ပြည်ထောင်စုသမ္မတမြန်မာနိုင်ငံတော်

ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ မူဝါဒ

၂၀၂၃ ခုနှစ်၊ မတ်လ

ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ မူဝါဒ

ပို့ဆောင်ရေးနှင့် ဆက်သွယ်ရေးဝန်ကြီးဌာန
သတင်းအချက်အလက်နည်းပညာနှင့် ဆိုက်ဘာလုံခြုံရေးဦးစီးဌာန
မှ ထုတ်ဝေသည်။
www.motc.gov.mm

မာတိကာ

ပြည်ထောင်စုသမ္မတမြန်မာနိုင်ငံတော်
ပို့ဆောင်ရေးနှင့်ဆက်သွယ်ရေးဝန်ကြီးဌာန
အမိန့်ကြော်ငြာစာအမှတ် (၉/၂၀၂၃)
၁၃၈၄ ခုနှစ်၊ တန်ခူးလဆန်း ၉ ရက်
(၂၀၂၃ ခုနှစ်၊ မတ်လ ၂၉ ရက်)

ပို့ဆောင်ရေးနှင့် ဆက်သွယ်ရေး ဝန်ကြီးဌာနသည် ဤ ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာမူဝါဒကို ၂၀၂၂ ခုနှစ်၊ ဒီဇင်ဘာလတွင် ကျင်းပပြုလုပ်သော ပြည်ထောင်စုသမ္မတမြန်မာနိုင်ငံတော်၊ ပြည်ထောင်စုအစိုးရအဖွဲ့ အစည်းအဝေး အမှတ်စဉ် (၉/၂၀၂၂) ၏ သဘောတူညီချက်ဖြင့် ထုတ်ပြန်လိုက်သည်။

အခန်း (၁)
နိဒါန်း

၁။ သတင်းအချက်အလက်နှင့် ဆက်သွယ်ရေးနည်းပညာ (Information and Communication Technology-ICT) အသုံးပြုခြင်း၏ အကျိုးကျေးဇူးများ ရရှိခံစားလာနိုင်သည်နှင့်အမျှ ဗိုင်းရပ်စ် (Virus)၊ အန္တရာယ်ရှိနိုင်သော ဆော့ဖ်ဝဲလ်ကုဒ် (Software Code) များပို့နှုန်းခြင်း၊ ဆိုက်ဘာရာဇဝတ်မှုများပေါ်ပေါက်လာခြင်း၊ ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာခြိမ်းခြောက်တိုက်ခိုက်မှုများ များပြားလာခြင်း၊ စီးပွားရေး၊ လူမှုရေးလုပ်ငန်းများ၏ အရေးကြီးသတင်းအချက်အလက်ဆိုင်ရာ အခြေခံအဆောက်အဦများ၏ ဝန်ဆောင်မှုကို နှောင့်ယှက်တိုက်ခိုက်ခံရခြင်း၊ အင်တာနက်မှတစ်ဆင့်

ကိုယ်ရေးဆိုင်ရာ အချက်အလက်များ ပေါက်ကြားခြင်း၊ ခိုးယူခံရခြင်း အစရှိသည့် ဆိုက်ဘာလုံခြုံရေးနှင့် ဆက်စပ်နေသော အခက်အခဲများ၊ ဆိုက်ဘာမှုခင်းများကို ကမ္ဘာတစ်ဝန်း ကြုံတွေ့နေရသည်။ အချို့ဆိုက်ဘာ တိုက်ခိုက်မှု ဖြစ်ရပ်များသည် အရေးကြီး သတင်းအချက်အလက်စနစ် များ၏ လုပ်ငန်းလည်ပတ်မှုကို ထိခိုက်စေခြင်းဖြင့် အခြားဆုံးရှုံးမှု များအပြင် အစိုးရ၊ ပြည်သူနှင့် ပုဂ္ဂလိကကဏ္ဍ အရင်းအမြစ်များနှင့် ဝန်ဆောင်မှုများ၏ ပုံရိပ်ကို ထိခိုက်ကျဆင်းစေနိုင်သည်။

၂။ မြန်မာနိုင်ငံတွင် ၂၀၁၃ ခုနှစ်၌ ဆက်သွယ်ရေးဥပဒေကို ပြဋ္ဌာန်း ခဲ့သောကြောင့် သတင်းအချက်အလက်နှင့် ဆက်သွယ်ရေးနည်းပညာ ဈေးကွက်ကို ဖွင့်လှစ်ပေးနိုင်ခဲ့ပြီး e-Government စနစ်အပါအဝင် အွန်လိုင်းဝန်ဆောင်မှုများအား ပိုမိုကျယ်ပြန့်စွာ အကောင်အထည်ဖော် ဆောင်ရွက်လာနိုင်သည့်အတွက် လူမှုအဖွဲ့အစည်းအတွင်း စီးပွားရေး လုပ်ငန်းများနှင့် ပြည်သူတို့၏ နေ့စဉ်ဘဝများသည် သတင်းအချက် အလက်နည်းပညာ အသုံးပြုမှုအပေါ် များစွာ မှီခိုလာကြသည်။

၃။ ပြည်ထောင်စုအဆင့်အဖွဲ့အစည်းများ၊ အစိုးရဌာန၊ အစိုးရအဖွဲ့ အစည်းများတွင် သတင်းအချက်အလက်နှင့် ဆက်သွယ်ရေးနည်းပညာ များကို အသုံးပြု၍ e-Government လုပ်ငန်းစဉ်များအား အရှိန်အဟုန်မြှင့် ဆောင်ရွက်နိုင်ရန်အတွက် ၂၀၁၈ ခုနှစ်၊ ဧန်နဝါရီလ ၂၃ ရက်နေ့၌ နိုင်ငံတော်သမ္မတရုံး၏ အမိန့်ကြော်ငြာစာအမှတ် ၁၄/၂၀၁၈ ဖြင့် ဖွဲ့စည်း ခဲ့သော e-Government ဦးဆောင်ကော်မတီနှင့် e-Government

အကောင်အထည်ဖော်ရေး လုပ်ငန်းကော်မတီတို့ကို နိုင်ငံတော်စီမံအုပ်ချုပ်ရေးကောင်စီ၏ ၂၀၂၁ ခုနှစ်၊ ဧပြီလ ၄ ရက်နေ့တွင် အမိန့်ကြော်ငြာစာအမှတ် ၉၇/၂၀၂၁ ဖြင့် e-Government ဦးဆောင်ကော်မတီကို လည်းကောင်း၊ အမိန့်ကြော်ငြာစာအမှတ် ၉၈/၂၀၂၁ ဖြင့် e-Government အကောင်အထည်ဖော်ရေး လုပ်ငန်းကော်မတီကိုလည်းကောင်း ပြင်ဆင်ဖွဲ့စည်းခဲ့ပြီးဖြစ်ပါသည်။

၄။ မြန်မာနိုင်ငံတွင် ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ ခြိမ်းခြောက်တိုက်ခိုက်မှုများနှင့် ဆိုက်ဘာရာဇဝတ်မှုခင်းများကို ကြိုတင်ကာကွယ်နိုင်ရန်နှင့် ဖော်ထုတ်အရေးယူနိုင်ရန်၊ လူ့စွမ်းအားအရင်းအမြစ် ဖွံ့ဖြိုးတိုးတက်စေရန်၊ ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ ပတ်ဝန်းကျင်အခြေခံကောင်းများတည်ဆောက်ရန် ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ မူဝါဒ လိုအပ်လျက်ရှိပါသည်။ မြန်မာနိုင်ငံ၏ ဆိုက်ဘာလုံခြုံရေးအနေအထားကို မြှင့်တင်ရန် တိကျသော လုပ်ထုံးလုပ်နည်းများနှင့် စီမံချက်များအား ဖော်ဆောင်နိုင်မည့် ဆိုက်ဘာလုံခြုံရေးဥပဒေ၊ ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ မဟာဗျူဟာနှင့် မူဘောင်တို့ကို အကောင်အထည်ဖော်ဆောင်ရန် ဦးတည်၍ ဤဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ မူဝါဒကို e-Government အကောင်အထည်ဖော်ရေး လုပ်ငန်းကော်မတီ၏ ကြီးကြပ်မှုဖြင့် ရေးဆွဲခြင်းဖြစ်သည်။

