲ့အစည်းများ၏ လိပ်စာများကို ထည့်သွင်း ရမည်၊

(ဂ) E-mail ၏ Subject တွင် မိမိပေးပို့သော ရုံးစာ (အမှာစာ)၏ အကြောင်းအရင်းတွင် ပါရှိသည့် အချက်များကို ပြည့်စုံစွာ ဖော်ပြရမည်၊

(ဃ) E-mail ၏ Body နေရာတွင် မိမိပေးပို့သော ရုံးစာပါ အချက်အလက်အကျဉ်းချုပ်နှင့် ပြန်ကြားပေးရန် နောက်ဆုံးတောင်းခံသည့် ရက်စွဲပါရှိပါက ၎င်းရက်စွဲတို့ကို ဖော်ပြ ရမည်၊

(င) E-mail Body ၏ အောက်တွင် စုံစမ်းမေးမြန်းရန် သက်ဆိုင်ရာ တာဝန်ခံ၏ အမည်၊ ရာထူး၊ ဌာနခွဲ၊ ဌာန၊ ရုံးဖုန်း၊ လက်ကိုင်ဖုန်းတို့ကို ဖော်ပြရမည်၊

(စ) E-mail Disclaimer ကို E-mail ၏ အောက်ဆုံးတွင် ဖော်ပြရမည် (ဥပမာ၊ ဤစာပါ အကြောင်းအရာများသည် စီမံကိန်းနှင့် ဘဏ္ဍာရေးဝန်ကြီးဌာန ရုံးကိစ္စများ ဖြစ်ပါသည်၊ အကယ်၍ ချွတ်ယွင်းမှုတစ်ခုခုကြောင့် သင့်ထံ ပေးပို့ခြင်းမဟုတ်ဘဲ လက်ခံရရှိခြင်းဖြစ်လျှင် ကျေးဇူးပြု၍ E-mail ပြန်ခြင်းဖြင့် အကြောင်းကြားပါ၊ ထို့နောက် စာကိုဖျက်ပါ၊ ဤစာပါအကြောင်းအရာများကို မသက်ဆိုင် သည့်သူ မည်သူ့ကိုမဆို မည်သည့်နည်းနှင့်မဆို ကူးယူခြင်း၊ Forward ပေးပို့ခြင်း၊ သိရှိစေရန် ဆောင်ရွက်ခြင်း မပြုလုပ်ရန်)၊

(ဆ) EDMS E-mail ၊ ဦးစီးဌာန/ လုပ်ငန်း/ အဖွဲ့အစည်းအလိုက် အကောင်အထည်ဖော် ဆောင်ရွက်လျက်ရှိသည့် E-mail စသည့် E-mail အမျိုးအစားတစ်ခုခုဖြင့် ပေးပို့/ လက်ခံသည့် စာကို ဦးစီးဌာန/ လုပ်ငန်း/ အဖွဲ့အစည်း၏ တရားဝင်ပေးပို့/လက်ခံသော ရုံးစာအဖြစ်မှတ်ယူရမည်၊

(ဇ) ရုံးဖွင့်ရက်တွင် E-mail ပေးပို့ပြီး (၂၄) နာရီကျော်သည်အထိ လက်ခံမည့်သူဘက်မှ လက်ခံရရှိကြောင်း ပြန်ကြားခြင်းမရှိပါက E-mail ရရှိကြောင်းပြန်ကြားပေးရန် ဆက်သွယ် အကြောင်းကြားရမည်၊

(ဈ) ရုံးပိတ်ရက်တွင် E-mail ပေးပို့ခြင်းဖြစ်ပါက ရုံးဖွင့်ရက်သို့ရောက်ရှိပြီး (၂၄) နာရီ ကျော်သည်အထိ လက်ခံမည့်သူဘက်မှ လက်ခံရရှိကြောင်း ပြန်ကြားခြင်းမရှိပါက E-mail ရရှိကြောင်းပြန်ကြားပေးရန် ဆက်သွယ်အကြောင်းကြားရမည်၊

(ည) ပေးပို့သည့်စာ၏ ဦးစားပေးအဆင့်အတန်းပေါ်မူတည်၍ E-mail ရရှိကြောင်းပြန်ကြား ပေးရန် ဆက်သွယ်အကြောင်းကြားရမည်၊

(ဋ) ပေးပို့ထားသော E-mail ကို သက်ဆိုင်ရာ E-mail လက်ခံသည့် ပုဂ္ဂိုလ် (သို့) ဌာနက E-mail လက်ခံရရှိခြင်းမရှိပါက ယခင်ပေးပို့ထားသော E-mail ကို Forward ပေးပို့ရမည်၊

(၄) လက်ခံမည့် E-mail address မှားယွင်းခြင်းမရှိပါက ပထမအကြိမ်ပို့လွှတ်သည့် E-mail ပေးပို့သည့်အချိန်ကို ရုံးစာ ပေးပို့သည့်အချိန်ဟုမှတ်ယူရန်နှင့် E-mail address မှားယွင်းပေးပို့မိသဖြင့် ထပ်မံပေးပို့ရပါက ထပ်မံ E-mail ပေးပို့သည့် အချိန်ကို ရုံးစာ ပေးပို့သည့် အချိန်ဟု မှတ်ယူရမည်၊

(၅) Attach File Size ကြီးမားနေပါက Win RAR ကို အသုံးပြု၍ ဖိုင်များခွဲ၍ ပေးပို့မည့် ဖိုင်အရေအတွက် (Email အစောင်ရေ)ကို ပထမဆုံး Email တွင် ဖော်ပြပေးပို့ရန် (သို့) Drive Share Function ပါရှိပါက Drive Share အသုံးပြုပေးပို့ရမည်၊

(၆) ပေးပို့မည့် အမှာစာကို Color Scan ဖတ်၍ pdf File Format (*.pdf) ဖြင့် Attach တွဲရန်နှင့် Editable Format (Microsoft Word, Excel, etc…) ရှိပါက ၎င်းတို့ကိုပါ လက်ခံမည့်ဌာနမှ လိုအပ်ပါက တစ်ပါတည်း Attach တွဲပေးပို့ရမည်၊

(၇) ရုံးဖွင့်ရက်များ၌ E-mail တွင် စာဝင်ရောက်ခြင်း ရှိ/မရှိ တစ်ရက်လျှင် အနည်းဆုံး (၃)ကြိမ် ကြည့်ရှုစစ်ဆေးပြီး စာများ ဝင်ရောက်ပါက လက်ခံရရှိကြောင်း ပေးပို့သည့် E-mail တွင် Reply ပြန်ကြားရမည်၊

