မြန်မာ ဆိုက်ဘာဥပဒေနှင့် မူဝါဒမူဘောင်

e-Government, အီလက်ထရောနစ် ကူးသန်းရောင်းဝယ်ရေး (e-Commerce), ဆိုက်ဘာလုံခြုံရေးတို့နှင့် သက်ဆိုင်သော မူဝါဒများ (မူကြမ်း - 25 Jan 2019)

မာတိကာ

e-Government, အီလက်ထရောနစ် ကူးသန်းရောင်းဝယ်ရေး (e-Commerce), ဆိုက်ဘာလုံခြုံရေးတို့နှင့် သက်ဆိုင်သော မြန်မာဆိုက်ဘာဥပဒေနှင့် မူဝါဒများ၏ အနှစ်ချုပ်

စီမံကိန်း မိတ်ဆက်

စီမံကိန်း၏ ရည်ရွယ်ချက်မှာ မြန်မာနိုင်ငံ၏ ICT အခန်းကဏ္ဍ ပြုပြင်ပြောင်းလဲရေး လုပ်ငန်းစဉ်များ၏ မူဝါဒ၊ ဥပဒေနှင့် လုပ်ထုံးလုပ်နည်းဆိုင်ရာ မူဘောင်များ ချမှတ်ဖော်ဆောင်ခြင်း ဖွံ့ဖြိုးတိုးတက်ရေးအတွက် ဖြစ်သည်။ **ဆိုက်ဘာဥပဒေနှင့် မူဝါဒဖွဲ့စည်းပုံ ("ဖွဲ့စည်းပုံ")** များက ပုဂ္ဂလိကနှင့် အစိုးရကပေးသော စနစ်၊ အခြေခံအဆောက်အအုံနှင့် ဝန်ဆောင်မှုများအပေါ် ယုံကြည်မှု တိုးမြင့်လာစေမည်။ အောက်ဖော်ပြပါ ဆိုက်ဘာနှင့် သက်ဆိုင်သော ရည်မှန်းချက်များကို ဦးတည်လုပ်ဆောင်စဉ်-

(က) အီလက်ထရောနစ် ကူးသန်းရောင်းဝယ်ရေးနှင့် ငွေသားသုံးစွဲမှု မရှိသော ဒစ်ဂျစ်တယ် ဂေဟစနစ် တိုးတက်ဖြစ်ထွန်းစေရန်

(ခ) ကိုယ်ရေးကိုယ်တာ အချက်အလက်များအား အလွဲသုံးစားပြုခြင်းကို ကာကွယ်ခြင်းနှင့် နိုင်ငံတကာစံနှုန်းများနှင့် ကိုက်ညီစေခြင်း

(ဂ) အရေးကြီးသည့် နိုင်ငံအဆင့် အခြေခံအဆောက်အအုံများနှင့် ဆက်စပ်သည့် လုပ်ငန်းများကို ဆိုက်ဘာတိုက်ခိုက်မှုများမှ ကာကွယ်ခြင်း

(ဃ) အရေးမကြီးသော အခြေခံအဆောက်အအုံများ အပါအဝင် စနစ်များကို ထိုးဖောက်ဝင်ရောက်သည့် ဆိုက်ဘာရာဇဝတ်မှုများကို တားမြစ်ခြင်းနှင့် ပြစ်ဒဏ်ပေးခြင်း

ဆိုင်ဘာဥပဒေနှင့် မူဝါဒများ၏ ဖွဲ့စည်းပုံ

(၁) ၂၀၁၈ ခုနှစ်၊ ဒီဇင်ဘာလ (၇) ရက်နေ့ နေပြည်တော်တွင် ပြုလုပ်သည့် ကဏ္ဍစုံပါဝင်ပတ်သက်သူများနှင့် ပထမဆုံး ဆွေးနွေးညှိနှိုင်းပွဲ (stakeholder consultation)၊ (၂) ၂၀၁၈ ခုနှစ် ဒီဇင်ဘာ (၄) ရက်နှင့် (၁၂) ရက်ကြား စီမံကိန်း ခရီးစဉ် (၁) အတွင်း သက်ဆိုင်ရာ အမှုဆောင်များ၊ ဝန်ကြီးရုံးများနှင့် တွေ့ဆုံမေးမြန်းခြင်းများ၊ (၃) ဆိုင်ဘာဥပဒေနှင့် မူဝါဒဖွဲ့စည်းပုံများအတွက် တစ်ကမ္ဘာလုံးကျင့်သုံးသော အကောင်းဆုံးနည်းလမ်းများ ညွှန်းကိန်းများနှင့် ယှဉ်လျက် နိုင်ငံတကာ စံနှုန်းသတ်မှတ်ချက် အလေ့အကျင့်များကို လုပ်ဆောင်ရင်း ဆိုင်ဘာဥပဒေနှင့် မူဝါဒ ဖွဲ့စည်းပုံ တိုးတက်ဖြစ်ထွန်းလာပါသည်။

ဤဖွဲ့စည်းပုံတွင် အပိုင်း (၂) ပိုင်း တင်ပြထားသည်။ - **(၁) မြန်မာ ဆိုက်ဘာဥပဒေ နှင့် (၂) e-Government, အီလက်ထရောနစ် ကူးသန်းရောင်းဝယ်ရေး (e-Commerce), ဆိုက်ဘာလုံခြုံရေးတို့နှင့် သက်ဆိုင်သော မူဝါဒများ** ဤစာရွက်စာတမ်းသည် စီမံကိန်း၏ ဆိုက်ဘာမူဝါဒ အဓိက အမျိုးအစား (၃) ခု၊ ၎င်းနှင့် ဆက်စပ်သည့် အကြောင်းရပ် (၁၅) ခုတို့ ဖြင့် ဖွဲ့စည်းထားသည်[1]-

1. e-Government - မြန်မာ ဆိုက်ဘာဥပဒေသည် ရှိရင်းစွဲ e-Government ဦးစီးကော်မတီ၊ e-Government အကောင်အထည်ဖော် လုပ်ဆောင်ရေးအဖွဲ့၊ E-ID (အီလက်ထရောနစ် ကိုယ်ပိုင်အမှတ်အသား) လုပ်ဆောင်ရေးကော်မတီတို့၏ အခန်းကဏ္ဍနှင့် လုပ်ဆောင်ချက်များ အပါအဝင်၊ အပိုင်း (၃) ရှိ e-Government တရားဝင်ဖြစ်ပေါ်ရန် ရည်ရွယ်သည်။ အဆိုပြုထားသည့် **နိုင်ငံအဆင့် ICT မဟာဗျူဟာ စီမံချက်**သည် "မြန်မာ e-Government မဟာ စီမံကိန်း (Master Plan) ၂၀၁၆-၂၀၂၀"[2] ၏ လုပ်ငန်းများကို ရှိရင်းစွဲ e-Government ဦးစီးကော်မတီ၏ လမ်းညွှန်ချက်အတိုင်း ဖြည့်စွက်လုပ်ဆောင်ရန် ပေါ်ပေါက်လာခြင်းဖြစ်သည်။ အမျိုးသားအဆင့် ICT မဟာဗျူဟာ စီမံချက်သည် e-Government အောက်မှ A1 အီလက်ထရောနစ် သတင်းအချက်အလက်များနှင့် အွန်လိုင်း ဝန်ဆောင်မှုများ၊ A2 စံနှုန်းများ သတ်မှတ်ခြင်း၊ A4 လူ့စွမ်းအားအရင်းအမြစ် ဖွံ့ဖြိုးတိုးတက်ရေး A5 အစိုးရ၏ ပွင့်လင်းမြင်သာမှုရှိသော အချက်အလက်များ (Open Government Data) နှင့် Open Source ဆော့ဖ်ဝဲရ်များ၊ A6 ဥဏာပစ္စည်း အခွင့်အရေးများ အပါအဝင် အဓိက အရေးကိစ္စများကို ဦးတည် လုပ်ဆောင်မည်။ အခြားသော မဟာဗျူဟာများထဲတွင် နိုင်ငံအဆင့် ICT မဟာဗျူဟာ စီမံချက်သည် သီးခြား မူဝါဒ စာရွက်စာတမ်းများအဖြစ် စဉ်းစားရမည့် မူဝါဒခွဲ (၃) ခုပါဝင်သည် : **အစိုးရ Cloud First မူဝါဒ၊ အချက်အလက် အမျိုးအစားခွဲခြားခြင်း မူဘောင်များနှင့် အစိုးရ၏ ပွင့်လင်းမြင်သာရှိသော အချက်အလက်များဆိုင်ရာ မူဝါဒ** တို့ဖြစ်သည်။