အခန်း (၂)

မျော်မှန်းချက်၊ ရည်မှန်းချက်နှင့် ရည်ရွယ်ချက်များ

မျော်မှန်းချက်

၅။ ပြည်ထောင်စုသမ္မတ မြန်မာနိုင်ငံတော်အတွက် လုံခြုံစိတ်ချ၍ တည်ငြိမ်၊ ကောင်းမွန်၊ ကြွံခိုင်သော ဆိုက်ဘာနယ်ပယ်တစ်ခု တည်ဆောက်နိုင်ရန်။

ရည်မှန်းချက်

၆။ ဆိုက်ဘာလုံခြုံရေးအတွက် လိုအပ်သော ဥပဒေ ပြဋ္ဌာန်းခြင်း၊ နည်းဥပဒေ၊ စည်းမျဉ်းဥပဒေ၊ စည်းကမ်းဥပဒေ၊ အမိန့်ကြော်ငြာစာ၊ အမိန့်၊ လုပ်ထုံးလုပ်နည်း၊ လမ်းညွှန်ချက်နှင့် ညွှန်ကြားချက်များ ထုတ်ပြန်ခြင်း၊ စံသတ်မှတ်ချက်များ ထုတ်ပြန်ခြင်း၊ ဖွဲ့စည်းဆောင်ရွက်မှု ပုံစံ၊ လူစွမ်းအားအရင်းအမြစ် မြှင့်တင်ရေး၊ ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ နည်းစနစ်များအား မူဝါဒချမှတ်ခြင်းတို့ကို ဆောင်ရွက်သွားရမည်။

ရည်ရွယ်ချက်များ

၇။ ဤမူဝါဒ၏ ရည်ရွယ်ချက်များမှာ အောက်ဖော်ပြပါအတိုင်း ဖြစ်ပါသည်-

(က) လုံခြုံစိတ်ချ၍ တည်ငြိမ်ကောင်းမွန် ကြွံခိုင်သော ဆိုက်ဘာဂေဟစနစ်ကို ဖန်တီးရန်၊

(ခ) သတင်းအချက်အလက် ဖလှယ်မှုများ ပြုလုပ်ရာတွင်

ယုံကြည်စိတ်ချမှု ဖြစ်ပေါ်စေရေးနှင့် ကဏ္ဍအားလုံးတွင် ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ သတင်းအချက်အလက်နှင့် ဆက်သွယ်ရေး နည်းပညာအသုံးပြုမှုကို တိုးမြှင့်စေရန်၊

(ဂ) အရေးကြီး သတင်းအချက်အလက် အခြေခံအဆောက်အဦများ၏ လုံခြုံမှုကို ကာကွယ်နိုင်ရန် အမျိုးသားအဆင့်နှင့် ကဏ္ဍအလိုက် ယန္တရားများကိုဖော်ဆောင်ရန်၊

(ဃ) ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာနည်းပညာများဖြင့် ဆိုက်ဘာမှုခင်းများအပေါ် ကြိုတင်ကာကွယ်မှု၊ စုံစမ်းစစ်ဆေးမှုနှင့် တရားဥပဒေစိုးမိုးမှု မြှင့်တင်ရန်၊

(င) ပြည်ထောင်စုအဆင့်အဖွဲ့အစည်းများ၊ အစိုးရဌာန၊ အစိုးရအဖွဲ့အစည်းများ၊ ပုဂ္ဂလိက အဖွဲ့အစည်းနှင့် ပြည်သူများ၏ ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ အသိအမြင်ကို တိုးမြှင့်ပေးရန်၊

(စ) ဆိုက်ဘာလုံခြုံရေး ပိုမိုမြင့်မား တိုးတက်စေရန်အတွက် ဒေသတွင်းနှင့် နိုင်ငံတကာအဖွဲ့အစည်းများ အကြား အသိပညာများ မျှဝေ၍ ပြည်တွင်း၊ ပြည်ပ ပူးပေါင်းဆောင်ရွက်မှုများကို မြှင့်တင်ရန်၊

(ဆ) e-Government စနစ်နှင့် ဒီဂျစ်တယ် စီးပွားရေးစနစ်တည်ဆောက်မှုကို အထောက်အကူပြုရန်၊

အခန်း (၃)

နိုင်ငံတော်၏ ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ မူဝါဒ

၈။ နိုင်ငံတော်၏ ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ မူဝါဒမှာ အောက်ဖော်ပြပါအတိုင်း ဖြစ်သည်-

(က) ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ ဥပဒေ ပြဋ္ဌာန်းခြင်း၊ နည်းဥပဒေ၊ စည်းမျဉ်းဥပဒေ၊ စည်းကမ်းဥပဒေ၊ အမိန့်ကြော်ငြာစာ၊ အမိန့်၊ လုပ်ထုံးလုပ်နည်း၊ လမ်းညွှန်ချက်၊ ညွှန်ကြားချက်များနှင့်စံသတ်မှတ်ချက်များထုတ်ပြန်ရန်၊

(ခ) ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ စီမံခန့်ခွဲမှုယန္တရားကို စနစ်တကျ တည်ဆောက်ရန်၊

(ဂ) ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ အရေးကြီးသည့် ကဏ္ဍများကို သတ်မှတ်ဆောင်ရွက်ရန်၊

(ဃ) ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ လူ့စွမ်းအားအရင်းအမြစ်ဖွံ့ဖြိုးတိုးတက်ရေးနှင့် သုတေသန လုပ်ငန်းများကို ဆောင်ရွက်ရန်၊

(င) ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ ပြည်တွင်း၊ ဒေသတွင်းနှင့် နိုင်ငံတကာ ပူးပေါင်းဆောင်ရွက်မှုများကို တိုးမြှင့်ဆောင်ရွက်သွားရန်။

အခန်း (၄)

ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ ဥပဒေပြဋ္ဌာန်းခြင်း၊ ၊ နည်းဥပဒေ၊ စည်းမျဉ်းဥပဒေ၊ စည်းကမ်းဥပဒေ၊ အမိန့်ကြော်ငြာစာ၊ အမိန့်၊ လုပ်ထုံးလုပ်နည်း၊ လမ်းညွှန်ချက်၊ ညွှန်ကြားချက်များနှင့် စံသတ်မှတ်ချက်များ ထုတ်ပြန်ခြင်း

၉။ ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ ဥပဒေပြဋ္ဌာန်းခြင်း၊ နည်းဥပဒေ၊ စည်းမျဉ်းဥပဒေ၊ စည်းကမ်းဥပဒေ၊ အမိန့်ကြော်ငြာစာ၊ အမိန့်၊ လုပ်ထုံးလုပ်နည်း၊ လမ်းညွှန်ချက်၊ ညွှန်ကြားချက်များနှင့် စံသတ်မှတ်ချက်များ ထုတ်ပြန်ခြင်း ဆောင်ရွက်ရာတွင် အောက်ဖော်ပြပါ ရှုထောင့်တို့ကို ထည့်သွင်းစဉ်းစားရမည်-