(တ) E-mail ပေးပို့ထားသူက ဆက်သွယ်အကြောင်းကြားလာလျှင် E-mail တွင် စာဝင်ရောက်မှု ရှိ/မရှိ စစ်ဆေး၍ E-mail လက်ခံရရှိမှု အခြေအနေကို ပေးပို့သည့် E-mail တွင် reply ပြန်ကြားရမည်၊

(ထ) မိမိထံသို့ ပေးပို့ရမည့် စာမဟုတ်ပါက မိမိထံသို့ ပေးပို့ရမည့် စာမဟုတ်ကြောင်း၊ ပေးပို့ရမည့် E-mail ကို သိရှိပါက ပေးပို့ရန် E-mail ကို ပြန်ကြားရန် (သို့) ဌာနတွင်း ဖြစ်ပါက သက်ဆိုင်ရာ E-mail သို့ Forward ပေးပို့ထားကြောင်း ပေးပို့သည့် E-mail တွင် reply ပြန်ကြားရမည်၊

(ဒ) လက်ခံရရှိသော E-mail တွင် ပူးတွဲ (Attach) ဖိုင်များ မပါရှိခြင်း (သို့) (Attach)ဖိုင်များ ကျန်ရှိပါက Attach ဖိုင်များ ထပ်မံပေးပို့ရန် ပေးပို့သည့် E-mail တွင် Reply ပြန်ကြား ရမည်၊

(ဓ) အမှာစာတွင် ပါဝင်သည့် အချက်အလက်များ (Attach ဖိုင်များ) ပြည့်စုံစွာ လက်ခံ ရရှိသည့် အချိန်ကို ရုံးစာလက်ခံရရှိသည့် အချိန်ဟု မှတ်ယူရမည်၊

(န) အမှာစာတွင် ပါဝင်သည့် အချက်အလက်များ (Attach ဖိုင်များ) ပြည့်စုံစွာ လက်ခံ ရရှိကြောင်း E-mail Reply ပြန်ကြားပြီးနောက် Document Database Management System တွင် Register ရေးသွင်းရမည်၊

(ပ) E-mail ဝင်ရောက်မှုကို အဟန့်အတားမဖြစ်စေရန် E-mail Storage တွင် အနည်းဆုံး 3GB Free Space ဖြစ်နေစေရေး စီစဉ်ထားရှိရမည်၊

(ဖ) မိမိထံပေးပို့သည့် E-mail လိပ်စာသည် သက်ဆိုင်ရာ ဦးစီးဌာန/လုပ်ငန်း/အဖွဲ့အစည်း မှပေးပို့ခြင်းဖြစ်ကြောင်း သေချာဂရုပြုစစ်ဆေးပြီးမှ E-mail ပါ Link များ၊ ပူးတွဲပါ (Attach) ဖိုင်များအား ကြည့်ရှုရမည်၊

(ဗ) E-mail Account များ၏ Password များကို လုံခြုံရေးအရ (၃) လ (ရက် ၉၀) လျှင် တစ်ကြိမ်ပုံမှန်အပြောင်းအလဲပြုလုပ်ပေး(Password Change)ရမည်၊

(ဘ) E-mail Account ကို အသုံးပြုပြီးသည့်အခါ Sign Out ပြုလုပ်ရာတွင် စနစ်တကျ စောင့်ကြည့်ပြီးမှ ထွက်ရမည် (တခါတရံ အင်တာနက်လိုင်းကြောင့် Sign Out Process Complete မဖြစ်ဘဲ Browser ကိုပိတ်လိုက်သည့်အခါ နောက်တကြိမ် ပြန်ဝင်သည့်အခါ Auto Sign in ဖြစ်နိုင်ပါသည်)၊

(မ) E-mail Password ကို သင်္ကေတများ၊ ဂဏန်းများ၊ အက္ခရာအကြီးအသေးများ ပေါင်းစပ်၍ အနည်းဆုံး (၈) လုံးပေးရမည်၊ (ဥပမာ။ ဖ@QPw07)၊ E-mail Password များကို ကိုယ်ရေးကိုယ်တာနှင့် သက်ဆိုင်သော အချက်အလက်များ (တယ်လီဖုန်းနံပါတ်များ၊ မွေးနေ့ရက်စွဲများ၊ လိပ်စာများ) မပေးရ၊ E-mail Account များ၏ Password များကို Browser များတွင် Save Password မပြုလုပ်ရ၊

(ယ) E-mail Account များကို မည်သည့် Commercial Website များ၊ ဈေးကွက်ဆိုင်ရာ ဆိုရှယ်ကွန်ရက်များ သို့မဟုတ် အလားတူကိစ္စရပ်များတွင် Subscribe မပြုလုပ်ရ၊

(ရ) ဌာနများ၏ Official E-mail Account ဖြင့် ဆိုရှယ်မီဒီယာ Account များ ဖန်တီးခြင်း မပြုလုပ်ရ၊

(လ) E-mail Account များ၏ Password များဖြင့် လုပ်ငန်းနှင့် မသက်ဆိုင်သည့် Link များ အတွင်းသို့ ဝင်ရောက်ခြင်းမပြုရ၊

(ဝ) Personal Information များကို ရုံးလုပ်ငန်းအတွက်အသုံးပြုသော E-mail များတွင် သိမ်းဆည်းထားခြင်း မပြုလုပ်ရ၊

(သ) Official E-mail ကို အသုံးပြု၍ လုပ်ငန်းနှင့်မသက်ဆိုင်သည့် အကြောင်းအရာများ ပေးပို့/လက်ခံခြင်းများ မပြုလုပ်ရ၊

(ဟ) Official E-mail ကိုအသုံးပြုရန် ခွင့်ပြုပေးပိုင်ခွင့်ရှိသူ၏ ခွင့်ပြုချက်မရရှိဘဲ အခြားဝန်ထမ်းများကို အသုံးပြုခွင့်မပြုရ၊