[1] ဤစီမံကိန်းတွင် သတ်မှတ်ထားသည့် ဆိုက်ဘာဥပဒေနှင့် မူဝါဒဖွဲ့စည်းပုံ ကိစ္စရပ်များ : (က) e-Government: A1 အီလက်ထရောနစ် သတင်းအချက်အလက်များနှင့် အွန်လိုင်း ဝန်ဆောင်မှုများ၊ A2 စံနှုန်းများ သတ်မှတ်ခြင်း၊ A3 သတင်းအချက်အလက် အခြေခံအဆောက်အအုံ တည်ဆောက်ခြင်း၊ A4 လူ့စွမ်းအားအရင်းအမြစ် ဖွံ့ဖြိုးတိုးတက်ရေး A5 အစိုးရ၏ ပွင့်လင်းမြင်သာမှုရှိသော အချက်အလက်များ (Open Government Data) နှင့် Open Source ဆော့ဖ်ဝဲလ်များ၊ A6 အသိဉာဏ်ဆိုင်ရာပစ္စည်း အခွင့်အရေးများ ; (ခ) အီလက်ထရောနစ် ကူးသန်းရောင်းဝယ်ရေး : B1 အီလက်ထရောနစ် နည်းအားဖြင့် သတင်းအချက်အလက်များ အခြားနိုင်ငံများသို့ ရောက်ရှိခြင်း၊ B2 အီလက်ထရောနစ်နည်းအားဖြင့် ပြီးစီးအောင် ဆောင်ရွက်နိုင်ခြင်း၊ B3 စာရွက်စာတမ်း အသုံးမပြုသော ကုန်သွယ်ရောင်းဝယ်ရေး ; B4 သွင်းကုန်ခွန်များ၊ B5 အွန်လိုင်း ကုန်သွယ်ရောင်းဝယ်ရေး၊ (ဂ) ဆိုက်ဘာလုံခြုံရေး : C1 ကိုယ်ရေးကိုယ်တာနှင့် အချက်အလက်များကို ကာကွယ်ခြင်း၊ C2 ဆိုက်ဘာနှောင့်ယှက်မှုနှင့် ဆိုင်ဘာရာဇဝတ်မှုများအား ဖော်ထုတ်ခြင်း၊ C3 အီလက်ထရောနစ် သက်သေအထောက်အထား၊ C4 အီလက်ထရောနစ် အမှတ်အသား/ လက်မှတ်။

[2] https://www.motc.gov.mm/sites/default/files/Myanmar%20e-Governance%20Master%20Plan%20%282016-2020%29%20English%20Version%28Draft%29.pdf

e-government အောက်ရှိ အဓိက အရေးကိစ္စများထဲမှ တစ်ခုကို လတ်တလော **ပြန်လည်စိစစ်သုံးသပ်ခြင်းနှင့် ဖြည့်စွက်ခြင်း** ပြုလုပ်နေသည့် ဥပဒေမှာ (A6) ဥဏှာပစ္စည်း အခွင့်အရေးများ ဖြစ်သည်။ ၂၀၁၈ ခုနှစ် ဖေဖော်ဝါရီလတွင် မြန်မာနိုင်ငံ အထက်လွှတ်တော်က ကုန်စည်အမှတ်အသား ဥပဒေမူကြမ်း၊ စက်မှုလုပ်ငန်းဆိုင်ရာ ပုံစံဒီဇိုင်း ဥပဒေမူကြမ်း၊ မူပိုင်ခွင့်မှတ်ပုံတင်ခြင်း ဥပဒေမူကြမ်းနှင့် မူပိုင်ခွင့် ဥပဒေမူကြမ်းတို့ကို လက်ခံခဲ့သည်။ အောက်လွှတ်တော်သို့ ချပေးခဲ့သည့် မူပိုင်ခွင့် ဥပဒေမူကြမ်းသည် ပြင်ဆင်ချက်များ အဆိုပြုထားပြီး၊ ၂၀၁၈ ခုနှစ် စက်တင်ဘာလတွင် အထက်လွှတ်တော်သို့ ပြန်လည် ရောက်ရှိလာသည်။ မကြာသေးမီက လုပ်ဆောင်ချက်များနှင့် ပဋိပက္ခဖြစ်နိုင်သည့်၊ ဆင်တူဖြစ်နိုင်သည့် ဥပဒေပြုခြင်းများ ထပ်မံလုပ်ဆောင်မည့်အစား၊ ဖြည့်စွက်ပြင်ဆင်သည့် လုပ်ဆောင်ချက်များ ဆက်လက်လုပ်ဆောင်နေပါသည်။ အရှိန်မြှင့်လုပ်ဆောင်နိုင်ခြင်း မရှိလျှင် ဤလုပ်ငန်းစဉ်များကို စီမံချက်အတိုင်း ဆက်လက်လုပ်ဆောင်ရန် အကြံပြုအပ်ပါသည်။

အခြားသော အဓိကကိစ္စရပ်တစ်ခုမှာ ပို့ဆောင်ရေးနှင့် ဆက်သွယ်ရေး ဝန်ကြီးဌာန၊ ဆက်သွယ်ရေးညွှန်ကြားမှု ဦးစီးဌာန (PTD) အောက်ရှိ အခြေခံ ဆက်သွယ်ရေးလိုအပ်ချက် ဖြည့်ဆည်းခြင်းဆိုင်ရာ ရန်ပုံငွေ (Universal Service Fund, USF)[3] ဖြင့် လက်ရှိ စဉ်းစားသုံးသပ်နေဆဲဖြစ်သည့် (A3) သတင်းအချက်အလက် အခြေခံအဆောက်အအုံ တည်ဆောက်ခြင်း ဖြစ်သည်။ ၂၀၁၈ ခုနှစ် ဒီဇင်ဘာလတွင် အခြေခံ ဆက်သွယ်ရေးလိုအပ်ချက် ဖြည့်ဆည်းခြင်းဆိုင်ရာ ရန်ပုံငွေ (Universal Service Fund, USF) စီမံခန့်ခွဲရေး ဘုတ်အဖွဲ့သို့ အဆိုပြုချက် တင်သွင်းထားပြီး၊ အစိုးရအဖွဲ့ အတည်ပြုချက်ကို စောင့်ဆိုင်းလျက်ရှိသည်။ (၎င်းကို ပရင့်ထုတ်ချိန်ထိ အတည်မပြုရသေးပါ။) အခြေခံ ဆက်သွယ်ရေးလိုအပ်ချက် ဖြည့်ဆည်းခြင်းဆိုင်ရာ ရန်ပုံငွေ (Universal Service Fund, USF) ဖြင့် မူဝါဒသစ်များ ဖော်ဆောင်ခြင်းအစား မြန်မာနိုင်ငံ နေရာအနှံ့သို့ ဆက်သွယ်ရေးနှင့် အင်တာနက် ချိတ်ဆက်ခြင်းများ ရရှိအောင် လုပ်ဆောင်ပေးခဲ့သည်။ ဆက်သွယ်ရေးညွှန်ကြားမှု ဦးစီးဌာန (PTD) အနေဖြင့် အခြေခံ ဆက်သွယ်ရေးလိုအပ်ချက် ဖြည့်ဆည်းခြင်းဆိုင်ရာ ရန်ပုံငွေ (Universal Service

[3] https://www.motc.gov.mm/sites/default/files/Universal%20Service%20Strategy%20%28Draft%29_0.pdf

Fund, USF) ကို အသုံးပြုပြီး မြန်မာနိုင်ငံ သတင်းအချက်အလက် အခြေခံအဆောက်အအုံ တည်ဆောက်ခြင်းလုပ်ငန်းကို ဆက်လက် အရှိန်မြှင့်လုပ်ဆောင်ရန် အကြံပြုအပ်ပါသည်။

သတင်းအချက်အလက် အခြေခံအဆောက်အအုံ တည်ဆောက်ခြင်းလုပ်ငန်းတွင် ပါဝင်နေသည့် အခြား ကိစ္စရပ်များမှာ ပြဋ္ဌာန်းမှု မရှိသေးသည့် ဆက်သွယ်ရေး မဟာစီမံကိန်း (Masterplan) ၂၀၁၅[4] တွင် ထည့်သွင်းဖော်ပြခဲ့ပြီး ဖြစ်သည်။ မူပွားများ ပြန်လည်ရေးသားနေမည့်အစား၊ တကမ္ဘာလုံး ကျင့်သုံးသည့် အကောင်းဆုံးနည်းလမ်းများ (global best practices) နှင့်အညီ ဆက်သွယ်ရေးညွှန်ကြားမှု ဦးစီးဌာန (PTD) ကို လွတ်လပ်သည့် ဆက်သွယ်ရေး ကြီးကြပ်အဖွဲ့အစည်းတစ်ရပ်အဖြစ် ထူထောင်ရန် အဆိုပြုချက်ပါဝင်သော ရေရှည်စီမံချက် (Masterplan) ကို စတင်ပြဋ္ဌာန်းရန် အကြံပြုပါသည်။