(က) အီလက်ထရောနစ် သက်သေခံ လက်မှတ်ဆိုင်ရာနှင့် ပုဂ္ဂိုလ်အသုံးပြုမှု၊

(ခ) ဒီဂျစ်တယ်ငွေကြေး၊ အွန်လိုင်း (Online) ငွေပေးချေမှု၊ ရောင်းဝယ်မှုနှင့် အွန်လိုင်းမှတစ်ဆင့် ဆောင်ရွက်ပေးသော ဝန်ဆောင်မှုများ၊

(ဂ) အရေးကြီး သတင်းအချက်အလက် အခြေခံအဆောက်အဦ ကာကွယ်ရေး၊

(ဃ) ဆိုက်ဘာလုံခြုံရေးနှင့် ဆိုက်ဘာရာဇဝတ်မှုခင်း၊

(င) လူမှုကွန်ရက်အသုံးပြုမှုဆိုင်ရာ ကျင့်ဝတ်နှင့်ဥပဒေရေးရာ၊

(စ) ပုဂ္ဂိုလ်ရေးနှင့် အဖွဲ့အစည်းဆိုင်ရာ အချက်အလက်များ လုံခြုံရေးနှင့် ကာကွယ်ရေး၊

(ဆ) ဒီဂျစ်တယ်စွေးကွက် စီးပွားရေးစနစ်တွင် စားသုံးသူ ကာကွယ်ရေးနှင့် အခွန်စည်းကြပ်ခြင်းမှ ကင်းလွတ်နေမှုများ မရှိစေရေး အစီအမံများထားရှိမှု၊

(ဇ) တရားဥပဒေစိုးမိုးရေး အဖွဲ့အစည်းများက ဥပဒေနှင့် အညီ စုံစမ်းစစ်ဆေးမှုများ ဆောင်ရွက်ရာတွင် သတင်းအချက်အလက်နှင့် ဆက်သွယ်ရေးဝန်ဆောင်မှုပေးသည့် အဖွဲ့အစည်းများ၊ သက်ဆိုင်ရာ နိုင်ငံများနှင့် ပူးပေါင်းဆောင်ရွက်ရေး။

၁၀။ ပြည်သူများ၏ နေ့စဉ်လူမှုစီးပွားဘဝတွင် သတင်းအချက်အလက်နည်းပညာ၏ အကျိုးကျေးဇူးများ ခံစားနိုင်ရန်အတွက် လုံခြုံ စိတ်ချ၍ တည်ငြိမ်ကောင်းမွန်ကြံ့ခိုင်သော ဆိုက်ဘာဂေဟစနစ်ကို ကြိုးပမ်းတည်ဆောက်ပေးရမည်။ နိုင်ငံတော်လုံခြုံရေးနှင့် တရားဥပဒေ စိုးမိုးရေးကို မထိခိုက်စေဘဲ သတင်းအချက်အလက် လွတ်လပ်စွာ စီးဆင်းရေးကို စဉ်းစားဆောင်ရွက်သင့်ပြီး တစ်ချိန်တည်းမှာပင် ဆိုက်ဘာဂေဟစနစ်အပေါ် ခြိမ်းခြောက်မှုနှင့် တိုက်ခိုက်မှုများကြောင့် အမျိုးသားလုံခြုံရေးနှင့် အများပြည်သူတို့၏ အကျိုးစီးပွားကို ထိခိုက်မှု ကြုံတွေ့လာနိုင်ကြောင်း သတိပြုအလေးထား ဆောင်ရွက်ရမည်။

အခန်း (၅)

ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ စီမံခန့်ခွဲမှုယန္တရားကို စနစ်တကျတည်ဆောက်ခြင်း

၁၁။ ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ စီမံခန့်ခွဲမှုယန္တရားကို ဖော်ပြပါ အတိုင်း အကောင်အထည်ဖော် ဆောင်ရွက်သွားရမည်-

(က) ပို့ဆောင်ရေးနှင့် ဆက်သွယ်ရေးဝန်ကြီးဌာနသည် ဦးဆောင်ဝန်ကြီးဌာနအနေဖြင့် သက်ဆိုင်ရာဌာနများနှင့် ပူးပေါင်း၍ ဤမူဝါဒကို အကောင်အထည်ဖော် ဆောင်ရွက်ရမည်။

(ခ) ပို့ဆောင်ရေးနှင့် ဆက်သွယ်ရေးဝန်ကြီးဌာန၏ ကြီးကြပ်မှုဖြင့် သတင်းအချက်အလက် နည်းပညာနှင့် ဆိုက်ဘာလုံခြုံရေးဦးစီးဌာနသည် ဒေသတွင်းနှင့် နိုင်ငံတကာ ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ သဘောတူညီချက်များ၊ ပူးပေါင်းဆောင်ရွက်မှု အစီအစဉ်များကို တာဝန်ယူ ဆောင်ရွက်ခြင်း၊ သက်ဆိုင်ရာကဏ္ဍအလိုက် ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ တုံ့ပြန်ရေးနှင့် ပူးပေါင်းဆောင်ရွက်မှုအဖွဲ့များအား ကြီးကြပ်ခြင်း၊ ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ အသိပညာမြှင့်တင်ပေးခြင်းတို့ကို ဆောင်ရွက်ရမည်။

(ဂ) ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ ကိစ္စရပ်များကို အကောင်အထည်ဖော် ဆောင်ရွက်ရန်အတွက် ဌာနအလိုက်

သတင်းအချက်အလက် လုံခြုံရေးဆိုင်ရာအရာရှိ Chief Information Security Officer (CISO) တစ်ဦးကို ခန့်အပ်တာဝန်ပေးထားရမည်။

(ဃ) သက်ဆိုင်ရာကဏ္ဍအလိုက် ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ တုံ့ပြန်ရေးအဖွဲ့များ Cyber Security Incident Response Team (CSIRT) ဖွဲ့စည်းဆောင်ရွက်ရမည်။

(င) အရေးကြီး သတင်းအချက်အလက် အခြေခံ အဆောက်အဦ စီမံခန့်ခွဲရန် တာဝန်ရှိသူများ ပူးပေါင်း၍ သတင်းအချက်အလက် မျှဝေခြင်းနှင့် သရုပ်ခွဲလေ့လာဆန်းစစ်ခြင်းစင်တာ (Information Sharing and Analytic Center - ISAC) ကို ဖွဲ့စည်းဆောင်ရွက်ရမည်။

(စ) သတင်းအချက်အလက် နည်းပညာနှင့် ဆိုက်ဘာလုံခြုံရေးဦးစီးဌာနသည် CSIRT များ၊ ISAC တို့နှင့် ပေါင်းစပ်ညှိနှိုင်းဆောင်ရွက်ရမည်။

၁၂။ ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ လုပ်ငန်းစဉ်များ ပိုမို ထိရောက်စွာ အကောင်အထည်ဖော် ဆောင်ရွက်နိုင်ရေးအတွက် ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ ကော်မရှင် သို့မဟုတ် ကော်မတီတစ်ရပ်ကို ဥပဒေနှင့်အညီ ဖွဲ့စည်းနိုင်ရေးကို ရည်ရွယ်ဆောင်ရွက်သွားရမည်။

အခန်း (၆)

ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ အရေးကြီးသည့်ကဏ္ဍများကို သတ်မှတ်ဆောင်ရွက်ခြင်း

၁၃။ လုံခြုံစိတ်ချ၍ တည်ငြိမ်ကောင်းမွန်ကြံ့ခိုင်သော ဆိုက်ဘာနယ်ပယ်တစ်ခု တည်ဆောက်ရေးအတွက် အောက်ဖော်ပြပါအတိုင်း ဦးစားပေးကဏ္ဍများ သတ်မှတ်ဆောင်ရွက်ရမည်-