(ဠ) အခွန်ရုံးများအနေဖြင့် မိမိအခွန်ထမ်းများသို့ အခွန်ဆိုင်ရာကိစ္စများအတွက် နှိုးဆော်အသိပေးအကြောင်းကြားခြင်း၊ အခွန်ပညာပေးဆွေးနွေးပွဲများဖိတ်ကြားခြင်းစသည့် အလားတူကိစ္စများကို အီလက်ထရောနစ်နည်းဖြင့် ဆက်သွယ်ဆောင်ရွက်သည့်အခါ ကုမ္ပဏီတစ်ခုချင်းစီအလိုက် ပေးပို့ဆောင်ရွက်ရန် အချိန်ကြာမြင့်သဖြင့် သမားရိုးကျ E-mail ပေးပို့ရသည့်ကိစ္စများတွင် လိပ်မူ To နေရာတွင် E-mail Address အားလုံးထည့်သွင်း၍ ပေးပို့ခြင်း (သို့မဟုတ်) မိတ္တူ CC ဖြင့် ပေးပို့ကြသည်။ E-mail လက်ခံရရှိသူအခွန်ထမ်း (သို့မဟုတ်) ယင်း၏ ကိုယ်စားလှယ်အနေဖြင့် မိမိနှင့်အတူပေးပို့ထားသည့် အခြားမသက်ဆိုင်သည့် အခွန်ထမ်း E-mail Address များကိုပါ သိရှိနိုင်သဖြင့် ကိုယ်ကျင့်သိက္ခာအားနည်းသည့် အခွန်ထမ်းတစ်ဦး၏ ဝန်ထမ်းတစ်စုံတစ်ယောက်ကြောင့် မသမာမှုဖြစ်စဉ်များ၊ ခြိမ်းခြောက်စာပေးပို့ခဲ့မှုဖြစ်စဉ်များ စသည့် လုံခြုံရေးကျိုးပေါက်မှုဖြစ်စဉ်များကို ကာကွယ်နိုင်ရန် လက်ရှိအသုံးပြုလျက်ရှိသော Gmail စနစ်သည် Personal Mail အစား လုံခြုံစွာ စုပေါင်းပေးပို့နိုင်သည့် (Mail Merge) လုပ်ဆောင်ချက်ဖြင့် ပေးပို့လိုသည့် ကုမ္ပဏီများအားလုံး၏ E-mail User အများအပြားကို တစ်ပြိုင်တည်းပေးပို့ ဆောင်ရွက်ရမည်။

Wi-Fi စနစ်ထားရှိအသုံးပြုရာတွင် လိုက်နာဆောင်ရွက်ရမည့် အချက်များ

၁၀။ ဌာနခွဲများတွင် အင်တာနက်ချိတ်ဆက်အသုံးပြု၍ ရုံးလုပ်ငန်းများ အဆင်ပြေချောမွေ့စွာ ဆောင်ရွက်နိုင်ရန်အတွက် Wi-Fi စနစ်များ တပ်ဆင်အသုံးပြုရာတွင် လိုက်နာဆောင်ရွက်ရမည့် လုပ်ငန်းစဉ်များမှာ အောက်ပါအတိုင်းဖြစ်ပါသည်-

(က) Wi-Fi စနစ်ထားရှိအသုံးပြုမှုအတွက် တာဝန်ခံအရာရှိကသာလျှင် Admin အဖြစ် ထိန်းချုပ်စီမံရမည်၊

(ခ) ဌာနခွဲများအလိုက်အသုံးပြုလျက်ရှိသော Wi-Fi များ၏ Password များကို မသက်ဆိုင်သူများ အသုံးမပြုနိုင်စေရေး ကြိုးကြပ်ဆောင်ရွက်ရမည်၊

(ဂ) Wi-Fi Password များအား (၃) လလျှင် တစ်ကြိမ်ခန့် အသစ်ပြောင်းလဲ အသုံးပြုရမည်၊

(ဃ) သတ်မှတ်ထားသော သက်ဆိုင်ရာ Wi-Fi များ၏ Password များကို မှတ်တမ်းစာအုပ်ပြုလုပ်၍ စနစ်တကျ ဖိုင်တွဲထားရှိရမည်။

အင်တာနက်အသုံးပြုသူများ လိုက်နာဆောင်ရွက်ရမည့်အချက်များ

၁၁။ ရုံးလုပ်ငန်းများအဆင်ပြေချောမွေ့စွာ ဆောင်ရွက်နိုင်ရန်အတွက် အင်တာနက်ချိတ်ဆက်အသုံးပြုရာတွင် ဌာန၏အရေးကြီးအချက်အလက်များ ပြင်ပသို့ပေါက်ကြားမှုမရှိစေရန်နှင့် လုံခြုံမှုရှိစေရန် အင်တာနက်အသုံးပြုသူများအနေဖြင့် လိုက်နာဆောင်ရွက်ရမည့် လုပ်ငန်းစဉ်များမှာ အောက်ပါအတိုင်းဖြစ်ပါသည်-

(က) ရုံးလုပ်ငန်းနှင့်မသက်ဆိုင်သည့် Social Media များ၊ Website များ အသုံးပြုခြင်းနှင့် Download ပြုလုပ်ခြင်းများ ဆောင်ရွက်မှုမရှိစေရေး ကြပ်မတ်ဆောင်ရွက်ရမည်၊

(ခ) ရုံးနှင့်သက်ဆိုင်သည့် စာရွက်စာတမ်းများ၊ ဓာတ်ပုံများကို Social Media များပေါ်သို့ ခွင့်ပြုချက်မရဘဲ Upload ပြုလုပ်ခြင်းများ ဆောင်ရွက်မှုမရှိစေရေး အထူးကြပ်မတ်ဆောင်ရွက်ရမည်၊

(ဂ) အရေးကြီးအချက်အလက်များကို Online မှတစ်ဆင့် ပေးပို့/လက်ခံရာတွင် Password များ ထားရှိဆောင်ရွက်ရမည်၊

(ဃ) အင်တာနက်ချိတ်ဆက်အသုံးပြုသည့် ကွန်ပျူတာများအတွက် သတ်မှတ်ထားသော လုပ်ငန်းစဉ်များအား မပျက်မကွက် ဆောင်ရွက်ရမည်၊

(င) အများပြည်သူများအတွက် ဖွင့်လှစ်ထားသည့် အင်တာနက်ကဖေးများနှင့် အခြားနေရာများတွင် အသုံးပြုသောကွန်ပျူတာများတွင် မိမိဌာန၏ အရေးကြီးအချက်အလက်များ ထည့်သွင်းခြင်းကို ရှောင်ကြဉ်ရမည်၊

(စ) မိမိဌာနတွင်ရှိသော သတင်းအချက်အလက်များနှင့် Network Structure များကို တာဝန်ရှိသူ၏ခွင့်ပြုချက်မပါဘဲ ယူဆောင်ခြင်း၊ လွှဲပြောင်းခြင်းတို့မှ ရှောင်ကြဉ်ရမည်၊

