**အင်တာနက်အသုံးပြုသူများ လိုက်နာဆောင်ရွက်ရမည့်အချက်များ**

၁၁။ ရုံးလုပ်ငန်းများ အဆင်ပြေချောမွေ့စွာ ဆောင်ရွက်နိုင်ရန်အတွက် အင်တာနက်ချိတ်ဆက် အသုံးပြုရာတွင် ဌာန၏ အရေးကြီးအချက်အလက်များ ပြင်ပသို့ ပေါက်ကြားမှုမရှိစေရန်နှင့် လုံခြုံမှုရှိစေရန် အင်တာနက်အသုံးပြုသူများအနေဖြင့် လိုက်နာဆောင်ရွက်ရမည့် လုပ်ငန်းစဉ်များ မှာ အောက်ပါအတိုင်းဖြစ်ပါသည်-

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

(ခ) ရုံးနှင့်သက်ဆိုင်သည့် စာရွက်စာတမ်းများ၊ ဓာတ်ပုံများကို Social Media များ ပေါ်သို့ ခွင့်ပြုချက်မရဘဲ Upload ပြုလုပ်ခြင်းများ ဆောင်ရွက်မှုမရှိစေရေး အထူးကြပ်မတ် ဆောင်ရွက်ရမည်၊

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

(ဃ) အင်တာနက်ချိတ်ဆက်အသုံးပြုသည့် ကွန်ပျူတာများအတွက် သတ်မှတ် ထားသော လုပ်ငန်းစဉ်များအား မပျက်မကွက်ဆောင်ရွက်ရမည်၊

(င) အများပြည်သူများအတွက် ဖွင့်လှစ်ထားသည့် အင်တာနက်ကဖေးများနှင့် အခြား နေရာများတွင် အသုံးပြုသော ကွန်ပျူတာများတွင် 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 များကို ဖွင့်ခြင်း၊ Link များကို Click နှိပ်ခြင်း၊ အချက်အလက်များ ဖြည့်သွင်းခြင်း၊ ထပ်မံဖြန့်ဝေခြင်းများမှ ရှောင်ကြဉ် ရမည်၊

(ဈ) email သို့မဟုတ် ဌာန၏ အခြားစနစ်များကို အသုံးပြုရာတွင် Password များအား devices များတွင် Browsers များ၌ သိမ်းဆည်းထား၍ အလွယ်တကူ ဝင်ရောက်သုံးစွဲခြင်း မပြုလုပ်ရန်နှင့် ဝင်ရောက်သုံးစွဲပြီးပါက User Account များ၊ စနစ်များ၊ Devices များမှ စနစ်တကျ Log Out ပြုလုပ်ရမည်၊

(ည) ရုံးတွင်း Network နှင့် ကွန်ပျူတာများအား ထိခိုက်စေနိုင်သည့် အန္တရာယ်ရှိသော Website များသို့ ဝင်ရောက်ကြည့်ရှုခြင်းများ မပြုလုပ်ရန် အထူးကြပ်မတ်ဆောင်ရွက်ရမည်၊