(က) အစိုးရအဖွဲ့အစည်းများ၏ ကဏ္ဍ၊

(ခ) အရေးကြီး သတင်းအချက်အလက် အခြေခံအဆောက်အဦများ၏ ကဏ္ဍ၊

(ဂ) ပုဂ္ဂလိက အဖွဲ့အစည်း/ ကုမ္ပဏီများ၏ ကဏ္ဍ၊

(ဃ) လူပုဂ္ဂိုလ်တစ်ဦးချင်းစီ၏ ကဏ္ဍ၊

(င) ပညာရေးနယ်ပယ်၊ တက္ကသိုလ်များနှင့် သင်တန်းကျောင်းများမှ သုတေသနအဖွဲ့အစည်းများ၏ ကဏ္ဍတို့ ဖြစ်သည်။

အစိုးရအဖွဲ့အစည်းများ၏ကဏ္ဍ

၁၄။ ပြည်ထောင်စုအဆင့်အဖွဲ့အစည်းများ၊ အစိုးရဌာန၊ အစိုးရအဖွဲ့အစည်းများ၏ သတင်းအချက်အလက် အများစုသည် အရေးကြီးသော သတင်းအချက်အလက်များဖြစ်ပြီး ပေါက်ကြားသွားလျှင်ဖြစ်စေ၊ ဖျက်ဆီးခံရလျှင်ဖြစ်စေ၊ မမှန်မကန် အသုံးပြုခြင်းခံရလျှင်ဖြစ်စေ မလိုလားအပ်သော အကျိုးဆက်များ ဖြစ်ပေါ်လာနိုင်သည်။ e-Government စနစ်

တည်ထောင်ခြင်းကြောင့် အစိုးရနှင့် အခြားသော အဖွဲ့အစည်းများကြား ဆက်သွယ်မှုများသည် ဆိုက်ဘာကွန်ရက်ပေါ်တွင် ပိုမိုမှီခိုလာရပြီး အုပ်ချုပ်ရေးဆိုင်ရာ ဝန်ဆောင်မှုများကိုလည်း အွန်လိုင်းမှ တစ်ဆင့်သာ ဆောင်ရွက်လာကြမည် ဖြစ်သည်။ အဆိုပါအုပ်ချုပ်ရေးဆိုင်ရာ ဝန်ဆောင်မှု စနစ်များကို ကြားဝင်နှောင့်ယှက်ခြင်း ခံရမည်ဆိုပါက ပြည်သူများ၏ ပုဂ္ဂလိကပိုင်ဆိုင်မှုများ၊ စီးပွားရေးလုပ်ငန်းများသာမက နိုင်ငံတော်လုံခြုံရေးအထိပါ ထိခိုက်နိုင်ပါသည်။ ထို့ကြောင့် အုပ်ချုပ်ရေးဆိုင်ရာ ဝန်ဆောင်မှုစနစ်များကို တစ်စုံတစ်ရာ ကြားဝင်နှောင့်ယှက်ခြင်း မဖြစ်အောင် ကာကွယ်ရမည်။

၁၅။ ပြည်ထောင်စုအဆင့်အဖွဲ့အစည်းများ၊ အစိုးရဌာန၊ အစိုးရအဖွဲ့အစည်းများအနေဖြင့် မြန်မာနိုင်ငံ၏ ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ အခြေခံအဆောက်အဦများကို အားဖြည့်ရန်နှင့် သက်ဆိုင်ရာ အဖွဲ့အစည်းအားလုံးတို့၏ အခန်းကဏ္ဍ အလိုက် အချင်းချင်း ပူးပေါင်းဆောင်ရွက်နိုင်ရေးကို အားပေးရမည်။ ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာစနစ်များနှင့် အဖွဲ့အစည်းများကို တည်ထောင်ခြင်း၊ ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ အသိပညာဖွံ့ဖြိုးတိုးတက်ရန်အတွက် သင်တန်းများ ဖွင့်လှစ်ပေးခြင်း၊ ဝန်ထမ်းများ၏ သတင်းအချက်အလက် နည်းပညာကျွမ်းကျင်မှုကို မြှင့်တင်ပေးခြင်း စသည်တို့ကို ဆောင်ရွက်ရမည်။

၁၆။ ဆိုက်ဘာလုံခြုံရေးကို ထိထိရောက်ရောက် မြှင့်တင်ဆောင်ရွက်ပေးရမည့် အဓိကအဖွဲ့အစည်းအဖြစ် တာဝန်ပေးအပ်ခြင်းခံရသော ဦးစီး

ဌာနသည် အစိုးရယန္တရားတစ်ခုလုံးအတွက် ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ စံနှုန်းများ ပြုစုခြင်း၊ ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ အသိပညာ ဖွံ့ဖြိုးတိုးတက်ရန် ဆောင်ရွက်ခြင်း၊ ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ ခြိမ်းခြောက်တိုက်ခိုက်မှုများကို စောင့်ကြည့်စစ်ဆေး တုံ့ပြန်ခြင်းနှင့် ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာပြဿနာများကို နိုင်ငံတကာနှင့် ပူးပေါင်းကိုင်တွယ် ဖြေရှင်းခြင်း စသည်တို့ကို ဆောင်ရွက်ရမည်။ ထို့အပြင် ပုဂ္ဂလိကကဏ္ဍရှိ ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ အသိပညာရှင်များနှင့် ပူးပေါင်း၍ ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ ကိစ္စရပ်များအား ဖြေရှင်းဆောင်ရွက်ရမည်။

၁၇။ သတင်းအချက်အလက်နည်းပညာနှင့် ဆိုက်ဘာလုံခြုံရေးဦးစီးဌာနသည် ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ ခြိမ်းခြောက်တိုက်ခိုက်မှုများအား အရေးပေါ်ဖြေရှင်းမှုများ ဆောင်ရွက်နိုင်ရေး အစိုးရဆိုက်ဘာလုံခြုံရေး အော်ပရေးရှင်း စင်တာ (Government Security Operation Center - GSOC) ကို တည်ထောင်ရမည်။

အရေးကြီးသတင်းအချက်အလက်အခြေခံအဆောက်အဦများ၏ကဏ္ဍ

၁၈။ အရေးကြီး သတင်းအချက်အလက် အခြေခံအဆောက်အဦ ဆိုသည်မှာ အစားထိုးလဲလှယ်ရန် အလွန်ခက်ခဲသော ဝန်ဆောင်မှုများ ပေးစွမ်းသည့် လုပ်ငန်းများကို ဆိုလိုခြင်းဖြစ်သည်။ အမျိုးသားလုံခြုံရေး၊ လမ်းပန်းဆက်သွယ်ရေး၊ ဘဏ္ဍာရေး၊ ငွေရေးကြေးရေး၊ ကျန်းမာရေး၊ သတ္တုတွင်း၊ အစိုးရနှင့် အုပ်ချုပ်ရေးပိုင်း ဝန်ဆောင်မှုလုပ်ငန်းများ၊

သတင်းအချက်အလက်နှင့် ဆက်သွယ်ရေး နည်းပညာ၊ လျှပ်စစ်နှင့် စွမ်းအင်ဆိုင်ရာ အခြေခံအဆောက်အဦများ စသည်တို့သည် အရေးကြီး သတင်းအချက်အလက် အခြေခံ အဆောက်အဦများ ဖြစ်သည်။ အရေးကြီးသတင်း အချက်အလက် အခြေခံအဆောက်အဦကို ဆိုက်ဘာ လုံခြုံရေးဆိုင်ရာ ခြိမ်းခြောက်တိုက်ခိုက်မှုခံရလျှင် လုံခြုံရေး၊ အုပ်ချုပ် ရေးဆိုင်ရာ ယန္တရားများနှင့် နေ့စဉ်လူမှုစီးပွားလုပ်ငန်းစဉ်များကို ထိခိုက် လာနိုင်သည့်အတွက် အရေးကြီး သတင်းအချက်အလက် အခြေခံ အဆောက်အဦများအား စီမံထိန်းသိမ်းရန် တာဝန်ရှိသူအနေဖြင့် အဆိုပါ ခြိမ်းခြောက်တိုက်ခိုက်မှုများအားလုံးကို ကာကွယ်ပေးရမည်။