(ဆ) ပြင်ပမှပေးပို့လာသော email များသည် မိမိဌာနအတွက် သေချာခြင်းမရှိလျှင် ၎င်း email များအား Reply မပြန်မီ ဖုန်းဖြင့်ဆက်သွယ်၍ မေးမြန်းစုံစမ်းရမည်၊

(ဇ) သံသယဖြစ်ဖွယ် email များမှတစ်ဆင့် ပေးပို့လာသည့် File များကိုဖွင့်ခြင်း၊ Link များကို Click နှိပ်ခြင်း၊ အချက်အလက်များ ဖြည့်သွင်းခြင်း၊ ထပ်မံဖြန့်ဝေခြင်းများမှ ရှောင်ကြဉ်ရမည်၊

(ဈ) email သို့မဟုတ် ဌာန၏ အခြားစနစ်များကို အသုံးပြုရာတွင် Password များအား devices များတွင် Browsers များ၌ သိမ်းဆည်းထား၍ အလွယ်တကူ ဝင်ရောက်

သုံးစွဲခြင်း မပြုလုပ်ရန်နှင့် ဝင်ရောက်သုံးစွဲပြီးပါက User Account များ၊ စနစ်များ၊ Devices များမှ စနစ်တကျ Log Out ပြုလုပ်ရမည်၊

(ည) ရုံးတွင်း Network နှင့်ကွန်ပျူတာများအား ထိခိုက်စေနိုင်သည့် အန္တရာယ်ရှိသော Website များသို့ ဝင်ရောက်ကြည့်ရှုခြင်းများ မပြုလုပ်ရန် အထူးကြပ်မတ် ဆောင်ရွက်ရမည်၊

(ဋ) Online မှတစ်ဆင့်ရရှိလာသော Installation File (Software/ Application/ .exe file) များကို Install ပြုလုပ်ခြင်းမှ ရှောင်ကြဉ်ရမည်။

လျှို့ဝှက်စကားလုံးများ(Passwords)သတ်မှတ်ထားရှိရာတွင် လိုက်နာဆောင်ရွက်ရမည့် အချက်များ

၁၂။ ကွန်ပျူတာစနစ်များ/ ပစ္စည်းကိရိယာများကို အသုံးပြုနိုင်စေရန်နှင့် သတင်းအချက်အလက်များကို အခွင့်မရှိဘဲ ရယူအသုံးပြုခြင်းမှ ကာကွယ်ရန်၊ စနစ်များ/ ပစ္စည်းကိရိယာများအားလုံးအတွက် အသုံးပြုသူအမည် (user ids)နှင့် လျှို့ဝှက်စာလုံးများကို အသုံးပြုသင့်ပါသည်။ အသုံးပြုမှုဆိုင်ရာ လုံခြုံရေးထိန်းချုပ်မှု(security access control)သည် ခွင့်ပြုချက်မရသောအသုံးပြုမှုမှ အဓိက ကာကွယ်ပေးသည်။ မိမိတို့သည် စနစ်တစ်ခုစီအတွက် သီးခြားတစ်ခုတည်းဖြစ်သော၊ ကောင်းစွာ တည်ဆောက်ထားသော လျှို့ဝှက်စကားလုံးတစ်ခုကို ရွေးချယ်ရန် အလွန်အရေးကြီးသည်။ လျှို့ဝှက်စကားလုံး Password များဖန်တီးရာတွင် လိုက်နာဆောင်ရွက်ရမည့် လုပ်ငန်းစဉ်များမှာ အောက်ပါအတိုင်း ဖြစ်ပါသည်-

(က) အရေးကြီးသည့်အချက်အလက်များ ပေါက်ကြားမှုမရှိစေရန်နှင့် လုံခြုံမှုရှိစေရန်အတွက် သူတစ်ပါးအလွယ်တကူမခန့်မှန်းနိုင်သော Password များထားရှိရမည်၊

(ခ) လျှို့ဝှက်စကားလုံး Password များထားရှိရာတွင် Special Character (ဥပမာ- ! , @ , # , $, & စသည်) များ၊ Number များ၊ Small letter နှင့် Capital letter များအပါအဝင် အက္ခရာ၊ ကိန်းဂဏန်းနှင့် အထူးစာလုံးတို့ ပေါင်းစပ်ပါဝင်သည့် အနည်းဆုံး (၈) လုံး ထားရှိရမည်၊ သို့ရာတွင် စာလုံး (၈) လုံးထက်ပို၍ အသုံးပြုခြင်းသည် ပိုမိုလုံခြုံမှုရှိစေပါသည်၊

(ဂ) Dictionary ထဲတွင် ပါဝင်သော စကားလုံးများကို Password အဖြစ် အသုံးပြုခြင်းမှ ရှောင်ကြဉ်ရမည်၊

(ဃ) Repetitive and Sequential Character များကို Password အဖြစ် အသုံးပြုခြင်းမှ ရှောင်ကြဉ်ရမည်၊

(ဂ) ဌာနအမည် သို့မဟုတ် ဌာနခွဲအမည်များကို Password အဖြစ် အသုံးပြုခြင်းမှ ရှောင်ကြဉ်ရမည်၊

(စ) တယ်လီဖုန်းနံပါတ်များ၊ မွေးနေ့ရက်စွဲများ၊ မှတ်ပုံတင်နံပါတ်များ၊ Credit Card နံပါတ်များနှင့် လိပ်စာများ မိသားစုဝင်များ၏ အမည်များ၊ အိမ်မွေးတိရစ္ဆာန်များ၊ ဝါသနာများ၊ စားပွဲပေါ်ရှိပစ္စည်းများ အစရှိသည်တို့ကို Password အဖြစ် အသုံးပြုခြင်းမှ ရှောင်ကြဉ်ရမည်၊

(ဆ) Password များကို သုံးလတစ်ကြိမ် မဖြစ်မနေ ပြောင်းလဲပေးရမည်၊

(ဇ) Password များမပေါက်ကြားစေရန်အတွက် သတ်မှတ်ထားသည့် Password များကို မြင်သာထင်သာရှိသည့် နေရာများတွင် (ဥပမာ Stick Notes များတွင် ရေးသား၍ ကွန်ပျူတာမျက်နှာပြင်ထောင့် သို့မဟုတ် ခုံပေါ်တွင်) ကပ်ထားခြင်းများ၊ Password File များအား အများမြင်သာစေသည့် နေရာများတွင် အလွယ်တကူသိမ်းဆည်းထားခြင်းများ မပြုလုပ်ဘဲ တာဝန်ခံအရာရှိမှ စနစ်တကျ လုံခြုံစွာသိမ်းဆည်းအသုံးပြုရမည်၊