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

**လျှို့ဝှက်စကားလုံးများ (Passwords) သတ်မှတ်ထားရှိရာတွင် လိုက်နာဆောင်ရွက်ရမည့် အချက်များ**

၁၂။ ကွန်ပျူတာစနစ်များ/ပစ္စည်းကိရိယာများကို အသုံးပြုနိုင်စေရန်နှင့် သတင်းအချက် အလက်များကို အခွင့်မရှိဘဲ ရယူအသုံးပြုခြင်းမှ ကာကွယ်ရန်၊ စနစ်များ/ပစ္စည်းကိရိယာများ အားလုံးအတွက် အသုံးပြုသူအမည် (user ids )နှင့် လျှို့ဝှက်စာလုံးများကို အသုံးပြုသင့်ပါသည်။ အသုံးပြုမှုဆိုင်ရာ လုံခြုံရေးထိန်းချုပ်မှု (security access control )သည် ခွင့်ပြုချက်မရသော အသုံးပြုမှုမှ အဓိကကာကွယ်ပေးသည်။ မိမိတို့သည် စနစ်တစ်ခုစီအတွက် သီးခြား တစ်ခုတည်းဖြစ်သော၊ ကောင်းစွာတည်ဆောက်ထားသော လျှို့ဝှက်စကားလုံးတစ်ခုကို ရွေးချယ်ရန် အလွန်အရေးကြီးသည်။ လျှို့ဝှက်စကားလုံး Password များဖန်တီးရာတွင် လိုက်နာဆောင်ရွက်ရမည့် လုပ်ငန်းစဉ်များမှာ အောက်ပါအတိုင်းဖြစ်ပါသည်-

(က) အရေးကြီးသည့်အချက်အလက်များ ပေါက်ကြားမှုမရှိစေရန်နှင့် လုံခြုံမှု ရှိစေရန်အတွပ် သူတစ်ပါးအလွယ်တကူမခန့်မှန်းနိုင်သော Password များထားရှိရမည်၊

(ခ) လျှို့ဝှက်စကားလုံးPassword များထားရှိရာတွင် Special Character (ဥပမာ-!,@,#,$ စသည်)များ၊ Number များ၊ Small Letter နှင့် Capital Letter များအပါအဝင် အက္ခရာ၊ ကိန်းဂဏန်းနှင့် အထူးစာလုံးတို့ ပေါင်းစပ်ပါဝင်သည့် အနည်းဆုံး(၈)လုံးထားရှိရမည်၊ သို့ရာတွင် စာလုံး(၈)လုံးထက်ပို၍ အသုံးပြုခြင်းသည် ပိုမိုလုံခြုံမှုရှိစေပါသည်၊

(ဂ) Dictionary ထဲတွင် ပါဝင်သောစကားလုံးများကို Password အဖြစ် အသုံးပြုခြင်းမှ ရှောင်ကြဉ်ရမည်၊

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

(င) ဌာနအမည် သို့မဟုတ် ဌာနခွဲအမည်များကို Password မဖြစ် 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 များ မပေါက်ကြားစေရန်အတွက် သတ်မှတ်ထားသည့် Password များကို မြင်သာထင်သာရှိသည့် နေရာများတွင်(ဥပမာ Stick otes များတွင် ရေးသား၍ ကွန်ပျူတာမျက်နှာပြင်ထောင့် သို့မဟုတ် ခုံပေါ်တွင် )ကပ်ထားခြင်းများ၊ Password File များအား အများမြင်သာစေသည့် နေရာများတွင် အလွယ်တကူသိမ်းဆည်းထားခြင်းများ မပြုလုပ်ဘဲ တာဝန်ခံအရာရှိမှ စနစ်တကျ လုံခြုံစွာသိမ်းဆည်းအသုံးပြုရမည်၊

(ဈ) လျှို့ဝှက်စကားလုံးကို လျှို့ဝှက်ထားပါ။ မည်သူနှင့်မျှ ဝေမျှခြင်းမပြုပါနှင့်၊

(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၏ လျှို့ဝှက်စကားလံဒးကို ချက်ချင်းပြောင်းပါ၊

**Removable Devices များအသုံးပြု၍ အချက်အလက်များ ကူးယူရာတွင် လိုက်နာဆောင်ရွက်ရမည့် အချက်များ**

၁၃။ ရုံးလုပ်ငန်းများဆောင်ရွက်ရာ၌ Remavable Devices များအသုံးပြု၍ အချက်အလက်များ ကူးယူလေ့ရှိရာ Virus ဝင်ရောက်မှုများနှင့် အချက်အလက်များဆုံးရှုံးမှု၊ ပေါက်ကြားမှုများ မဖြစ်ပေါ်စေရန် 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 ပြုလုပ်ပြီးမှသာ ကူးယူရမည်၊