၁၉။ ပြည်ထောင်စုအဆင့်အဖွဲ့အစည်းများ၊ အစိုးရဌာန၊ အစိုးရအဖွဲ့ အစည်းများအနေဖြင့် စီမံချက်များအပေါ် အခြေခံပြီး အရေးကြီး သတင်း အချက်အလက် အခြေခံအဆောက်အဦကို ရွေးချယ်သတ်မှတ်၍ သက်ဆိုင်ရာ အဖွဲ့အစည်းများနှင့် ပူးပေါင်းပြီး ဆိုက်ဘာလုံခြုံရေး အဆင့် မြှင့်တင် ဆောင်ရွက်သွားရမည်။

၂၀။ အရေးကြီး သတင်းအချက်အလက် အခြေခံ အဆောက်အဦများ အား စီမံထိန်းသိမ်းရန် တာဝန်ရှိသူသည် ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ ခြိမ်းခြောက် တိုက်ခိုက်မှုများကို ဖြေရှင်းခြင်း၊ စဉ်ဆက်မပြတ် ဝန်ဆောင်မှုပေးနေသည့် စနစ်များအား ကြားဝင်နှောင့်ယှက်မှုမှ ကာကွယ်ခြင်း၊ သတင်းအချက်အလက်စနစ် ပြတ်တောက်မှုကို ကာကွယ် ခြင်း၊ သတင်းအချက်အလက်စနစ် ချို့ယွင်းမှုများ ဖြစ်ပေါ်လာပါက

တည်ငြိမ်သော ဆိုက်ဘာလုံခြုံရေး ဆောင်ရွက်ချက်များ အကောင်အထည်ဖော်ခြင်း၊ ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ အရေးပေါ်တုံ့ပြန်မှု အစီအစဉ်များ ရေးဆွဲခြင်း၊ ဗိုင်းရပ်စ်အန္တရာယ်ကို ကာကွယ်ရန် အတွက် သက်ဆိုင်ရာအဖွဲ့အစည်းများကို ချက်ချင်း အသိပေးခြင်း၊ ဖြစ်ပေါ်လာသော သတင်းအချက်အလက်ပိုင်းဆိုင်ရာ လုံခြုံရေးအန္တရာယ်များကို ကာကွယ်နိုင်ရန် သတင်းအချက်အလက်လုံခြုံရေး စီမံခန့်ခွဲရေးတွင် (Information Security Management System -ISMS) စနစ်၏ စံနှုန်းများအတိုင်း အကောင်အထည်ဖော်ခြင်းတို့ကို ဆောင်ရွက်ရမည်။

၂၁။ အရေးကြီး သတင်းအချက်အလက် အခြေခံ အဆောက်အဦများအား စီမံထိန်းသိမ်းရန် တာဝန်ရှိသူသည် ဆိုက်ဘာလုံခြုံရေး ဆောင်ရွက်ချက်များ ထိရောက်အောင်မြင်စေရန်အတွက် Information Sharing and Analytics Center (ISAC) ဖွဲ့စည်းခြင်း၊ လုံခြုံရေးစံနှုန်းများ (Safety Standards) သတ်မှတ်ခြင်း စသည်တို့ကို စီမံဆောင်ရွက်ရမည်။ ဆောင်ရွက်ထားရှိမှုအပေါ် စံနှုန်းများနှင့် ကိုက်ညီမှု ရှိ၊ မရှိ စစ်ဆေး၍ မှတ်တမ်းတင်ထားရှိရမည်။

၂၂။ အရေးကြီး သတင်းအချက်အလက် အခြေခံ အဆောက်အဦများအား စီမံထိန်းသိမ်းရန် တာဝန်ရှိသူများသည် စက်ပိုင်းဆိုင်ရာ ကာကွယ်ရေး၊ နည်းပညာပိုင်းဆိုင်ရာ တည်ဆောက်ရေးနှင့် တုံ့ပြန်ရေးများတွင် စွမ်းဆောင်ရည်ကို ဖြည့်တင်းမြှင့်တင်ရမည်။

၂၃။ သတင်းအချက်အလက် နည်းပညာနှင့် ဆိုက်ဘာလုံခြုံရေးဦးစီး

ဌာနသည် ပြည်ထောင်စုအဆင့် အဖွဲ့အစည်းများ၊ အစိုးရဌာန၊ အစိုးရ အဖွဲ့အစည်းများ၊ သက်ဆိုင်ရာအဖွဲ့အစည်းများနှင့် အရေးကြီး သတင်း အချက်အလက် အခြေခံအဆောက်အဦများအတွက် လိုအပ်သော ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ ပြင်ဆင်ဆောင်ရွက်ချက်များကို စံချိန်စံနှုန်း များနှင့် ကိုက်ညီစွာ ဆောင်ရွက်ထားခြင်း ရှိ၊ မရှိကို လုပ်ထုံးလုပ်နည်း များနှင့်အညီ စစ်ဆေးပြီး လိုအပ်သည်များ ညှိနှိုင်းဖြေရှင်း ဆောင်ရွက် သွားရမည်။

ပုဂ္ဂလိကအဖွဲ့အစည်း/ ကုမ္ပဏီများ၏ကဏ္ဍ

၂၄။ ပုဂ္ဂလိကကုမ္ပဏီများ ထိန်းသိမ်းရသည့် သတင်းအချက်အလက် များတွင် နည်းပညာဆိုင်ရာ သတင်းအချက်အလက်များ၊ ဘဏ္ဍာရေး ဆိုင်ရာ သတင်းအချက်အလက်များ၊ ဥဇာပစ္စည်းဆိုင်ရာ မူပိုင်ခွင့်နှင့် သက်ဆိုင်သော သတင်းအချက်အလက်များ (ဥပမာ- ကုန်ထုတ်လုပ်မှု နည်းလမ်းများ) နှင့် ကိုယ်ရေးဆိုင်ရာအချက်အလက်များ ပါဝင်သည်။

၂၅။ ပုဂ္ဂလိက အဖွဲ့အစည်း/ ကုမ္ပဏီများသည် နိုင်ငံ၏ စီးပွားရေး ဖွံ့ဖြိုးတိုးတက်ရန်အတွက် အဓိကကျသော အခန်းကဏ္ဍမှ ပါဝင်ကြ သည်။ ထို့ကြောင့် ၎င်းတို့အနေဖြင့် ဆိုက်ဘာလုံခြုံရေးကို မြှင့်တင် ဆောင်ရွက်ရန် လိုအပ်ပြီး ဆိုက်ဘာတိုက်ခိုက်မှုများကို ပြန်လည်တုံ့ပြန် နိုင်စေရန်အတွက် စွမ်းဆောင်ရည်မြှင့်တင်ပေးခြင်း၊ လုပ်ငန်းခွင်အတွင်း ဆိုက်ဘာလုံခြုံရေးအသိ၊ သတိရှိရန်နှင့် လူ့စွမ်းအားအရင်းအမြစ် ဖွံ့ဖြိုး

တိုးတက်ရန် မြှင့်တင်ဆောင်ရွက်ပေးခြင်း စသည့်လုပ်ငန်းစဉ်များကို ဦးစားပေးဆောင်ရွက်သွားရမည်။