(ဈ) လျှို့ဝှက်စကားလုံးကို လျှို့ဝှက်ထားပါ၊ မည်သူနှင့်မျှ ဝေမျှခြင်း မပြုပါနှင့်၊

(ည) လျှို့ဝှက်စကားလုံးကို မည်သည့်နေရာတွင်မှ မရေးသားထားပါနှင့်၊ မိမိ၏ မှတ်ဉာဏ်အတွင်းတွင်သာ သိမ်းဆည်းထားပါ၊

(ဋ) ကွန်ပျူတာအနီးမှ ထွက်ခွာပါက အမြဲတစေ ကွန်ပျူတာကို log off လုပ်ပါ၊ အသုံးမပြုတော့သည့် စနစ်အပိုင်းများ(systems sessions) ကို မှန်ကန်စွာပိတ်ပါ၊

(ဌ) လျှို့ဝှက်စကားလုံး ဖော်ထုတ်ခံရသည်ဟုထင်ပါက သင်၏ လျှို့ဝှက်စကားလုံးကို ချက်ချင်းပြောင်းပါ။

Removable Devices များအသုံးပြု၍ အချက်အလက်များကူးယူရာတွင် လိုက်နာဆောင်ရွက်ရမည့် အချက်များ

၁၃။ ရုံးလုပ်ငန်းများဆောင်ရွက်ရာ၌ Removable Devices များအသုံးပြု၍ အချက်အလက်များကူးယူလေ့ရှိရာ Virus ဝင်ရောက်မှုများနှင့် အချက်အလက်များဆုံးရှုံးမှု၊ ပေါက်ကြားမှုများမဖြစ်ပေါ်စေရန် လိုက်နာဆောင်ရွက်ရမည့် လုပ်ငန်းစဉ်များမှာ အောက်ပါအတိုင်းဖြစ်ပါသည်-

(က) အချက်အလက်များ ကူးယူရာ၌ Removable Devices (Memory Sticks, External Drives, CDs, DVDs) များကို ကွန်ပျူတာနှင့်ချိတ်ဆက်၍ အသုံးပြုရာတွင် ပထမဦးစွာ Virus Scan ပြုလုပ်ပြီးမှသာ ဆက်လက်အသုံးပြုရမည်၊

(ခ) Scan ဖတ်ရာ၌ Virus များပါလာသည့်အခါ ဆက်လက်အသုံးမပြုတော့ဘဲ Virus များ ရှင်းလင်းပြီးမှသာ ဆက်၍အသုံးပြုရမည်၊

(ဂ) အချက်အလက်များကူးယူရာတွင် ဖိုင်များအား Password ဖြင့် Encrypt ပြုလုပ်ပြီး မှသာ ကူးယူရမည်၊

(ဃ) အချက်အလက်များအား ကူးယူပြီးသည့်အခါ Removable Devices ထဲတွင် ဆက်လက် ထားရှိခြင်းမပြုဘဲ ဖိုင်များအား ဖျက်ပစ်ရမည်၊

(င) ဌာနတစ်ခုမှတစ်ခုသို့ အချက်အလက်များ ပေးပို့ရန်လိုအပ်သည့်အခါ Password ဖြင့် Encrypt ပြုလုပ်၍ ၎င်းအချက်အလက်များ အသုံးပြုမည့်သူထံသို့ Password အား တိုက်ရိုက်ပေးပို့ အသုံးပြုရမည်။

Data Center ရှိ သတင်းအချက်အလက်များ လုံခြုံမှုရှိစေရေးအတွက် လိုက်နာဆောင်ရွက်ရမည့် အချက်များ

၁၄။ ပြည်တွင်းအခွန်များဦးစီးဌာန၏ Data Center နှင့်သက်ဆိုင်သည့် အချက်အလက်များ လုံခြုံမှု ရှိစေရေးအတွက် ဆောင်ရွက်ရမည့်လုပ်ငန်းများမှာ အောက်ပါအတိုင်းဖြစ်ပါသည်-

(က) Data Center နှင့် သက်ဆိုင်သည့်သော့များကို သက်ဆိုင်ရာ တာဝန်ခံအရာရှိမှ စနစ်တကျ ထိန်းသိမ်းထားရှိရမည်၊

(ခ) Data Center သို့ဝင်ရောက်ရန်အတွက် ဝင်ခွင့်ကတ်များ၊ Finger Print များ၊ Password များကို တာဝန်ရှိသူများအတွက်သာ သတ်မှတ်ပြုလုပ်ပေးရမည်၊

(ဂ) Data Center ဝင်ခွင့်ကတ်များအား မပျောက်ပျက်အောင် စနစ်တကျ ထိန်းသိမ်းထား ရှိရမည်၊

(ဃ) Data Center အတွင်းသို့ တာဝန်ရှိသူများမှအပ အခြားမသက်ဆိုင်သူများ ဝင်ရောက်ခွင့် မရှိစေရေးအတွက် အထူးကြပ်မတ်ဆောင်ရွက်ရမည်၊

(င) Data Center အတွင်းသို့ ဝင်ရောက်သည့်အခါ မှတ်ပုံတင်စာအုပ်တွင် မပျက်မကွက် ရေးသွင်းရမည်၊

(စ) Data Center အတွင်းရှိ စနစ်များကို စောင့်ကြည့်စစ်ဆေးခြင်း၊ ပြုပြင်ထိန်းသိမ်းခြင်း များပြုလုပ်ရာတွင် Data Center အတွက် သတ်မှတ်ထားသည့် သီးခြားကွန်ပျူတာဖြင့်သာ ဝင်ရောက်အသုံးပြုရမည်၊

(ဆ) Data Center အတွင်းရှိ စနစ်များကို ဝင်ရောက်အသုံးပြုရာတွင် ကဏ္ဍအလိုက် သတ်မှတ်တာဝန်ခွဲဝေထားသည့် တာဝန်ခံအရာရှိများမှ စနစ်တကျ တာဝန်ယူဆောင်ရွက်ရမည်၊

(ဇ) Data Center အတွင်းရှိ အချက်အလက်များသိမ်းဆည်းရာတွင် လုံခြုံရေးကျိုးပေါက်မှု မဖြစ်ပွားစေရန် ဖိုင်များ၊ အချက်အလက်များကို Password ဖြင့် စနစ်တကျသိမ်းဆည်း၍ အချက်အလက်များဆုံးရှုံးမှုမရှိစေရန်အတွက်လည်း စနစ်တကျ Backup ပြုလုပ်ဆောင်ရွက်ရမည်၊