(ဃ) အချက်အလက်များအား ကူးယူပြီးသည့်အခါ Removable Devices ထဲတွင် ဆက်လက်ထားရှိခြင်းမပြုဘဲ ဖိုင်များအား ဖျက်ပစ်ရမည်၊

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

**Data Center ရှိ သတင်းအချက်အလက်များ လုံခြုံမှုရှိစေရေးအတွက် လိုက်နာ ဆောင်ရွက်ရမည့်အချက်များ**

၁၄။ ပြည်တွင်းအခွန်များဦးစီးဌာန၏ Data Center နှင့် သက်ဆိုင်သည့် အချက်အလက်များ လုံခြုံမှုရှိစေရေးအတွက် ဆောင်ရွက်ရမည့်လုပ်ငန်းများမှာ အောက်ပါအတိုင်းဖြစ်ပါသည်-

(က) Data Center နှင့် သက်ဆိုင်သည့်သော့များကို သက်ဆိုင်ရာတာဝန်ခံအရာရှိမှ စနစ်တကျထိန်းသိမ်းထားရှိရမည်၊

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

(ဂ) Data Center ဝင်ခွင့်ကတ်များအား မပျောက်ပျက်အောင် စနစ်တကျ ထိန်းသိမ်းထားရှိရမည်၊

(ဃ) Data Center အတွင်းသို့ တာဝန်ရှိသူများမှအပ အခြားမသက်ဆိုင်သူများ ဝင်ရောက်ခွင့်မရှိစေရေးအတွက် အထူးကြပ်မတ်ဆောင်ရွက်ရမည်၊

(င) Data Center အတွင်းသို့ ဝင်ရောက်သည့်အခါ မှတ်ပုံတင်စာအုပ်တွင် မပျက်မကွက်ရေးသွင်းရမည်၊

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

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

(ဇ) Data Center အတွင်းရှိ အချက်အလက်များသိမ်းဆည်းရာတွင် လုံခြုံရေးကျိုးပေါက်မှုမဖြစ်ပွားစေရန် 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 အတွင်းရှိ စနစ်များ၏ Password များအား Devices များနှင့် Browsers များတွင် သိမ်းဆည်းထား၍ အလိုအလျောက် အလွယ်တကူ ဝင်ရောက်သုံးစွဲခြင်းမပြုလုပ်၍၊

(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 သက်ဆိုင်ရာတာဝန်ခံအရာရှိအဆင့်ဆင့်သို့ ချက်ချင်းသတင်းပို့တင်ပြရမည်။

**အချက်အလက် Database များကိုင်တွယ်အသုံးပြုသူများ လိုက်နာဆောင်ရွက်ရမည့်အချက်များ**

၁၅။ မြန်မာ့စီးပွားရေးဘဏ်သည် ဌာနပိုင် Data Center များအသုံးပြု၍ Database တည်ဆောက်ကာ အချက်အလက်များကို ထိန်းသိန်းထားရှိခြင်းအပြင် e-RTS ကဲ့သို့သော Standalone Based စနစ်များသည် သက်ဆိုင်ရာရုံးများ၏ ကွန်ပျူတာဆာဗာများတွင်သာ Database တည်ဆောက်၍ အချက်အလက်များကို သိမ်းဆည်းထားရှိခြင်းများလည်းရှိပါသည်။ အဆိုပါ Database သည် ရုံးနှင့်အခွန်ထမ်းများ၏ အရေးကြီးသော အခွန်ဆို်ငရာနှင့်စီးပွားရေးဆိုင်ရာ အချက်အလက်များ စသည့် Critical Information များကို ထိန်းသိမ်းထားသည်ဖြစ်ရာ သတင်းအချက်အလက်းများ ဆုံးရှုံးမှုမဖြစ်စေရေးနှင့် လုံခြုံမှုပျက်ယွင်းခြင်းမရှိစေရေးအတွက် ကိုင်တွယ်အသုံးပြုသည့်ဝန်ထမ်းများအနေဖြင့် အောက်ဖော်ပြပါအတိုင်း တိကျစွာလိုက်နာဆောင်ရွက်ရပါမည်-