လူပုဂ္ဂိုလ်တစ်ဦးချင်းစီ၏ ကဏ္ဍ

၂၆။ မိုဘိုင်းဖုန်းများ၊ အဆင့်မြင့်လုပ်ဆောင်ချက် (Function) များပါဝင်သော အီလက်ထရောနစ် ပစ္စည်းများနှင့် မိုဘိုင်းစနစ်ဖြင့် ဘဏ်ဝန်ဆောင်မှု (Mobile Banking) ကဲ့သို့သော ဝန်ဆောင်မှုစနစ်များကို အင်တာနက် (Internet) နှင့် အချိန်ပြည့်ချိတ်ဆက်ပြီး နေရာဒေသမရွေး သယ်ဆောင် အသုံးပြုလာကြသည်။ ထို့ကြောင့် အင်တာနက်နှင့် အွန်လိုင်း အပလီကေးရှင်းများ (Internet and Online Applications)၊ အွန်လိုင်း ဝန်ဆောင်မှုများ (Online Services) သုံးစွဲသူများအနေဖြင့် ဆိုက်ဘာလုံခြုံရေးကို နားလည်ပြီး လိုက်နာရန် လိုအပ်သည်။ ဆိုက်ဘာလုံခြုံရေးကျိုးပေါက်ပါက အသုံးပြုသူကိုယ်တိုင် ဆုံးရှုံးရုံသာမက ၎င်းနှင့်ဆက်စပ်သော အဖွဲ့အစည်းများသို့လည်း အန္တရာယ်များ သက်ရောက်စေနိုင်ပါသည်။

၂၇။ လူပုဂ္ဂိုလ်တစ်ဦးချင်းစီ၏ ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ အသိပညာတိုးမြင့်လာပါက အသုံးပြုသူ ကိုယ်တိုင်သာမက အခြားသူများအတွက်ပါ ဆိုက်ဘာလုံခြုံရေး ကျိုးပေါက်မှုရန်မှ ကာကွယ်နိုင်မည် ဖြစ်သောကြောင့် ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ အသိပညာပေး အစီအစဉ်များကို စဉ်ဆက်မပြတ် လေ့လာပြီး လိုက်နာကျင့်သုံးရမည်။

ပညာရေးနယ်ပယ်၊ တက္ကသိုလ်များနှင့် သင်တန်းကျောင်းများမှ သုတေသနအဖွဲ့အစည်းများ၏ ကဏ္ဍ

၂၈။ တက္ကသိုလ်များ၊ သင်တန်းကျောင်းများနှင့် သုတေသနအဖွဲ့အစည်းများကဲ့သို့သော အဆင့်မြင့်ပညာရေးအဖွဲ့များသည် ဆိုက်ဘာလုံခြုံရေးကဏ္ဍ ဖွံ့ဖြိုးတိုးတက်ရေးနှင့် လူ့စွမ်းအားအရင်းအမြစ်များ ဖွံ့ဖြိုးတိုးတက်ရေးအတွက် အဓိကကျသည်။ ၎င်းတို့အနေဖြင့် ဝန်ထမ်းများနှင့် ကျောင်းသား/ ကျောင်းသူများကို လေ့ကျင့်ပညာသင်ကြား ပေးသကဲ့သို့ ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ သုတေသနနှင့် ဖွံ့ဖြိုးရေးလုပ်ငန်းများကိုလည်း ဆောင်ရွက်ရန်လိုအပ်ပါသည်။ ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ လူ့စွမ်းအားအရင်းအမြစ် မွေးထုတ်မြှင့်တင်နိုင်ရန် လိုအပ်သည့် သင်ရိုးများ ပြဋ္ဌာန်းခြင်း၊ စီမံချက်များရေးဆွဲခြင်း စသည်တို့ကို ဆောင်ရွက်ရမည်။

အခန်း (၇)

လူ့စွမ်းအားအရင်းအမြစ်ဖွံ့ဖြိုးတိုးတက်ရေးကို ဆောင်ရွက်ခြင်း

၂၉။ လုံခြုံစိတ်ချ၍ တည်ငြိမ်ကောင်းမွန် ကြံ့ခိုင်သော ဆိုက်ဘာနယ်ပယ်တစ်ခု အောင်မြင်စွာ ထူထောင်နိုင်ရန် အဖွဲ့အစည်း/ ဌာန တစ်ခုချင်းစီတိုင်းတွင် ဆိုက်ဘာလုံခြုံရေး ဆောင်ရွက်ချက်များ ချမှတ်ရန် လိုအပ်ပြီး အသိပညာနှင့် စွမ်းရည်ပြည့်ဝသော ပုဂ္ဂိုလ်များကို ပြုစုပျိုးထောင်ပြီး မြေတောင်မြှောက်ပေးရမည်ဖြစ်သည်။ ထို့အပြင် ဆိုက်ဘာလုံခြုံရေးအဆင့်ကို မြှင့်တင်ရန်အတွက် လိုအပ်ချက်များကို ပံ့ပိုးပေးသည့်

ရပ်ဝန်းတစ်ခုတည်ဆောက်ရန် ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ အသိပညာ မြှင့်တင်ပေးရေးကို ဆောင်ရွက်ရမည်။

၃၀။ မြန်မာနိုင်ငံအနေဖြင့် အမျိုးသားလုံခြုံရေးကဏ္ဍအတွက် မရှိမဖြစ် အသုံးပြုရမည့် နည်းပညာများကို သုတေသနပြုရန်နှင့် အဆင့်မြှင့်တင်ပေးရန် ကြိုးပမ်းဆောင်ရွက်သွားရမည်။ သုတေသနနှင့် ဖွံ့ဖြိုးရေး လုပ်ငန်းများမှတစ်ဆင့် နိုင်ငံကို အထောက်အကူပြုနိုင်ရန် နည်းပညာ စွမ်းရည်ကို ဟန်ချက်ညီညီ ကူညီပံ့ပိုးပေးနိုင်မည့် သုတေသီများနှင့် အသိပညာရှင်၊ အတတ်ပညာရှင်များကို သက်ဆိုင်ရာဝန်ကြီး ဌာနက အားပေးကူညီရမည်။

၃၁။ ပြည်ထောင်စုအဆင့်အဖွဲ့အစည်းများ၊ အစိုးရဌာန၊ အစိုးရအဖွဲ့ အစည်းများတွင် ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ ကျွမ်းကျင်သည့် ဝန်ထမ်းများ မရှိမဖြစ်လိုအပ်သည့်အတွက် သတင်းအချက်အလက် စနစ်လုံခြုံမှု ကြီးကြပ်ရေးကဏ္ဍတွင် လူစွမ်းအားအရင်းအမြစ် ဖွံ့ဖြိုးတိုးတက်အောင် ဆောင်ရွက်ပေးရမည်ဖြစ်ပြီး တက္ကသိုလ်များ၊ ဒီဂရီကောလိပ်များ၊ ကောလိပ်များနှင့်လည်း ပူးပေါင်းသွားရမည် ဖြစ်သည်။

၃၂။ ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ အသိပညာ မြှင့်တင်ရန်အတွက် ပြည်ထောင်စုအဆင့် အဖွဲ့အစည်းများ၊ အစိုးရဌာန၊ အစိုးရအဖွဲ့အစည်း များရှိ ဝန်ထမ်းများကို သင်တန်းများ ပို့ချလေ့ကျင့်ပေးရမည်။ အစိုးရ ဝန်ထမ်းများအားလုံးအတွက် ပညာပေးအစီအစဉ်ကို အကောင်အထည် ဖော်ပေးပြီး အထွေထွေ အသိပညာများ ဖြန့်ဝေပေးသွားရမည့်အပြင်

ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ တိုက်ခိုက်မှုများကို ကာကွယ်ခြင်း နည်းလမ်းများ၊ တုံ့ပြန်ခြင်း သင်ခန်းစာများကို သင်ကြားပို့ချပေးရမည်။