2. အီလက်ထရောနစ် ကူးသန်းရောင်းဝယ်ရေး (e-Commerce) - မြန်မာ ဆိုင်ဘာဥပဒေသည် နိုင်ငံတကာ စံနှုန်းများကို ထည့်သွင်းရန်၊ လိုက်နာရန်နှင့်အီလက်ထရောနစ် ကူးသန်းရောင်းဝယ်ရေးအတွက်နှင့် အီလက်ထရောနစ် အမှတ်အသား (Electronic Signatures) အတွက် အမေရိကန်ပြည်ထောင်စု ကော်မရှင် နိုင်ငံတကာ ကုန်သွယ်ရေးဥပဒေကို စံနမူနာယူသည့် ဥပဒေ (UNCITRAL Model Law) တို့နှင့် လိုက်လျောညီထွေဖြစ်ရန် ရှိပြီးသား ဥပဒေများဖြစ်သည့် အီလက်ထရောနစ် လုပ်ငန်းများ ဥပဒေ၊ သက်သေခံ အက်ဥပဒေ ကို ပြင်ဆင်ဖြည့်စွက်ရန် အဆိုပြုချက်နှင့် ကိုးကားချက်များ အပါအဝင် အပိုင်း (၄) အောက်ရှိ အီလက်ထရောနစ် ကူးသန်းရောင်းဝယ်ရေး (e-Commerce) ကို တရားဝင်ဖြစ်ရန် ရည်ရွယ်သည်။ ထို့ပြင် မြန်မာနိုင်ငံ၌ အီလက်ထရောနစ် ကူးသန်းရောင်းဝယ်ရေး (e-Commerce) တိုးတက်ဖြစ်ထွန်းလာခြင်းတွင် သီးခြား ကိစ္စရပ်များပါဝင်သည်။ အီလက်ထရောနစ် ကူးသန်းရောင်းဝယ်ရေး (e-Commerce) အတွက် (B1) အီလက်ထရောနည်းအားဖြင့် သတင်းအချက်အလက်များ အခြားနိုင်ငံများသို့ ရောက်ရှိခြင်း၊ (B2) အီလက်ထရောနစ်နည်းအားဖြင့် ပြီးစီးအောင် ဆောင်ရွက်နိုင်ခြင်း၊ (B3) စာရွက်စာတမ်း အသုံးမပြုသော ကုန်သွယ်ရောင်းဝယ်ရေး၊ (B4) သွင်းကုန်ခွန်များ၊ (B5) အွန်လိုင်း

[4] http://www.mcit.gov.mm/content/draft-telecommunications-masterplan.html

ကုန်သွယ်ရောင်းဝယ်ရေးနှင့် (ဆိုက်ဘာလုံခြုံရေးခေါင်းစဉ်အောက်မှ မူလ စာရင်းထဲတွင် ပါဝင်သော ကိစ္စရပ်များ) အပါအဝင် အဓိက ကိစ္စရပ်များကို ဦးတည်လုပ်ဆောင်ရန် အီလက်ထရောနစ် ကူးသန်းရောင်းဝယ်ရေး (e-Commerce) ဦးစီးကော်မတီကို တည်ထောင်ဖွဲ့စည်းရန် အကြံပြုပါသည်။ ; (C3) အီလက်ထရောနစ် သက်သေအထောက်အထားနှင့် (C4) အီလက်ထရောနစ် အမှတ်အသား/ လက်မှတ်

3. ဆိုင်ဘာလုံခြုံရေး - မြန်မာ ဆိုင်ဘာဥပဒေသည် အရေးကြီးသော သတင်းအချက်အလက် အခြေခံအဆောက်အအုံကို ကာကွယ်ခြင်းအတွက် လုပ်ထုံးလုပ်နည်းများအပါအဝင် ဆိုက်ဘာလုံခြုံရေးအတွက် နိုင်ငံအဆင့် မဟာဗျူဟာကို အဆိုပြုထားပြီး၊ အပိုင်း (၅) ရှိ ဆိုက်ဘာလုံခြုံရေးကို ဦးတည်လုပ်ဆောင်ရန် ဖြစ်သည်။ ထို့ပြင် မြန်မာ ဆိုက်ဘာဥပဒေသည် ကိစ္စရပ် (C1) ကိုယ်ရေးကိုယ်တာနှင့် အချက်အလက်များ ကာကွယ်ခြင်းကို ဦးတည်လုပ်ဆောင်ရင်း၊ အပိုင်း (၆) ရှိ ကိုယ်ရေးကိုယ်တာ အချက်အလက်များ ကာကွယ်ရေး ကော်မရှင်ကို တည်ထောင်ရန် ရည်ရွယ်သည်။ မြန်မာ ဆိုင်ဘာဥပဒေသည် ကိစ္စရပ် (C2) ဆိုက်ဘာနှောင့်ယှက်မှုနှင့် ဆိုင်ဘာရာဇဝတ်မှုများအား ဖော်ထုတ်ခြင်းကို ဦးတည်လုပ်ဆောင်ရင်း၊ အပိုင်း (၇) ရှိ ကွန်ပြူတာ အလွဲသုံးစားလုပ်ခြင်းနှင့် ဆိုက်ဘာရာဇဝတ်မှုများအတွက် ဥပဒေပြုရေး အခြေခံကို ရရှိစေသည်။ ဆိုင်ဘာရာဇဝတ်မှုရေးရာ ဆောင်ရွက်ဖြေရှင်းရေး အဖွဲ့ကိုလည်း အဆိုပြုပြီးဖြစ်သည်။

နောက်ထပ် ခြေလှမ်းများ

၂၀၁၉ ခုနှစ် ဖေဖော်ဝါရီလ (၁၈) ရက်တွင် စီစဉ်ထားသည့် စီမံကိန်းခရီးစဉ် (၂) အတွင်း ပါဝင်ပတ်သက်သူများ၊ လူထုနှင့် နောက်ထပ် ဆွေးနွေးညှိနှိုင်းပွဲ (stakeholder and public consultation) တွင် မြန်မာ ဆိုက်ဘာဥပဒေနှင့် မူဝါဒဖွဲ့စည်းပုံများ၏ နှစ်ပိုင်းလုံး - (၁) မြန်မာ ဆိုက်ဘာဥပဒေနှင့် (၂) e-Government, အီလက်ထရောနစ် ကူးသန်းရောင်းဝယ်ရေး (e-Commerce) နှင့် ဆိုက်ဘာလုံခြုံရေးကို ဖြန့်ချိသွားမည်။ ကဏ္ဍစုံမှပါဝင်ပတ်သက်သူ (stakeholder) များနှင့် ဆွေးနွေးညှိနှိုင်းခြင်း နှစ်မျိုး ရှိပါသည်။

- ၂၀၁၉ ခုနှစ် ဖေဖော်ဝါရီလ (၁၉) ရက်၊ အင်္ဂါနေ့၊ နေပြည်တော်တွင် ကျင်းပမည့် အစိုးရနှင့် ဝန်ကြီးဌာနများရှိ ကဏ္ဍစုံမှပါဝင်ပတ်သက်သူများ (stakeholder) များ အဓိကအားဖြင့်

တက်ရောက်မည့် ကဏ္ဍစုံပါဝင်ပတ်သက်သူများနှင့် ဆွေးနွေးညှိနှိုင်းပွဲ (Stakeholder Consultation)၊

- ၂၀၁၉ ခုနှစ် ဖေဖော်ဝါရီလ (၂၁) ရက်၊ ရန်ကုန်မြို့တွင် ကျင်းပမည့် ပုဂ္ဂလိကနှင့် အစိုးရမဟုတ်သော ကဏ္ဍများမှ ပါဝင်ပတ်သက်သူများ အဓိကအားဖြင့် တက်ရောက်မည့် လူထု ဆွေးနွေးညှိနှိုင်းပွဲ (Public Consultation)။

မြန်မာ ဆိုက်ဘာဥပဒေ (မူကြမ်း)

သီးခြား စာရွက်ကို ကြည့်ပါ။

အပိုင်း (၁) : e-Government နှင့် သက်ဆိုင်သော မူဝါဒများ : နိုင်ငံအဆင့် ICT မဟာဗျူဟာ စီမံချက်

မိတ်ဆက် :

အမြော်အမြင်ရှိသော မြန်မာ့ခေါင်းဆောင်များသည် အလွန်အရေးပါသော စီးပွားရေးစနစ် ဆန်းသစ်ပြောင်းလဲခြင်းအတွက် အဆင့်မြင့် ICT ကဏ္ဍမှာ အလွန်အရေးပါကြောင်း သိရှိနားလည်ကြပြီး ဖြစ်ပါသည်။ မြန်မာနိုင်ငံတွင် ကဏ္ဍအသီးသီး၌ ရေရှည်တည်တံ့ခိုင်မြဲသော စီးပွားရေး ဖွံ့ဖြိုးတိုးတက်မှု ဖြစ်လာစေရန် ICT က ပံ့ပိုးလုပ်ဆောင်ပေးပါလိမ့်မည်။