(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 ပြင်ပမှ စနစ်ရေးဆွဲသူထံ Data Base ပေးပို့ရန်လိုအပ်သောကိစ္စများတွင် Dummy Database ကို တည်ဆောက်၍ လုပ်ငန်းများကို ဆောင်ရွက်ရမည်၊

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

(စ) တာဝန်ပေးအပ်ထားသော ဝန်ထမ်းပြောင်းရွှေ့ရပါက User ID နှင့် Password တို့ကို ဖြစ်နိုင်သမျှ အမြန်ဆုံးပယ်ဖျက်ရမည်။

**ဆိုရှယ်မီဒီယာအသုံးပြုသူဝန်ထမ်းများလိုက်နာရန်စည်းကမ်းချက်များ**

၁၆။ မြန်မာ့စီးပွားရေးဘဏ်ရှိ ဝန်ထမ်းများအားလုံးသည် ဆိုရှယ်မီဒီယာ(Social Media)ကို အသုံးပြုခြင်းနှင့် ပတ်သက်၍ မြန်မာ့စီးပွားရေးဘဏ်၏ ------ရက်စွဲပါစာအမှတ်၊ -------- ဖြင့် ညွှန်ကြားထားသော “ဆိုရှယ်မီဒီယာဆိုင်ရာမူဝါဒ” ပါအတိုင်းလိုက်နာ၍ အောက်ပါစည်းကမ်းချက်များအတိုင်း အသုံးပြုရမည်-

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

(ခ) မိမိကိုယ်တိုင်နှင့် မိမိဌာန၏ ရုံးလုပ်ငန်းကိစ္စများကို အနှောင့်အယှက်မဖြစ်အောင် ဂရုပြုသုံးစွဲရန်၊

(ဂ) လုပ်ငန်းတာဝန်အရ ရရှိထားသောသတင်းအချက်အလက်များကို ဆိုရှယ်မီဒီယာတွင် ဖြန့်ဝေခြင်းမပြုရန်၊

(ဃ) ဆိုရှယ်မီဒီယာပေါ်တွင် မည်သည့် အခွန်ဆိုင်ရာအငြင်းပွားမှုများ၌မဆို ဝင်ရောက်ရေးသား ဆွေးနွေးခြင်းမပြုရန်၊

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

(စ) အငြင်းပွားဖွယ်ကာတွန်းများ၊ ဟာသများ၊ နိုင်ငံရေး၊ ဘာသာရေးဆိုင်ရာလှုံ့ဆော်မှုများနှင့် အတင်းအဖြင်းများကို ဖော်ပြခြင်း၊ ဖြန့်ဝေခြင်းမပြုရန်၊

(ဆ) မိမိတို့၏ဆိုရှယ်မီဒီယာတွင် ဖော်ပြချက်များသည် နှစ်ပေါင်းကြာမြင့်စွာ လူမှုကွန်ယက်စာမျက်နှာများတွင် ဖော်ပြထားရှိနိုင်ခြင်းကြောင့် ယင်းဖော်ပြချက်များအတွက် မိမိတို့တွင် တာဝန်ရှိကြောင်း အလေးအနက်ဂရုပြုရန်၊

(ဇ) ဌာနဝန်ထမ်းတစ်ဦး၏ ရေးသားဖော်ပြမှု၊ ဖြန့်ဝေမှုများသည် ဌာန၏ လုပ်ဆောင်မှုအနေဖြင့်သာ လူအများစုက သတ်မှတ်တတ်သဖြင့် မိမိတို့၏ ပြောဆိုရေးသားမှုများတွင် ဌာန၏ ပုံရိပ်ကို ထိခိုက်မှုမရှိစေရေး အထူးသတိပြုရန်၊