၃၃။ ဆိုက်ဘာကွန်ရက်စနစ်ကို လူကြီး၊ လူငယ်မရွေး၊ အချိန်မရွေး၊ နေရာမရွေး၊ နေ့စဉ် လူမှုစီးပွား လုပ်ငန်းများတွင် ကျယ်ကျယ်ပြန့်ပြန့် အသုံးပြုနေကြပြီ ဖြစ်သည့်အတွက် လူပုဂ္ဂိုလ် တစ်ဦးချင်းစီတိုင်း ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ အန္တရာယ်များ သိရှိနားလည်စေရန်နှင့် ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ ဆောင်ရွက်ချက်များ ပြုလုပ်ကြရန် အသိပညာ မျှဝေပေးရမည်။ ထို့ကြောင့် ပြည်သူလူထုကို ဆိုက်ဘာလုံခြုံရေး ဆောင်ရွက်ချက်များနှင့် လူစွမ်းအား အရင်းအမြစ် ဖွံ့ဖြိုးတိုးတက်ရေးတို့အတွက် အသိပညာပေးခြင်းများ ပြုလုပ်သွားရမည်။

၃၄။ အခြေခံပညာနှင့် အဆင့်မြင့်ပညာ ကျောင်းသူ၊ ကျောင်းသားများကို ကွန်ပျူတာ၊ သတင်းအချက်အလက်နှင့် ဆက်သွယ်ရေး၊ ကွန်ရက်လုံခြုံရေးဆိုင်ရာတို့ကို အသိပညာပေးခြင်းနှင့် ကျောင်းသား၊ ကျောင်းသူများ၏ ဖွံ့ဖြိုးရေး အဆင့်များအရ ဆိုက်ဘာလုံခြုံရေး အပါအဝင် သတင်းအချက်အလက်ဆိုင်ရာ အသိပညာ မြှင့်တင်ပေးခြင်းနှင့် သင်ရိုးအစီအစဉ်များတွင် သင့်လျော်သလို ထည့်သွင်းခြင်းတို့ကို ဆောင်ရွက်ရမည်။

၃၅။ လူစွမ်းအားအရင်းအမြစ် ဖွံ့ဖြိုးတိုးတက်ရေးအတွက် ပံ့ပိုးပေးသည့်အပိုင်းတွင် တက္ကသိုလ်များ၌ လက်တွေ့ပိုင်းနှင့် အခြေခံကျသော ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ သင်ရိုးအစီအစဉ်များကို သင်ကြားပို့ချသွားရန် ဆောင်ရွက်ရမည်။

၃၆။ ဆိုက်ဘာလုံခြုံရေး အန္တရာယ်များ၏ သဘောသဘာဝအရ တိုက်ခိုက်မှုများအားလုံးကို တုံ့ပြန်ဖြေရှင်းနိုင်ရန် ခက်ခဲပါသည်။ ထို့ကြောင့် တိုက်ခိုက်မှုများကို ကာကွယ်ရန်နှင့် တုံ့ပြန်ဖြေရှင်းနိုင်ရန် အတွက် ဝန်ဆောင်မှုပေးသည့် ဝဘ်ဆိုဒ်များ၊ ဆော့ဖ်ဝဲများ၊ Application များ၏ အားနည်းချက်များကို ရှာဖွေပြီး သတိထားရမည့်အချက်များကို သက်ဆိုင်ရာသို့ အသိပေးခြင်းဖြင့် ကာကွယ်တားဆီးရေး ဆောင်ရွက်ချက်များ ပြုလုပ်ခြင်း၊ ဆိုက်ဘာတိုက်ခိုက်ခံရသည့် သတင်းအချက်အလက်နည်းပညာမျှဝေခြင်း၊ သင့်တော်သောတုံ့ပြန်မှုများ အလျင်အမြန် ဆောင်ရွက်ခြင်းနှင့် ပျက်စီးဆုံးရှုံးမှုများ တတ်နိုင်သမျှ လျော့နည်းအောင် ကာကွယ်ခြင်းအစရှိသည့် စီမံချက်များကို ရေးဆွဲ အကောင်အထည်ဖော်ရန် လိုအပ်ပါသည်။ နိုင်ငံတော်အဆင့်တွင် ဆိုက်ဘာလုံခြုံရေး စံနှုန်းများကို အဆင့်မြှင့်တင်နိုင်စေရန်အတွက် ဦးဆောင်ဝန်ကြီးဌာနနှင့် ဆက်စပ်အစိုးရဌာနများက စီမံချက်များကို ဦးဆောင်ချမှတ်ရမည်ဖြစ်ပြီး မိမိတို့၏ တုံ့ပြန်မှုစွမ်းဆောင်ရည်ကို နည်းလမ်းတကျ မြှင့်တင်ရမည်။

အခန်း (၈)

ပြည်တွင်း၊ ဒေသတွင်းနှင့် နိုင်ငံတကာပူးပေါင်း ဆောင်ရွက်မှုများကို တိုးမြှင့်ဆောင်ရွက်ခြင်း

၃၇။ ကမ္ဘာတစ်ဝှမ်း၌ ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ ခြိမ်းခြောက်တိုက်ခိုက်မှုများ သိသိသာသာ တိုးမြင့်ဖြစ်ပွားလာသဖြင့် မြန်မာနိုင်ငံ

သည်လည်း အထူးအလေးထား သတိပြုရန် လိုအပ်သည်။ ဘဏ္ဍာရေး ဝန်ဆောင်မှု၊ ငွေရေးကြေးရေးဝန်ဆောင်မှုနှင့် ဆက်သွယ်ရေးဝန်ဆောင်မှုလုပ်ငန်းများကဲ့သို့သော လုပ်ငန်းနယ်ပယ်များတွင်လည်း ခြိမ်းခြောက်မှုများ တဖြည်းဖြည်း မြင့်တက်လာပြီး ထိုခြိမ်းခြောက်မှုများကို ကောင်းမွန်စွာ ကိုင်တွယ်ဖြေရှင်းရမည် ဖြစ်သည်။

၃၈။ မြန်မာနိုင်ငံ၏ စဉ်ဆက်မပြတ် ဖွံ့ဖြိုးတိုးတက်မှုကို ထိန်းသိမ်းရန်နှင့် နိုင်ငံသားများအတွက် ပိုမိုကောင်းမွန်သော လူနေမှုဘဝများ ဖန်တီးပေးနိုင်ရန်အတွက် မိမိတို့၏ သတင်းအချက်အလက် ဆက်သွယ်ရေး နည်းပညာ အခြေခံအဆောက်အဦများကို ခိုင်မာပြီး ယုံကြည်စိတ်ချရစေရေး အားဖြည့်ဆောင်ရွက်ရမည် ဖြစ်သည်။ ထို့ကြောင့် သတင်း အချက်အလက် ဆက်သွယ်ရေးနည်းပညာ အဖွဲ့အစည်းတွင် ပါဝင်သော ဌာန/ အဖွဲ့အစည်းများအနေဖြင့် လုံခြုံမှုရှိသည့် သတင်းအချက်အလက် ဆက်သွယ်ရေး နည်းပညာရပ်ဝန်းကို ပူးပေါင်းတည်ဆောက်ရမည် ဖြစ်သည်။

၃၉။ ပို့ဆောင်ရေးနှင့် ဆက်သွယ်ရေးဝန်ကြီးဌာန၏ ကြီးကြပ်ကွပ်ကဲမှုဖြင့် ဆိုက်ဘာလုံခြုံရေး ပညာရှင်များ ပါဝင်သော အစိုးရ/ပုဂ္ဂလိက အဖွဲ့အစည်းတစ်ရပ်ကို ဖွဲ့စည်း၍ လိုအပ်သော အသိပညာမျှဝေခြင်း၊ ပူးပေါင်းဖြေရှင်းခြင်းတို့ကို ပိုမိုထိရောက်စွာ ဆောင်ရွက်ရမည်။