နိုင်ငံအဆင့် ICT မဟာဗျူဟာ စီမံချက်ကို လွန်ခဲ့သော နှစ်များကတည်းက မြန်မာနိုင်ငံတွင် လုပ်ဆောင်လျက်ရှိပါသည်။ လူထုကို အထောက်အပံ့နှင့် လုပ်ပိုင်ခွင့်ပေးသည့် အားအင်ပြည့်ဝသော ICT အခန်းကဏ္ဍကို အရှိန်အဟုန်မြှင့်တင် ကြိုးပမ်းဖော်ဆောင်ရာတွင် အစိုးရ၏ ထက်သန်မြဲပန့်မှုရှိရန် ထပ်မံ အတည်ပြုပြောကြားပါသည်။ ဤ ICT စီမံချက်တွင် အကျဉ်းဖော်ပြထားသည့် များစွာသော အစီအစဉ်နှင့် မူဝါဒများမှာ မြန်မာနိုင်ငံ၏ အနာဂတ် ဖွံ့ဖြိုးတိုးတက်မှုအတွက် အဓိကအချက်များ ဖြစ်သည်။ ၎င်းက အဆင့်မြင့် ICT အခြေခံ အဆောက်အအုံများမှတဆင့် ချိတ်ဆက်မှု (connectivity) ကို တိုးတက်စေလိမ့်မည်။

ICT မှတဆင့် အစိုးရ၏ ဝန်ဆောင်မှုများပေးခြင်းသည် မြန်မာနိုင်ငံ တိုးတက်မှုအတွက် အဓိကအချက်ဖြစ်ပါသည်။ ဤစီမံချက်က ပုဂ္ဂလိက ကဏ္ဍ၏ ICT အရည်အသွေးများနှင့် ပြည်သူ့ဝန်ဆောင်မှုလုပ်ငန်းများ တိုးတက်စေရန် ဆန်းသစ်သော application များနှင့် programme များ အသုံးပြုခြင်းကို အသေအချာ ဖွံ့ဖြိုးတိုးတက်စေနိုင်ပါသည်။ cloud computing ဝန်ဆောင်မှုများ၏ အကျိုးကျေးဇူးများကို သိရှိပြီး မြန်မာ အစိုးရသည် သတင်းအချက်အလက် လုံခြုံရေး စီမံခန့်ခွဲမှုအတွက် အချက်အလက် အမျိုးအစားခွဲခြားခြင်း မူဘောင်များနှင့်တကွ cloud-first မူဝါဒကို ကျင့်သုံးလာလိမ့်မည်။ အချက်အလက်များ ဖလှယ်ဆောင်ရွက်နိုင်စွမ်း (interoperability) နှင့် ပွင့်လင်းမြင်သာမှုရှိခြင်း (openness) ကို တိုးမြင့်စေရန် ကြိုးပမ်းအားထုတ်သည့်အနေဖြင့် အစိုးရသည် ပွင့်လင်းမြင်သာသော အချက်အလက် မူဝါဒ (Open Data policy) ကို စတင်ဆောင်ရွက်နေပါသည်။

ဤကြိုးပမ်းအားထုတ်မှုသည် မြန်မာနိုင်ငံတွင် ဆန်းသစ်ပြောင်းလဲခြင်း၊ ထုတ်လုပ်မှုစွမ်းအား၊ သတင်းအချက်အလက်လုံခြုံရေးနှင့် ဒစ်ဂျစ်တယ် စီးပွားရေး ဖြစ်ထွန်းခြင်းတို့ကို တိုးတက်စေပါလိမ့်မည်။

ရည်မှန်းချက်များ ပြည့်မီရန် ကျယ်ပြန့်၍ မဟာဗျူဟာကျသော မူဘောင်များ ချမှတ်ပြီးဖြစ်သည်။ ၎င်းကို ရေရှည်တည်တံ့ခိုင်မြဲသော ဒစ်ဂျစ်တယ် အနာဂတ်ကို ဖော်ဆောင်ရန် လိုအပ်သည့် အရေးကြီး အစိတ်အပိုင်းများဖြစ်သည့် မဟာဗျူဟာကျသော လုပ်ဆောင်ချက် (၅) ခုဖြင့် ဖွဲ့စည်းထားသည်။ အစိုးရ၏ ပိုမိုကျယ်ပြန့်သော ရည်မှန်းချက်များနှင့် ကိုက်ညီသည့် ထိုလုပ်ဆောင်ချက် (၅) ခုမှာ မြန်မာနိုင်ငံတွင် အရေးပါသော ဗဟုသုတအခြေပြု စီးပွားရေးကို ဖြစ်ပေါ်စေနိုင်ပါသည်။

၁။ ပြည်သူ့ဝန်ဆောင်မှု တိုးမြှင့်ပေးခြင်း - သတင်းအချက်အလက်နှင့် အွန်လိုင်း ဝန်ဆောင်မှုများ၊ စံသတ်မှတ်ခြင်း

၂။ ချိတ်ဆက်မှု တိုးတက်စေခြင်း - သတင်းအချက်အလက် အခြေခံ အဆောက်အအုံ

၃။ အရည်အသွေး တိုးတက်စေခြင်း - ICT လူသားအရင်းအနှီးနှင့် ဉာဏ်ပစ္စည်း အခွင့်အရေးများ

၄။ အစိုးရအဆင့် ICT ကို အဆင့်မြှင့်ခြင်း - Cloud First မူဝါဒ၊ အချက်အလက် အမျိုးအစားခွဲခြားဖြင်း မူဘောင်များ

၅။ ပွင့်လင်းမှုကို အားပေးမြှင့်တင်ခြင်း - ပွင့်လင်းသော အချက်အလက်များဆိုင်ရာ မူဝါဒ

အောက်ပါ အခန်းသည် ပို၍ အသေးစိတ်ကျသော၊ ကနဦးလုပ်ဆောင်ချက်များနှင့် မူဝါဒများကို အဓိကထားသော မဟာဗျူဟာကျသော လုပ်ဆောင်ညှိနှိုင်းချက်များ ပေါင်းစပ်ထားသည့် ICT မဟာဗျူဟာ စီမံချက် အကျဉ်းချုပ် ဖြစ်သည်။

၁။ ပြည်သူ့ ဝန်ဆောင်မှုများ တိုးမြှင့်ပေးခြင်း (A1, A2)

သတင်းအချက်အလက်နှင့် အွန်လိုင်း ဝန်ဆောင်မှုများ (A1)

1. အစိုးရဌာနဆိုင်ရာများမှ နိုင်ငံသားများအတွက် သတင်းအချက်အလက်နှင့် ဝန်ဆောင်မှုများ အွန်လိုင်းမှ ပေးခြင်းသည် e-Government ၏ အဓိက အချက်ဖြစ်သည်။ နောက်ထပ် ဖွံ့ဖြိုးတိုးတက်မှုများ ဖြစ်ပေါ်လာလျက်၊ အွန်လိုင်းတွင် လုပ်ဆောင်နိုင်သည့်

သတင်းအချက်အလက်နှင့် အရောင်းအဝယ်လုပ်ငန်း ဝန်ဆောင်မှုများ အရေအတွက် တိုးတက်လာသည်။

2. e-Government ဦးစီးကော်မတီသည် "လူထုဝန်ဆောင်မှုလုပ်ငန်းများတွင် နည်းပညာ၊ အွန်လိုင်း ဝန်ဆောင်မှုများနှင့် အီလက်ထရောနစ် သတင်းအချက်အလက်များကို အသုံးပြုခြင်းအားဖြင့် ထုတ်လုပ်မှု၊ အကျိုးဖြစ်ထွန်းခြင်းနှင့် ထိရောက်မှုရှိခြင်းတို့ တိုးတက်စေရေးအတွက် အားပေးရန်" တာဝန်ရှိသည်။ (မြန်မာ ဆိုက်ဘာဥပဒေကို ကြည့်ပါ။)
3. ပိုမို အကျိုးရှိစေရန်၊ ရောင်းဝယ်ခြင်းနှင့် သတင်းအချက်အလက် ဝန်ဆောင်မှုအသစ်များ ပေးရန်၊ အစိုးရဌာနများနှင့် ဝန်ကြီးဌာနများကြားတွင် ညှိနှိုင်းဆောင်ရွက်ခြင်းများ တိုးတက်စေရန်နှင့် ထိုဝန်ဆောင်မှုများအပေါ် နားလည်သဘောပေါက်ခြင်း မြင့်မားလာစေရန် ပြောင်းလဲဆန်းသစ်သော ICT application များကို အသုံးပြုခြင်းအတွက် e-Government ဦးစီးကော်မတီက အစိုးရကို လမ်းညွှန်မှု ပေးလိမ့်မည်။
4. e-Government ဦးစီးကော်မတီသည် မြန်မာနိုင်ငံဆိုင်ရာ ပေါ်တယ်လ် (Myanmar National Portal) နှင့် အခြား အွန်လိုင်း အရင်းအမြစ်များ[5] (တကမ္ဘာလုံးဆိုင်ရာ ညွှန်းကိန်းများနှင့်ယှဉ်၍ စံနှုန်းများ လေ့လာခြင်း (Benchmark Study Against Global Indexes) တွင် ဖော်ပြထားသည်) တွင် အရင်းအမြစ်ရရှိနိုင်မှုများ တိုးပွားလာစေရန်နှင့် အစိုးရချိတ်ဆက်မှုနှင့် ပွင့်လင်းမြင်သာမှု တိုးမြင့်လာစေရန် ဆက်လက် လုပ်ဆောင်လိမ့်မည်။