(ဈ) Data Center နှင့်သက်ဆိုင်သည့် အချက်အလက်များအား တာဝန်ရှိသူ၏ ခွင့်ပြုမိန့်မပါဘဲ ယူဆောင်ခြင်း၊ လွှဲပြောင်းခြင်း မပြုလုပ်ရ၊

(ည) Data Center ကိုင်တွယ်ထိန်းသိမ်းရသည့် တာဝန်ရှိသူများသည် သက်ဆိုင်ရာ User Name များနှင့် Password များအား ပြင်ပသို့ပေါက်ကြားမှုမရှိစေရန် အထူးဂရုပြုဆောင်ရွက်ရမည်၊

(ဋ) Data Center အတွင်းရှိစနစ်များ၏ Password များအား Devices များနှင့် Browsers များတွင် သိမ်းဆည်းထား၍ အလိုအလျောက် အလွယ်တကူ ဝင်ရောက်သုံးစွဲခြင်း မပြုလုပ်ရ၊

(ဌ) Data Center အတွင်းရှိစနစ်များကို ဝင်ရောက်သုံးစွဲပြီးပါက User Account များ၊ စနစ်များ၊ Devices များမှ စနစ်တကျ Log Out ပြုလုပ်ရမည်၊

(ဍ) Data Center ကိုင်တွယ်ထိန်းသိမ်းရသည့် တာဝန်ရှိသူများသည် Data Center IT/Non-IT Devices များ၊ စနစ်များကို အမြဲတစေစောင့်ကြည့်၍ ထူးခြားမှုတစ်စုံတစ်ရာရှိပါက သက်ဆိုင်ရာ တာဝန်ခံအရာရှိအဆင့်ဆင့်သို့ ချက်ချင်းသတင်းပို့တင်ပြရမည်။

အချက်အလက် Database များကိုင်တွယ်အသုံးပြုသူများ လိုက်နာဆောင်ရွက်ရမည့် အချက်များ

၁၅။ ပြည်တွင်းအခွန်များဦးစီးဌာနသည် ဌာနပိုင် Data Center များအသုံးပြု၍ Database တည်ဆောက်ကာ အချက်အလက်များကို ထိန်းသိမ်းထားရှိခြင်းအပြင် e-RTS ကဲ့သို့သော Standalone Based စနစ်များသည် သက်ဆိုင်ရာရုံးများ၏ ကွန်ပျူတာဆာဗာများတွင်သာ Database တည်ဆောက်၍ အချက်အလက်များကို သိမ်းဆည်းထားရှိခြင်းများလည်းရှိပါသည်။ အဆိုပါ Database သည် ရုံးနှင့်အခွန်ထမ်းများ၏ အရေးကြီးသော အခွန်ဆိုင်ရာနှင့် စီးပွားရေးဆိုင်ရာ အချက်အလက်များ စသည့် Critical Information များကို ထိန်းသိမ်းထားသည်ဖြစ်ရာ သတင်းအချက်အလက်များ ဆုံးရှုံးမှု

မဖြစ်စေရေးနှင့် လုံခြုံမှုပျက်ယွင်းခြင်းမရှိစေရေးအတွက် ကိုင်တွယ်အသုံးပြုသည့်ဝန်ထမ်းများအနေဖြင့် အောက်ဖော်ပြပါအတိုင်း တိကျစွာလိုက်နာ ဆောင်ရွက်ရပါမည်-

(က) အချက်အလက်များဆုံးရှုံးမှုမရှိစေရေးအတွက် Database Backup and Recovery Guideline များ ရေးဆွဲချမှတ်ဆောင်ရွက်ရမည်၊

(ခ) Database သည် အခွန်ထမ်းများ၏ အရေးကြီးသော အခွန်ဆိုင်ရာနှင့် စီးပွားရေးဆိုင်ရာ အချက်အလက်များကို ထိန်းသိမ်းထားသည့် Critical Information Database ဖြစ်သည်ကို အစဉ်သတိပြု၍ ဆောင်ရွက်ရမည်၊

(ဂ) အချက်အလက်များကို ကူးယူခြင်း၊ ရယူခြင်း၊ အပြန်အလှန်ပေးပို့ခြင်းသည် သတင်းအချက်အလက်ဆိုင်ရာ လုံခြုံမှုပျက်ယွင်းခြင်းပင်ဖြစ်၍ Data Base Backup များကို ကူးယူ၍ Removable Disk, Compatible Disc, Hard Disk တွင် သိမ်းဆည်းထားရှိရာတွင် Data Base File ကို Encrypt (Password Protected)ဖြင့် သိမ်းဆည်းထားရမည်၊ (Removable Disk သည် အလွယ်တကူပျောက်ဆုံးနိုင်သဖြင့် မသိမ်းဆည်းထားသင့်ပါ)၊

(ဃ) စနစ်အသုံးပြုရာတွင် မှားယွင်းမှု error ဖြစ်ပေါ်ခြင်းကြောင့် ပြင်ပမှစနစ်ရေးဆွဲသူထံ Data Base ပေးပို့ရန်လိုအပ်သောကိစ္စများတွင် Dummy Database ကို တည်ဆောက်၍ လုပ်ငန်းများကိုဆောင်ရွက်ရမည်၊

(င) Database ကိုင်တွယ်ထိန်းသိမ်းရန်အတွက် သတ်မှတ်ဝန်ထမ်းကို တာဝန်ပေးအပ်ရမည်၊ တာဝန်ပေးထားသည့် ဝန်ထမ်းများအား non-Disclosure ကတိခံဝန်ချက် ရေးထိုးထားရှိဆောင်ရွက်ရမည်၊

(စ) တာဝန်ပေးအပ်ထားသောဝန်ထမ်းပြောင်းရွှေ့ရပါက User ID နှင့် Password တို့ကို ဖြစ်နိုင်သမျှ အမြန်ဆုံးပယ်ဖျက်ရမည်။