၄၀။ ပို့ဆောင်ရေးနှင့် ဆက်သွယ်ရေးဝန်ကြီးဌာနသည် နိုင်ငံလုံးဆိုင်ရာ ဆိုက်ဘာလုံခြုံရေးစီမံချက်များကို ရေးဆွဲချမှတ်ပြီး၊ ဌာန/ အဖွဲ့အစည်းများက မိမိတို့နှင့် သက်ဆိုင်သည့် စီမံချက်လုပ်ငန်း တာဝန်များ

ကို အောင်မြင်စွာ အကောင်အထည်ဖော် ဆောင်ရွက်ရန် တာဝန်ရှိသည်။

၄၁။ ဆိုက်ဘာကွန်ရက်များတွင် ခြိမ်းခြောက်လာသည့် ပြဿနာများ ပိုမိုများပြားလာသဖြင့် ပြည်ထောင်စုအဆင့် အဖွဲ့အစည်းများ၊ အစိုးရဌာန၊ အစိုးရအဖွဲ့အစည်းများအနေဖြင့် ဆိုက်ဘာလုံခြုံရေးအတွက် အစိုးရနှင့် ပုဂ္ဂလိက အဖွဲ့အစည်းများအချင်းချင်း ပူးပေါင်းဆောင်ရွက်ကြရန် လိုအပ်ပါသည်။

၄၂။ တစ်ကမ္ဘာလုံးဆိုင်ရာ စီးပွားရေးပေါင်းစည်းခြင်းနှင့် သတင်းအချက်အလက် ဆက်သွယ်ရေးနည်းပညာကို လက်တွေ့အသုံးပြုလာကြခြင်းတို့ကြောင့် နိုင်ငံလုံးဆိုင်ရာ ဆိုက်ဘာလုံခြုံရေးအခြေခံ အဆောက်အဦများ တည်ဆောက်ရန်သာမက အပြည်ပြည်ဆိုင်ရာ ဆိုက်ဘာလုံခြုံရေး အခြေခံအဆောက်အဦများ ထူထောင်ရန် လိုအပ်လာပါသည်။ ထို့ကြောင့် ဆိုက်ဘာလုံခြုံရေးနယ်ပယ်တွင် နိုင်ငံတကာနှင့် ပူးပေါင်းမှုမြှင့်တင်ဆောင်ရွက်ရန်အတွက် အောက်ပါမူဝါဒများကို အဓိကထား ဆောင်ရွက်သွားရမည်-

(က) **လုံခြုံစိတ်ချရသော ဆိုက်ဘာကွန်ရက်တစ်ခု ထူထောင်ရန်အတွက် နိုင်ငံတကာနှင့် ပူးပေါင်းခြင်း။**

ခွင့်ပြုချက်မရဘဲ ကွန်ရက်အတွင်း၊ ကွန်ပျူတာစနစ်အတွင်းသို့ ဝင်ရောက်ခြင်း၊ ဖြန့်ဝေခြင်း၊ Spam များ၊ DDoS တိုက်ခိုက်မှုများ၊ ဝဘ်ဆိုဒ်များမှ Malware ကူးစက်မှုများစသည့် ဆိုက်ဘာတိုက်ခိုက်မှုများသည်

နယ်စပ်ဖြတ်ကျော် ဖြစ်ပွားလေ့ရှိသည်။ အဆိုပါ တိုက်ခိုက်မှုများသည် တည်နေရာ၊ ယဉ်ကျေးမှုအရ၊ နိုင်ငံရေးအရ၊ ဘာသာရေးအရ၊ စီးပွားရေးအရ စသည် ဖြင့် ဆက်စပ်မှုရှိနေသဖြင့် ဒေသတွင်း နိုင်ငံများနှင့် ဆိုက်ဘာလုံခြုံရေး ပူးပေါင်းဆောင်ရွက်မှုများ ပြုလုပ် ရမည်။ အာဆီယံပြင်ပ အခြားသော နိုင်ငံများရှိ ကွန်ပျူတာ အရေးပေါ် တုံ့ပြန်ရေးအဖွဲ့ (Computer Emergency Response Team - CERT) အဖွဲ့များနှင့် ပူးပေါင်းပြီး နိုင်ငံတကာနှင့် ချိတ်ဆက်မှုကို မြှင့်တင် ရမည် ဖြစ်သည်။

(ခ) **နိုင်ငံတကာနှင့် ပူးပေါင်းခြင်းဖြင့် လူ့စွမ်းအား အရင်း အမြစ် ဖွံ့ဖြိုးတိုးတက်အောင် ဆောင်ရွက်ခြင်း။** နိုင်ငံတကာနှင့် သတင်းအချက်အလက် ဖလှယ်ခြင်း၊ အသိပညာ မျှဝေခြင်း၊ လူ့စွမ်းအား အရင်းအမြစ် ဖွံ့ဖြိုး တိုးတက်ရေးအတွက် သင်တန်းများ၊ ဆွေးနွေးပွဲများ တက်ရောက်ခြင်း၊ နားလည်မှုစာချွန်လွှာများ ရေးထိုးခြင်း တို့ကို ဆောင်ရွက်ရမည်။

အခန်း (၉)

နိဂုံး

၄၃။ ဤဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ မူဝါဒသည် နိုင်ငံတကာနှင့် မြန်မာနိုင်ငံ၏ ဆိုက်ဘာလုံခြုံရေး အတွေ့အကြုံကောင်းများကို လေ့လာပြီး ရေးဆွဲထားခြင်းဖြစ်ပါသည်။ ပြည်သူတို့၏ နေ့စဉ်ဘဝ၊ လူမှုစီးပွားလုပ်ငန်းများနှင့် ကျယ်ကျယ်ပြန့်ပြန့် ဆက်စပ်နေသည့်အတွက် ဤမူဝါဒကို အကောင်အထည်ဖော်ရန် ပြည်ထောင်စုအဆင့် အဖွဲ့အစည်းများ၊ အစိုးရဌာန၊ အစိုးရအဖွဲ့အစည်းများအားလုံး ပူးပေါင်းလုပ်ဆောင်ရန် လိုအပ်ပါသည်။

၄၄။ ဤဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ မူဝါဒကို အကောင်အထည်ဖော်ဆောင်ရွက်ရန်အတွက် (၂၀၂၃ မှ ၂၀၂၈) အထိ ၅ နှစ် လျာထားသတ်မှတ်ပါသည်။ ခေတ်နှင့်အညီ စဉ်ဆက်မပြတ် ပြောင်းလဲတိုးတက်နေသော ဆိုက်ဘာလုံခြုံရေးနည်းပညာများကို လေ့လာ၍ ဤဆိုက်ဘာလုံခြုံရေးဆိုင်ရာမူဝါဒကို ပို့ဆောင်ရေးနှင့် ဆက်သွယ်ရေးဝန်ကြီးဌာနက ဆက်စပ်ဌာနများ၊ ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ ပညာရှင်များနှင့် ပေါင်းစပ်ညှိနှိုင်းပြီး လိုအပ်သလို စဉ်ဆက်မပြတ် ဆက်လက်ပြင်ဆင် မွမ်းမံရေးဆွဲရမည် ဖြစ်သည်။

ပို့ဆောင်ရေးနှင့် ဆက်သွယ်ရေးဝန်ကြီးဌာန
သတင်းအချက်အလက်နည်းပညာနှင့် ဆိုက်ဘာလုံခြုံရေးဦးစီးဌာန
မှ ထုတ်ဝေသည်။
www.motc.gov.mm