စံနှုန်းသတ်မှတ်ခြင်း (A2)

1. စံနှုန်းများ ချမှတ်ခြင်းသည် ထိရောက်သော အစိုးရ လုပ်ငန်းလည်ပတ်မှုနှင့် ဝန်ဆောင်မှုများအတွက် အခြေခံအုတ်မြစ်ဖြစ်သည်။ မြန်မာနိုင်ငံတွင် e-Government စတင်မှုအတွက် ဌာနဆိုင်ရာ အမျိုးမျိုးက မိတ်ဆက်ရာတွင် အစိုးရနှင့် အသုံးပြုသူများကြားတွင် တည်ငြိမ်သော၊ လုံခြုံချောမွေ့သော သတင်းအချက်အလက် ဖလှယ်မှုများ ဖြစ်စေရန် စံနှုန်းများက ထောက်ကူပါလိမ့်မည်။
2. ဤကိစ္စနှင့် စပ်လျဉ်း၍ ကနဦးလုပ်ဆောင်ချက် (၃) ခု လုပ်ဆောင်လိမ့်မည်။

[5] မြန်မာနိုင်ငံ ဥပဒေဆိုင်ရာ သတင်းအချက်အလက်စနစ်၊ မြန်မာနိုင်ငံအဆင့် ကုန်သွယ်ရောင်းဝယ်ရေး ပေါ်တယ်၊ မြန်မာ စက်မှုလုပ်ငန်း ပေါ်တယ်၊ အစိုးရ အေဂျင်စီများနှင့် ဝဘ်ဆိုဒ်များ။

a. ဆိုက်ဘာလုံခြုံရေး စံနှုန်းများအတွက် လမ်းညွှန်ချက်များ တိုးတက်ဖွံ့ဖြိုးရေးနှင့် ထုတ်ဝေဖြန့်ချီရေးအတွက် မြန်မာ ဆိုက်ဘာဥပဒေမှ ကော်မတီသို့ အပ်နှင်းထားသော အခွင့်အာဏာအရ E-Government ဦးစီးကောက်မတီ၏ အားထုတ်မှုများနှင့် ကိုက်ညီသည့် တရားဝင် စံနှုန်းသတ်မှတ်ခြင်း အဖွဲ့ တည်ထောင်ခြင်း။ [Chapter (III) Section C/12/a] ဤအဖွဲ့သည် နိုင်ငံအတွင်း စံနှုန်းများ ဖွံ့ဖြိုးတိုးတက်ရေးကို တည်ထောင်၊ စောင့်ကြည့်၊ ညှိနှိုင်းဆောင်ရွက်ပြီး၊ နိုင်ငံတကာ စံနှုန်းချမှတ်ရေးအဖွဲ့များနှင့် အတူပါဝင်ဆောင်ရွက်လိမ့်မည်။
b. အစိုးရဌာနဆိုင်ရာများနှင့် CIIs အတွင်း နိုင်ငံတကာ အသိအမှတ်ပြု စံနှုန်းများ အကောင်အထည်ဖော် ဆောင်ရွက်ခြင်း။[6]
c. ဆိုင်ဘာလုံခြုံရေးစံနှုန်းများ အတွက် "Baseline Plus" ဖြင့် ချဉ်းကပ်ခြင်းကို အစပြုခြင်း။ (အခန်း (၆) Baseline အသိအမှတ်ပြုလက်မှတ်များ၊ ကနဦး စံနှုန်းများနှင့် ကျင့်ဝတ်များ၊ မြန်မာ Cloud First မူဝါဒတွင် ကြည့်ပါ။)

၂။ ချိတ်ဆက်မှု တိုးတက်စေခြင်း (A3)

သတင်းအချက်အလက် အခြေခံအဆောက်အအုံ (A3)

1. မြန်မာအစိုးရသည် အဆင့်မြင့် လုံခြုံစိတ်ချရသော အခြေခံအဆောက်အအုံကို အသုံးပြုရန် ရည်ရွယ်သည်။ လွန်ခဲ့သော နှစ်အနည်းငယ်အတွင်း တိုးတက်နေသော တည်ဆောက်မှုသည် မြန်နှုန်းမြင့်၍ စွမ်းဆောင်ရည် မြင့်မားသော လုံခြုံ စိတ်ချရသည့် အခြေခံအဆောက်အအုံကို ချိတ်ဆက် ရယူသုံးစွဲနိုင်စေမည်။
2. ၎င်းမှာ ပို့ဆောင်ရေးနှင့် ဆက်သွယ်ရေး ဝန်ကြီးဌာန၊ ဆက်သွယ်ရေးညွှန်ကြားမှု ဦးစီးဌာန (PTD) ဇ အောက်ရှိ အခြေခံ ဆက်သွယ်ရေးလိုအပ်ချက် ဖြည့်ဆည်းခြင်းဆိုင်ရာ ရန်ပုံငွေ (Universal Service

[6] ထို စံနှုန်းများတွင် : International Organisation for Standardisation (ISO) (နိုင်ငံတကာ စံနှုန်းသတ်မှတ်ခြင်း အဖွဲ့အစည်း), International Telecommunication Union (ITU) (နိုင်ငံတကာ ဆက်သွယ်ရေး သမဂ္ဂ), Internet Engineering Task Force (IETF) (အင်တာနက် အင်ဂျင်နီယာနှင့်ဆိုင်သော လုပ်ဆောင်ချက်များ အင်အားစု), Institute of Electrical and Electronics Engineers (IEEE) (အီလက်ထရစ်ကယ်နှင့် အီလက်ထရောနစ် အင်ဂျင်နီယာများ အင်စတီကျု) , Alliance for Telecommunications Industry Standards (ATIS) (ဆက်သွယ်ရေးလုပ်ငန်း စံနှုန်းများ အဖွဲ့အစည်း) , Organisations for the Advancement of Structured Information Standards (OASIS) (ဖွဲ့စည်းပုံစနစ်ကျသော သတင်းအချက်အလက် စံနှုန်းများ အဆင့်မြင့်မားရေး အဖွဲ့အစည်း) , 3rd Generation Partnership Project (3GPP) (တတိယမျိုးဆက် မိတ်ဖက်စီမံကိန်း) , Interactive Advertising Bureau (IAB) (အပြန်အလှန် သက်ရောက်မှုရှိသော ကြော်ငြာဗျူရို), Internet Society (ISOC) (အင်တာနက် လူ့အဖွဲ့အစည်း), Industry Specification Groups (ISG) (စက်မှုလုပ်ငန်းဆိုင်ရာ သတ်မှတ်ချက်အဖွဲ့), Indian Standards Institute (ISI) (အိန္ဒိယ စံနှုန်း အင်စတီကျု), European Telecommunications Standards Institute (ETSI) (ဥရောပ ဆက်သွယ်ရေးစံနှုန်း အင်စတီကျု), Information Security Forum (ISF) (သတင်းအချက်အလက် လုံခြုံရေး ဆွေးနွေးပွဲ), Request for Comments (RFC) (မှတ်ချက်များ တောင်းခံခြင်း), International Standards for Auditing (ISA) (စာရင်းစစ်ခြင်းအတွက် နိုင်ငံတကာ စံနှုန်းများ), International Electrotechnical Commission (IEC), North American Electric Reliability Corporation (NERC) (နိုင်ငံတကာ အီလက်ထရိုနည်းပညာ ကော်မရှင်), National Institute of Standards and Technology (NIST) (စံနှုန်းများနှင့် နည်းပညာ အမျိုးသားအင်စတီကျု), Federal Information Processing Standard (FIPS) (ဖက်ဒရယ် သတင်းအချက်အလက် ဆောင်ရွက်ခြင်း စံနှုန်း), and Payment Card Industry Data Security Standard (PCI DSS) (ငွေချေကဒ်လုပ်ငန်း အချက်အလက် လုံခြုံရေး စံနှုန်း) တို့ ပါဝင်သည်။