(ဈ) ဆိုရှယ်မီဒီယာပေါ်တွင် မိမိအားအမည်တပ်၍ အတိုးနှုန်းဆိုင်ရာကိစ္စရပ်များရေးသားမေးမြန်းလာပါက [www.meb.gov.mm](http://www.meb.gov.mm) တွင် လေ့လာနိုင်ကြောင်းသာ ဖြေကြားရန်၊

(ည) မိမိတို့၏ ကိုယ်ရေးအချက်အလက်များ၊ တစ်ခြားသူတို့၏ ကိုယ်ရေးအချက်အလက်များအား ဆိုရှယ်မီဒီယာတွင် ဖော်ပြခြင်းမပြုရန်၊

(ဋ) ဆိုရှယ်မီဒီယာများတွင် မိမိဌာနနှင့်ပတ်သက်သောဖော်ပြချက်များကို တွေ့ရှိရပါက ဦးစီးရုံးဌာနခွဲ၊ ညွှန်ကြားရေးမှူးထံ ဆက်သွယ်တင်ပြရန်၊

**လိုက်နာဆောင်ရွက်သင့်သည့် အထွေထွေအကြံပြုချက်များ**

၁၇။ နိုင်ငံ့ဝန်ထမ်းနည်းဥပဒေများ ၁၆၃၊ နည်းဥပဒေခွဲ(န)တွင် “လုံခြုံမှုအဆင့်အတန်း သတ်မှတ်ထားသည့် ဌာနဆိုင်ရာစာရွက်စာတမ်းများကို ထိန်းသိမ်းစောင့်ရှောက်ရန် ပျက်ကွက်ခြင်း သို့မဟုတ် လုပ်ငန်းဆိုင်ရာ လျှို့ဝှက်ချက်များကို မသက်ဆိုင်သူများအား တိုက်ရိုက်ဖြစ်စေ၊ သွယ်ဝိုက်၍ဖြစ်စေ အသိပေးခြင်းတို့အတွက် ဌာနဆိုင်ရာအရေးယူအပြစ်ပေးနိုင်သည်”ဟူ၍ ပြဋ္ဌာန်းထားသည်ဖြစ်ရာ မလိုလားအပ်သော ဖြစ်စဉ်များ မဖြစ်ပွားစေရန် ဝန်ထမ်းများ၏ သတင်းအချက်အလက်လုံခြုံရေးဆိုင်ရာ အသိအမြင်၊ အသိသညာများ တိုးတက်စေရေးနှင့် ဌာန၏ သတင်းအချက်အလက် လုံခြုံရေးပိုမိုကောင်းမွန်စေရန်အတွက် လိုအပ်ပါက သတင်းအချက်အလက်နှင့် နည်းပညာဌာနခွဲ၏ နည်းပညာဆိုင်ရာ အကြံပြုချက်ရယူ၍ အောက်ပါအချက်များကို ဆောင်ရွက်ထားရှိရမည်-

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

(ခ) သတင်းအချက်အလက်လုံခြုံမှုနှင့် ကာကွယ်တားဆီးမှုနည်းလမ်းများ၊ ဗဟုသုတများပြန့်ပွားတိုးတက်စေရေးအတွက် ပညာရပ်ဆိုင်ရာကျွမ်းကျင်မှု Seminar Workshop Forum များ အခါအားလျော်စွာ ကျင်းပပြုလုပ်ပေးရန်၊

(ဂ) Virus အမျိုးအစားအသစ်များ အမြဲပေါ်ပေါက်နေသဖြင့် Computer အားလုံးတွင် လိုင်စင် Antivirus Software များ ဝယ်ယူသုံးစွဲပြီး မိမိ Software သည် အဆိုပါ Virus အားနှိမ်နင်းနိုင်ခြင်း 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၊