ဆိုရှယ်မီဒီယာအသုံးပြုသူဝန်ထမ်းများလိုက်နာရန်စည်းကမ်းချက်များ

၁၆။ ပြည်တွင်းအခွန်များဦးစီးဌာနရှိ ဝန်ထမ်းများအားလုံးသည် ဆိုရှယ်မီဒီယာ (Social Media) ကို အသုံးပြုခြင်းနှင့်ပတ်သက်၍ ပြည်တွင်းအခွန်များဦးစီးဌာန၏ ၂၅-၁၁-၂၀၂၀ ရက်စွဲပါစာအမှတ်၊ ၈(၁)/ဥစ-၃/ပတခ/၂၀၂၁(၁၂၇၀၆) ဖြင့် ညွှန်ကြားထားသော **"ဆိုရှယ်မီဒီယာဆိုင်ရာမူဝါဒ"** ပါအတိုင်း လိုက်နာ၍ အောက်ပါစည်းကမ်းချက်များအတိုင်း အသုံးပြုရမည်-

(က) လုပ်ငန်းချိန်ပြင်ပတွင်သာ ကိုယ်ရေးကိုယ်တာကိစ္စရပ်များအတွက် ဆိုရှယ်မီဒီယာကို သုံးစွဲရန်၊ (နေ့လည်စာနားချိန်၊ နံနက် ၀၉:၃၀ နာရီမတိုင်မီနှင့် ညနေ ၀၄:၃၀ နာရီ နောက်ပိုင်း)၊

(ခ) မိမိကိုယ်တိုင်နှင့် မိမိဌာန၏ရုံးလုပ်ငန်းကိစ္စများကို အနှောင့်အယှက်မဖြစ်အောင် ဂရုပြု သုံးစွဲရန်၊

(ဂ) လုပ်ငန်းတာဝန်အရ ရရှိထားသောသတင်းအချက်အလက်များကို ဆိုရှယ်မီဒီယာတွင် ဖြန့်ဝေခြင်းမပြုရန်၊

(ဃ) ဆိုရှယ်မီဒီယာပေါ်တွင် မည်သည့် အခွန်ဆိုင်ရာအငြင်းပွားမှုများ၌မဆို ဝင်ရောက် ရေးသား ဆွေးနွေးခြင်းမပြုရန်၊

(င) ရင့်သီးသော၊ ညစ်ညမ်းသော၊ ခွဲခြားဆက်ဆံသော၊ ရိုင်းစိုင်းသော၊ အသရေဖျက်သော၊ ဌာန၏ဂုဏ်သိက္ခာကိုကျဆင်းစေသော၊ ဌာနဝန်ထမ်းအချင်းချင်းစိတ်ဝမ်းကွဲစေသော အကြောင်းအရာများကို မတင်ရန်၊ မဖြန့်ဝေရန်၊

(စ) အငြင်းပွားဖွယ်ကာတွန်းများ၊ ဟာသများ၊ နိုင်ငံရေး၊ ဘာသာရေးဆိုင်ရာလှုံ့ဆော်မှုများ နှင့် အတင်းအဖျင်းများကိုဖော်ပြခြင်း၊ ဖြန့်ဝေခြင်းမပြုရန်၊

(ဆ) မိမိတို့၏ဆိုရှယ်မီဒီယာတွင်ဖော်ပြချက်များသည် နှစ်ပေါင်းကြာမြင့်စွာ လူမှုကွန်ယက် စာမျက်နှာများတွင် ဖော်ပြထားရှိနိုင်ခြင်းကြောင့် ယင်းဖော်ပြချက်များအတွက် မိမိတို့တွင် တာဝန်ရှိကြောင်း အလေးအနက်ဂရုပြုရန်၊

(ဇ) ဌာနဝန်ထမ်းတစ်ဦး၏ရေးသားဖော်ပြမှု၊ ဖြန့်ဝေမှုများသည် ဌာန၏လုပ်ဆောင်မှု အနေဖြင့်သာ လူအများစုကသတ်မှတ်တတ်သဖြင့် မိမိတို့၏ ပြောဆိုရေးသားမှုများတွင် ဌာန၏ပုံရိပ်ကို ထိခိုက်မှုမရှိစေရေး အထူးသတိပြုရန်၊

(ဈ) ဆိုရှယ်မီဒီယာပေါ်တွင် မိမိအား‌အမည်တပ်၍ အခွန်ဆိုင်ရာကိစ္စရပ်များရေးသား မေးမြန်းလာပါက အခွန်ထမ်းဝန်ဆောင်မှုဗဟိုအဖွဲ့ရုံး၊ အခွန်ဆိုင်ရာဝန်ဆောင်မှုရုံးများသို့ မေးမြန်းနိုင်ကြောင်းနှင့် www.ird.gov.mm တွင် လေ့လာနိုင်ကြောင်းသာဖြေကြားရန်၊

(ည) မိမိတို့၏ ကိုယ်ရေးအချက်အလက်များ၊ တစ်ခြားသူတို့၏ ကိုယ်ရေးအချက်အလက်များ အား ဆိုရှယ်မီဒီယာတွင်ဖော်ပြခြင်းမပြုရန်၊

(၄) ဆိုရှယ်မီဒီယာများတွင် မိမိဌာနနှင့်ပတ်သက်သောဖော်ပြချက်များကို တွေ့ရှိရပါက ဦးစီးရုံးဌာနခွဲ၊ ညွှန်ကြားရေးမှူးထံ ဆက်သွယ်တင်ပြရန်။

လိုက်နာဆောင်ရွက်သင့်သည့်အထွေထွေအကြံပြုချက်များ

၁၇။ နိုင်ငံ့ဝန်ထမ်းနည်းဥပဒေများ ၁၆၃၊ နည်းဥပဒေခွဲ(န) တွင် "လုံခြုံမှုအဆင့်အတန်း သတ်မှတ်ထားသည့် ဌာနဆိုင်ရာစာရွက်စာတမ်းများကို ထိန်းသိမ်းစောင့်ရှောက်ရန် ပျက်ကွက်ခြင်း သို့မဟုတ် လုပ်ငန်းဆိုင်ရာ လျှို့ဝှက်ချက်များကို မသက်ဆိုင်သူများအား တိုက်ရိုက်ဖြစ်စေ၊ သွယ်ဝိုက်၍ဖြစ်စေ အသိပေးခြင်းတို့အတွက် ဌာနဆိုင်ရာအရေးယူအပြစ်ပေးနိုင်သည်"ဟူ၍ ပြဋ္ဌာန်းထားသည်ဖြစ်ရာ မလိုလားအပ်သောဖြစ်စဉ်များ မဖြစ်ပွားစေရန် ဝန်ထမ်းများ၏ သတင်းအချက်အလက် လုံခြုံရေးဆိုင်ရာ အသိအမြင်၊ အသိသညာများ တိုးတက်စေရေးနှင့် ဌာန၏သတင်းအချက်အလက် လုံခြုံရေးပိုမိုကောင်းမွန်စေရန်အတွက် လိုအပ်ပါက သတင်းအချက်အလက်နှင့်နည်းပညာဌာနခွဲ၏ နည်းပညာဆိုင်ရာအကြံပြုချက်ရယူ၍ အောက်ပါအချက်များကိုဆောင်ရွက်ထားရှိရမည်-