Fund, USF)[7] ဖြင့် လက်ရှိတွင် တိုးတက်လျက်ရှိသည်။ ၂၀၁၈ ခုနှစ် ဒီဇင်ဘာလတွင် အခြေခံဆက်သွယ်ရေးလိုအပ်ချက် ဖြည့်ဆည်းခြင်းဆိုင်ရာ ရန်ပုံငွေ (Universal Service Fund, USF) စီမံခန့်ခွဲရေး ဘုတ်အဖွဲ့သို့ အဆိုပြုချက် တင်သွင်းထားပြီး၊ အစိုးရအဖွဲ့ အတည်ပြုချက်ကို စောင့်ဆိုင်းလျက်ရှိသည်။ (၎င်းကို ပရင့်ထုတ်ချိန်ထိ အတည်မပြုရသေးပါ။) USF ဖြင့် မြန်မာနိုင်ငံ နေရာအနှံ့သို့ ဆက်သွယ်ရေးနှင့် အင်တာနက် ချိတ်ဆက်ခြင်းများ ရရှိအောင် လုပ်ဆောင်ပေးခဲ့သည်။ ဆက်သွယ်ရေးညွှန်ကြားမှု ဦးစီးဌာန (PTD) အနေဖြင့် USF ကို အသုံးပြုပြီး မြန်မာနိုင်ငံ သတင်းအချက်အလက် အခြေခံအဆောက်အအုံ တည်ဆောက်ခြင်းလုပ်ငန်းကို ဆက်လက် အရှိန်မြှင့်လုပ်ဆောင်သင့်ပါသည်။

3. ဆက်သွယ်ရေး မဟာစီမံကိန်း ၂၀၁၅ (Telecommunications Masterplan 2015) တွင် သတင်းအချက်အလက် အခြေခံအဆောက်အအုံတွင် ပါဝင်သော အခြားကိစ္စရပ်များလည်း ပါဝင်သည်။ တရားဝင် ပြဌာန်းပြီးသည့်နောက်တွင် ၎င်းကို အပြည့်အဝ အကောင်အထည်ဖော် ဆောင်ရွက်သင့်ပါသည်။ ထို့နောက် PTD ကို တကယ္ဗာလုံးဆိုင်ရာ ကျင့်ဝတ်ကောင်းများနှင့်အညီ လွတ်လပ်သည့် ဆက်သွယ်ရေး ကြီးကြပ်အဖွဲ့အစည်းတစ်ခုအဖြစ် ပြုလုပ်သင့်ပါသည်။

3။ အရည်အသွေး တိုးတက်စေခြင်း (A4, A6)

ICT လူသားအရင်းအနှီး (A4)

1. မြန်မာအစိုးရသည် ဒစ်ဂျစ်တယ် နည်းပညာတတ်မြောက်မှု တိုးတက်မြင့်မားရန်နှင့် ၎င်း၏ အလုပ်သမားအင်အားစုများတွင် လိုအပ်သော ကျွမ်းကျင်မှုများ တိုးတက်ဖွံ့ဖြိုးလာပြီး အသိသညာ အခြေပြု စီးပွားရေးတွင် ပြောင်းလဲ ဆန်းသစ်ခြင်းနှင့် ပါဝင်လုပ်ဆောင်ခြင်းပြုနိုင်ရန် ရည်ရွယ်သည်။ ပညာပေးရေးနှင့် လေ့ကျင့်သင်ကြားရေး အစီအစဉ်များကို အာရုံစိုက်လုပ်ဆောင်ရန် နိုင်ငံအဆင့် ညှိနှိုင်းဆောင်ရွက် အားထုတ်မှုများ ပြုလုပ်ရန် လိုအပ်ပါသည်။
2. အတိအကျဆိုသော် ၎င်း အားထုတ်မှုများတွင် :
    a. အစိုးရ ဝန်ထမ်းများကြားတွင် ICT ကျွမ်းကျင်မှုများ အားကောင်းလာစေရန် ရည်ရွယ်သော လူသားအရင်းအနှီး တိုးတက်ဖွံ့ဖြိုးရေး အစီအစဉ်များ စတင်ခြင်း။

[7] https://www.motc.gov.mm/sites/default/files/Universal%20Service%20Strategy%20%28Draft%29_0.pdf

b. ICT သင်ရိုးညွှန်းတမ်းများ တိုးတက်ဖွံ့ဖြိုးလာစေရန် ပုဂ္ဂလိကနှင့် လူထု ပညာရေး အဖွဲ့အစည်းများကို လမ်းညွှန်ခြင်း။

c. ဝန်ထမ်းများကို အလုပ်လုပ်ရင်း ICT သင်ယူလေ့ကျင့်နိုင်ခွင့်ရစေရန် ကုမ္ပဏီများအား လုပ်ဆောင်စေခြင်း။

d. ICTကို ဆွဲဆောင်မှုရှိသော အလုပ်အကိုင် လမ်းကြောင်းအဖြစ် မြှင့်တင်ပြီး၊ ICT ကဏ္ဍတွင် လူသစ်များ ခန့်ထားရန် အားပေးခြင်းတို့ ပါဝင်သည်။

ဉာဏ်ပစ္စည်း အခွင့်အရေးများ (A6)

1. တိုးတက်စည်ပင်သည့် ဒစ်ဂျစ်တယ် စီးပွားရေး ဖန်တီးနိုင်ခြင်းသည် ကျေနပ်အားရမှုနှင့် တီထွင်ဖန်တီးမှုများကို အကာအကွယ်ပေးသည့် စွန့်ဦးတီထွင်နိုင်သည့် ပတ်ဝန်းကျင်ကို အားပေးမြှင့်တင်ခြင်းပေါ်တွင် တည်မှီပါသည်။ ထို့ကြောင့် ၎င်းသည် ဟန်ချက်ညီသော ဉာဏ်ပစ္စည်း လုပ်ဆောင်မှုစနစ်ကို ဖန်တီးရန်နှင့် တန်ဖိုးဖန်တီးမှု (value-creation) ကို အထောက်အပံ့ပေးရန် ရည်ရွယ်သည်။
2. ဉာဏ်ပစ္စည်း အခွင့်အရေးများသည် လက်ရှိတွင် ဥပဒေဆိုင်ရာ ပြန်လည်သုံးသပ်မှုနှင့် ပြင်ဆင်ဖြည့်စွက်ခြင်းများ ဆက်လက် လုပ်ဆောင်လျက်ရှိသည်။ ၂၀၁၈ ခုနှစ် ဖေဖော်ဝါရီလတွင် မြန်မာနိုင်ငံ အထက်လွှတ်တော်က ကုန်စည်အမှတ်အသား ဥပဒေမူကြမ်း၊ စက်မှုလုပ်ငန်းဆိုင်ရာ ပုံစံဒီဇိုင်း ဥပဒေမူကြမ်း၊ မူပိုင်ခွင့်မှတ်ပုံတင်ခြင်း ဥပဒေမူကြမ်းနှင့် မူပိုင်ခွင့် ဥပဒေမူကြမ်းတို့ကို လက်ခံခဲ့သည်။ အောက်လွှတ်တော်သို့ ချပေးခဲ့သည့် မူပိုင်ခွင့် ဥပဒေမူကြမ်းသည် ပြင်ဆင်ချက်များ အဆိုပြုထားပြီး၊ ၂၀၁၈ ခုနှစ် စက်တင်ဘာလတွင် အထက်လွှတ်တော်သို့ ပြန်လည် ရောက်ရှိလာသည်။ ပြင်ဆင်ဖြည့်စွက်ခြင်း လုပ်ငန်းများကို လုပ်ဆောင်လျက်ရှိပြီး၊ စီမံချက်အတိုင်း ဆက်လက်လုပ်ဆောင်သင့်ပါသည်။

၄။ အစိုးရ ICT ကို တိုးတက်စေခြင်း (A1-A6)

အစိုးရ ICT ကို တိုးတက်စေရန် ရည်ရွယ်ပြီး မြန်မာအစိုးရသည် ဌာနဆိုင်ရာများအကြားတွင် အချက်အလက်များ ဝေမျှခြင်း တိုးတက်စေရန်၊ ကုန်ကျစရိတ် နည်းပါးစေရန်၊ အစိုးရကို e-Government

ကြိုးပမ်းမှုအတွက် ဦးတည်ချက်ထားစေရန် မူဝါဒများချမှတ်ခဲ့ပြီး၊ အချက်အလက် အရင်းအမြစ်များ လုံခြုံရေးကို တိုးတက်စေခဲ့သည်။ ၎င်းတွင်

၁) Cloud First မူဝါဒ

၂) ဒေတာအချက်အလက် အမျိုးအစားခွဲခြားခြင်း မူဘောင်များ တို့ ပါဝင်သည်။

မြန်မာ Cloud First မူဝါဒ

အခန်း (၁) : Cloud First မူဝါဒ အဘယ်ကြောင့် ရှိရသနည်း။

မြန်မာ Cloud First မူဝါဒသည် မြန်မာ e-Government မဟာစီမံကိန်း (Master Plan) ကို ဖြည့်စွက်ပေးသည်[8]။ ၎င်းကို "cloud first" မူဝါဒ အဖြစ် ဖော်ဆောင်ထားသည်။ သီးခြား အချက်အလက် သိုလှောင်သည့် စနစ်များ တည်ဆောက်မည့်အစား အစိုးရကို cloud computing solution များကို ပထမဦးစားပေး ရွေးချယ်အသုံးပြုရန် အားပေးထားသည်။

cloud first မူဝါဒ လမ်းကြောင်းမှ ချဉ်းကပ်ခြင်းသည် ICT လိုအပ်ချက်များအတွက် cloud computing ကို အသုံးပြုနေပြီဖြစ်သော မြန်မာအစိုးရအဖွဲ့၏ နည်းပညာအသုံးပြုမှုကို လျှင်မြန်စွာ ပြောင်းလဲစေပါသည်။ cloud first လမ်းကြောင်းမှ ချဉ်းကပ်ခြင်းသည် ခေတ်သစ် အစိုးရ ICT စနစ်များ၏ ချိတ်ဆက်နိုင်စွမ်းနှင့် အချက်အလက်များ ဖလှယ်ဆောင်ရွက်နိုင်စွမ်း (interconnectivity and interoperability) ကို တိုးတက်လာစေနိုင်ပါသည်။

မြန်မာအစိုးရသည် ပြောင်းလဲဆန်းသစ်မှုနှင့် ထုတ်လုပ်မှုစွမ်းအားတို့ကို မောင်းနှင်ခြင်း၊ နိုင်ငံသားများအတွက် ဝန်ဆောင်မှုများ ပိုမို ထိရောက်စွာ ပေးအပ်ခြင်းနှင့် စီးပွားရေးလုပ်ငန်းများနှင့် အဖွဲ့အစည်းများ၏ လိုအပ်ချက်ကို ပိုမို မြန်ဆန်စွာ တုန့်ပြန်နိုင်ခြင်း၊ အရှိန်နှင့် လျှင်မြန်မှု တိုးတက်လာခြင်း၊ လုံခြုံမှု တိုးတက်လာခြင်း၊ တရိန်တည်းမှာပင် အကျိုးဖြစ်ထွန်းခြင်းနှင့် ကုန်ကျစရိတ် နည်းပါးခြင်းတို့အတွက် cloud computing ဝန်ဆောင်မှုများ၏ ပြည့်ဝသော အကျိုးကျေးဇူးများကို အသိအမှတ်ပြုရပါသည်။

Cloud First မူဝါဒသည် အစိုးရ၏ ရှိနေဆဲ IT မှ ကနဦးခြေလှမ်း ဖြစ်သည်။ Cloud First မူဝါဒသည် အစိုးရအား cloud IT solutions ကို အခြား ရွေးချယ်စရာ နည်းလမ်းများ မတိုင်မီ ထည့်သွင်းစဉ်းစားရန် ညွှန်ကြားသည်။ နောက်ဆုံးတွင် cloud ၏ နောက်ဆုံးပေါ် လုပ်ဆောင်ချက်များနှင့် "born in the cloud"

[8] https://www.motc.gov.mm/sites/default/files/Myanmar%20e-Governance%20Master%20Plan%20%282016-2020%29%20English%20Version%28Draft%29.pdf

solution များကို အကောင်းဆုံး အသုံးပြုထားသည့် အစိုးရပိုင်လုပ်ငန်းများမှာပြောင်းလဲဆန်းသစ်လာပြီး၊ အစိုးရ၏ IT အသုံးပြုမှု အကောင်းဆုံးအခြေအနေသို့ ရောက်ရှိလာပါသည်။

cloud အသုံးပြုနှုန်း တိုးတက် အရှိန်မြှင့်လာခြင်းအားဖြင့် မြန်မာအစိုးရသည် ဥပမာပြ ရှေ့ဆောင်နေပြီး၊ အကျိုးဆက်အားဖြင့် ဒစ်ဂျစ်တယ် စီးပွားရေးတွင် တိုးတက်လာအောင် စွမ်းဆောင်နိုင်လာလိမ့်မည်။ အစိုးရနှင့် ပုဂ္ဂလိက အခန်းကဏ္ဍများတွင် cloud computing ကို ကျယ်ပြန့်စွာ အသုံးချခြင်းသည် အခြားသော နည်းပညာများကို တိုးတက်ဖွံ့ဖြိုးလာစေသည့် အခြေခံ အုတ်မြစ်ဖြစ်သည်။ အကျိုးဆက်အားဖြင့် မျှဝေ လုပ်ဆောင်သည့် e-Government ဝန်ဆောင်မှုများ၊ ဒစ်ဂျစ်တယ်နည်းများဖြင့် စွမ်းဆောင်နိုင်သော အရပ်ဘက် ဝန်ဆောင်မှုများ၊ ဒစ်ဂျစ်တယ်နည်းများအား သုံးစွဲပိုင်ခွင့်ရှိသော နိုင်ငံသားများ စသည်ဖြင့် တိုးတက်လာပြီး၊ ကျွန်ုပ်တို့၏ ဒစ်ဂျစ်တယ် စီးပွားရေးလည်း တိုးတက်လာလိမ့်မည်။

Cloud computing သည် အစိုးရ၏ IT ကို စီမံခန့်ခွဲရာတွင် ပိုမို ထိရောက်သည့် နည်းလမ်းသစ်များ အဖြစ် ရောက်ရှိလာလိမ့်မည်။ အစိုးရအဆင့်အားလုံး၊ အဖွဲ့အစည်းနှင့် အင်စတီကျူရှင်းများကို "cloud first" နည်းလမ်းကို ထက်သန်စွာ အသုံးပြုကြရန် အားပေးပါသည်။ ဤစာရွက်စာတမ်းများကို အစိုးရ ဝန်ကြီးဌာနများ၊ အေဂျင်စီများနှင့် ဌာနခွဲများအတွက် cloud computing solution များကို ၎င်းတို့၏ IT စီမံချက်နှင့် ဖြည့်ဆည်းမှု၏ အဓိကအပိုင်းအဖြစ် အသုံးချဖို့ စဉ်းစားနိုင်ရန် အခြေခံသဘောတရားလမ်းညွှန်အဖြစ် ရည်ရွယ်ပါသည်။ နောက်ဆုံးတွင် အစိုးရသည် cloud native ဖြစ်လာပြီး၊ cloud ၏ နောက်ဆုံးပေါ် လုပ်ဆောင်ချက်များနှင့် "born in the cloud" solution များကို အကောင်းဆုံး အသုံးပြုထားသည့် အစိုးရပိုင်စီးပွားရေးလုပ်ငန်းများပြောင်းလဲဆန်းသစ်လာပြီး အကောင်းဆုံး အခြေအနေကို ရောက်ရှိလာမည်။

ဌာနဆိုင်ရာအလိုက် အကောင်အထည်ဖော် ဆောင်ရွက်ခြင်း

အစိုးရပိုင် ကော်ပိုရေးရှင်းများနှင့် ပညာရေးဆိုင်ရာ အဖွဲ့အစည်းများ အပါအဝင် အစိုးရဝန်ကြီးဌာန၊ ဌာနဆိုင်ရာများ၊ ဌာနခွဲများအားလုံး ၎င်းတို့၏ ကိုယ်ပိုင် စီမံခန့်ခွဲရေးနှင့် အစိုးရ၏ ဝန်ဆောင်မှုပေးခြင်း လုပ်ငန်းများအတွက် ICT ကို ထိရောက်စွာ အသုံးချရေးတွင် ဦးစားပေး မဟာဗျူဟာအဖြစ် -

- အစိုးရ ဌာနဆိုင်ရာများ၏ အထူးလိုအပ်ချက်များကို ဖြည့်ဆည်းနိုင်သည့်
- စုစုပေါင်း ပိုင်ဆိုင်မှု ကုန်ကျစရိတ် (Total Cost of Ownership, TCO) ရှုထောင့်မှကြည့်လျှင် ပို၍ ကုန်ကျစားရိတ်နှင့် ကာမိနိုင်သည့်
- cloud computing အသုံးပြုခြင်းနှင့် တူညီသော လုံခြုံရေး အာမခံချက်အဆင့်မျိုး ရှိသည့် ICT ကို ထိရောက်စွာ အသုံးချရေး နောက်ထပ် မဟာဗျူဟာတစ်ခု ပေါ်ပေါက်လာသည် မှအပ cloud computing ကို အသုံးပြုကြရန် တိုက်တွန်းပါသည်။

Cloud Computing ၏ အကျိုးကျေးဇူးများ

Cloud computing သည် လိုအပ်ချက်ပေါ် မူတည်၍ အရေအတွက်အမျိုးမျိုး ရရှိနိုင်သော IT အခြေခံအဆောက်အအုံ၊ တွက်ချက်လုပ်ဆောင်ခြင်း (processing)၊ သိမ်းဆည်းခြင်း၊ ကွန်ယက်များ၊ လုပ်ဆောင်လည်ပတ်သည့် စနစ်များ (operating systems) နှင့် အသုံးချ application များကို ခြုံငုံမိစေသည့် ခြုံငုံဖော်ပြသည့် (holistic) အသုံးအနှုန်းတစ်ခုဖြစ်သည်။ cloud အခြေခံသော ပုံစံသည် ပိုမိုခိုင်မာသော ဘတ်ဂျက်ထိန်းချုပ်မှု (budget control) နှင့် ဘဏ္ဍာရေးလိုအပ်ချက်များကို ပိုမို လျှင်မြန်စွာ ဖြေရှင်းနိုင်စေသည်။