(က) သတင်းအချက်အလက်လုံခြုံမှုအတွက် ကွန်ပျူတာသုံးစွဲသူများအား လိုက်နာဆောင်ရွက်မည့် Rules and Regulations များကို ခေတ်နှင့်လျော်ညီစွာ စုစည်းရေးဆွဲ ထုတ်ပြန်ပေးရန်၊

(ခ) သတင်းအချက်အလက်လုံခြုံမှုနှင့် ကာကွယ်တာဆီးမှုနည်းလမ်းများ၊ ဗဟုသုတများ ပြန့်ပွားတိုးတက်စေရေးအတွက် ပညာရပ်ဆိုင်ရာကျွမ်းကျင်မှု Seminar Workshop Forum များ အခါအားလျော်စွာ ကျင်းပပြုလုပ်ပေးရန်၊

(ဂ) Virus အမျိုးအစားအသစ်များ အမြဲပေါ်ပေါက်နေသဖြင့် Computer အားလုံးတွင် လိုင်စင် Antivirus Software များ ဝယ်ယူသုံးစွဲပြီး မိမိ Software သည် အဆိုပါ Virus အား နှိမ်နင်းနိုင်ခြင်း ရှိ/မရှိ စစ်ဆေးခြင်း၊ မိမိဝယ်ယူထားသည့် Antivirus Software သည် အသစ်ပေါ်လာသော Virus အား မနှိမ်နင်းနိုင်ပါက နှိမ်နင်းနိုင်သည့် လိုင်စင် Antivirus Software ရှာဖွေဝယ်ယူခြင်း (သို့မဟုတ်) မိမိဝယ်ယူထားသည့် လိုင်စင် Antivirus Software ၏ Website တွင် ၎င်းအမည်နှင့် နှိမ်နင်းနိုင်မည့် နည်းလမ်းရှာဖွေဆောင်ရွက်ခြင်း၊ နေ့စဉ် Virus Update ပြုလုပ်ခြင်းဖြင့် ဆောင်ရွက်ရန်၊

(ဃ) Memory Stick များအား မိမိကွန်ပျူတာနှင့် ချိတ်ဆက်အသုံးပြုရန် လိုအပ်လာပါက Virus စစ်ဆေးမှုအရင်ပြုလုပ်ရန်နှင့် Virus တွေ့ရှိပါက လိုင်စင် Virus Software ဖြင့် နှိမ်နင်းရန်၊

(c) ဌာနတစ်ခုမှတစ်ခုသို့ Soft Copy Data များ ပေးပို့ရန်လိုအပ်သည့်အခါ Password ထည့်သွင်းပေးပို့၍ အဆိုပါ Data ကိုအသုံးပြုခွင့်ရှိသူထံသို့ လုံခြုံမှုရှိသည့် နည်းလမ်းဖြင့် Password အား အသိပေးရန်၊

(စ) ကွန်ပျူတာ Hard Disk များပျက်စီးသည့်အခါ Disk Recovery Software များ အသုံးပြု၍ Data ပြန်လည်ဖော်ထုတ်နိုင်သဖြင့် ပျက်စီးနေသော Hard Disk အား လုံခြုံစွာသိမ်းဆည်းခြင်း၊ သုံးစွဲမရနိုင်အောင် ဖျက်ဆီးခြင်းများ ဆောင်ရွက်ရန်၊

(ဆ) အရေးကြီးစာများ Print ထုတ်ယူခြင်းများအတွက် စနစ်တကျ မှတ်တမ်းထားရန်၊

(ဇ) အရေးကြီးစာများကို Print ထုတ်ယူပြီးသည့်အခါ Printer Error ကြောင့် Printer တွင် Memory ကျန်ရှိမနေစေရေး အထူးဂရုပြုဆောင်ရွက်ရန်၊

(ဈ) ဌာနတွင်းအသုံးပြုသော ကွန်ပျူတာများ ချို့ယွင်းမှုရှိပါက ပြင်ပသို့ ယူဆောင်ခြင်း မပြုဘဲ IT ဌာနသို့သာ ပေးပို့ပြင်ဆင်ရန်၊

(ည) သတင်းအချက်အလက်လုံခြုံမှုဆိုင်ရာ ကျိုးပေါက်မှု၊ ဆိုက်ဘာတိုက်ခိုက်မှုများကြောင့် ပြဿနာတစ်စုံတစ်ရာ ပေါ်ပေါက်လာပါက အချက်အလက် ဆုံးရှုံးမှုများ ပေါ်ပေါက်မှု မရှိစေရန် ပြန်လည်ဆယ်ယူမည့် လုပ်ငန်းမဟာဗျူဟာအစီအစဉ်များ ချမှတ်၍ ညွှန်ကြားကြီးကြပ်ဆောင်ရွက်ရန်။

နိဂုံး

၁၈။ သို့ဖြစ်ပါ၍ ပြည်တွင်းအခွန်များဦးစီးဌာနမှ ဝန်ထမ်းများအနေဖြင့် အီလက်ထရောနစ် သတင်းအချက်အလက်လုံခြုံမှုရှိစေရေးနှင့် အချက်အလက်ပေါက်ကြားမှုမရှိစေရေးအတွက် ဝန်ထမ်းကျင့်ဝတ်၊ ပြည်တွင်းအခွန်များဦးစီးဌာန၏ ကိုယ်ကျင့်သိက္ခာနှင့်ကျင့်ဝတ်၊ အခွန်ဆိုင်ရာစီမံအုပ်ချုပ်မှုဥပဒေ၊ မြန်မာနိုင်ငံလျှို့ဝှက်ချက်အက်ဥပဒေအပါအဝင် အခြားတည်ဆဲဥပဒေများနှင့်အညီ တိတိကျကျ လိုက်နာစေရေးအတွက် တာဝန်ရှိသူအဆင့်ဆင့်မှလည်း အထူးအလေးထား ကြပ်မတ်ဆောင်ရွက်သွားရမည်ဖြစ်ပါသည်။

ပြည်တွင်းအခွန်များဦးစီးဌာန