ကနဦး၌ ပြောင်းလွယ်ပြင်လွယ်ရှိမှုနှင့် ကုန်ကျစရိတ်သက်သာမှုကို အလိုရှိသည့် အစိုးရ၏ ဆန္ဒကြောင့် Open Source Software များအပေါ် စိတ်ဝင်စားမှု ရှိခဲ့သည်။ ဤစိတ်ဝင်စားမှုကို cloud computing ၏ အသုံးဝင်သော မော်ဒယ်လ်များက ဖယ်ရှားလိုက်သည်။ cloud computing model များသည် မြန်ဆန်စွာ စွမ်းဆောင်နိုင်ခြင်းအားဖြင့် များပြားသည့် လိုအပ်ချက် အပြောင်းအလဲများမှ အစိုးရကို အကျိုးကျေးဇူးရရှိစေသည်။ ဤသည်မှာ cloud computing model ၏ အခြေခံကျသောအချက်ဖြစ်ပြီး၊ နိုင်ငံသားများအတွက် ဝန်ဆောင်မှုသစ်များ လျှင်မြန်စွာ ကျယ်ပြန့်တိုးတက်လာခြင်းကို ထောက်ပံ့ပေးခြင်းနှင့် လူထုဝန်ဆောင်မှု ပြောင်းလဲဆန်းသစ်ခြင်း၏ အရွေ့သစ်တစ်ခုကို စွမ်းဆောင်နိုင်ခြင်းပင် ဖြစ်သည်။

1. "သင်သုံးသည့်အရာအတွက် ပေး (pay for what you use)" ဟူသည့် သုံးစွဲမှုအခြေပြု (utility-based) ငွေကြေးထိန်းချုပ်မှု (budget control) ပုံစံ - အစိုးရအေဂျင်စီများသည် အနာဂတ်ခန့်မှန်းချက် (သို့) လိုအပ်ချက် အမြင့်ဆုံးအချိန်ပေါ် မူတည်၍ ပိုလွန်စွာဖြည့်တင်းထားခြင်း မရှိဘဲ သုံးစွဲလိုက်သော အရင်းအမြစ်များအတွက်သာ ပေးသည်။ အရွယ်အစား ချုံ့နိုင် ချဲ့နိုင်သော

cloud computing ဝန်ဆောင်မှုများသည် စနစ်၏ အသုံးပြုမှုကို တနှစ်ပတ်လုံး လိုအပ်သလို တိုးမြှင့်နိုင် (သို့) လျော့ချနိုင်သည်။ (ဥပမာ - ဝင်ငွေခွန်ဆောင်ရမည့် သတ်မှတ်ရက်များ အနီးတဝိုက်တွင်) သုံးစွဲမှုအခြေပြု ငွေကြေးကျသင့်မှု ပုံစံ (utility-based pricing structure) ၏ ပွင့်လင်းမြင်သာရှိခြင်းသည် ဘတ်ဂျက်ထိန်းချုပ်မှု (budget control) ကို အထောက်အကူပေးသော သုံးစွဲသည့်ပမာဏ သတိပေးချက် (spending caps and alerts) ကိုလည်း အသုံးပြုနိုင်သည်။

2. ICT အခြေခံအဆောက်အအုံအတွက် အရင်းအနှီး သုံးစွဲမှုကို လျော့ချခြင်း - အစိုးရဝန်ဆောင်မှုလုပ်ငန်းများကို cloud computing သို့ ခွဲဝေလုပ်ကိုင်စေခြင်း (outsourcing) အားဖြင့် ICT အခြေခံ အဆောက်အအုံနှင့် ထိန်းသိမ်းမှု ကုန်ကျစရိတ်အတွက် များပြားသော ရင်းနှီးငွေ လျော့ကျခြင်းအကျိုးကို ချက်ခြင်း ရရှိနိုင်သည်။ ပိုမို အသုံးများသော လုပ်ဆောင်ချက်များ - အကောင်းဆုံး ဝန်ဆောင်မှုများ အပါအဝင် - အစိုးရအေဂျင်စီများအတွက် cloud ဖြည့်ဆည်းခြင်းမှတဆင့် ပြုလုပ်နိုင်သည်။ ထို့ပြင် လုပ်ငန်းလည်ပတ်မှုဆိုင်ရာအခြေခံပေါ်တွင် မူတည်၍ ကုန်ကျစရိတ်ကို စီမံခန့်ခွဲနိုင်သည်။ ဟာ့ဒ်ဝဲရ်နှင့် ဆော့ဖ်ဝဲရ် နှစ်မျိုးလုံး၏ ဗားရှင်း အဆင့်မြှင့်ခြင်းကို cloud service provider (CSP) က စီမံခန့်ခွဲသည့်အတွက် cloud first model က အစိုးရ ICT ၏ ပြောင်းလွယ်ပြင်လွယ်ရှိမှုနှင့် လုံခြုံမှုကို တိုးမြင့်စေသည်။

3. ဝန်ဆောင်မှုများ အသုံးချခြင်းကို ပိုမို မြန်ဆန်စေခြင်း - ICT အခြေခံအဆောက်အအုံ တည်ဆောက်ရန် နေရာလိုအပ်ချက် ပမာဏနှင့် အစိုးရဌာနဆိုင်ရာများ၏ ပိုင်ဆိုင်မှုကို လျော့ချနိုင်ခြင်းသည် စုစုပေါင်း အချိန် အသုံးပြုမှုကိုလည်း လျော့ချနိုင်သည်။ ထို့ပြင် ဦးတည်ချက်ကိုလည်း အခြေခံအဆောက်အအုံ စီမံခန့်ခွဲခြင်းမှ ဝန်ဆောင်မှုများ ပေးအပ်ခြင်းပေါ် သို့ ပြောင်းလဲထားရှိလာနိုင်သည်။ အကယ်၍ အစိုးရဌာနဆိုင်ရာများသည် သီးသန့်ကွဲပြားသော ကိုယ်ပိုင် ကွန်ပျူတာဌာန များကို ကိုယ်တိုင် လည်ပတ်လုပ်ဆောင်လျှင်၊ လူထုအတွက် cloud ICT အသုံးချစရာများနှင့် ဝန်ဆောင်မှုများကို ပိုမို လျှင်မြန်စွာ စမ်းသပ် အသုံးပြုနိုင်သည်။ ပိုမို အကျိုးသက်ရောက်မှုရှိသော ကုန်ကျစရိတ်ဖြင့် ထိန်းသိမ်းနိုင်သည်။

4. နိုင်ငံသားများအတွက် ပိုမို စွမ်းဆောင်နိုင်သော၊ ပိုမိုကောင်းမွန်သော ဝန်ဆောင်မှုများအတွက် အေဂျင်စီအချင်းချင်း ပူးပေါင်းဆောင်ရွက်ခြင်း - cloud သည် လူထု

ဝန်ဆောင်မှုပေးခြင်းလုပ်ငန်းတွင် ပိုမို မြင့်မားသော စွမ်းဆောင်မှု၊ စွန့်ဦးတီထွင်မှုနှင့် တီထွင်ဖန်တီးနိုင်စွမ်းတို့ ဖြစ်ပေါ်စေလျက် ၎ နဆိုင်ရာများအချင်းချင်း အဖွဲ့အစည်းတစ်ခုမှ တစ်ခုသို့ အရင်းအမြစ်များနှင့် သတင်းအချက်အလက်များကို ပိုမိုလွယ်ကူစွာ ဝေမျှနိုင်ခြင်းသည့်အတွက် ပို၍ ထိရောက်အကျိုးရှိသော ပူးပေါင်းဆောင်ရွက်မှုကို ဖြစ်ပေါ်စေသည်။

5. လုပ်ငန်းလည်ပတ်မှုဆိုင်ရာ အလျင်မပြတ်ခြင်းနှင့် စီးပွားရေး ပြန်လည်ထူမတ်ခြင်း - cloud တွင် အချက်အလက်များ သိမ်းဆည်းခြင်း၊ စီမံခန့်ခွဲခြင်းနှင့် အရန်ထားခြင်းအားဖြင့် အကျဉ်းအကြပ်တွေ့ချိန်တွင် အချက်အလက်များ ပြန်လည်ထုတ်ယူခြင်း၊ စီးပွားရေးလုပ်ငန်း အလျင်မပြတ်ခြင်းနှင့် ပြန်လည်ထူထောင်ခြင်း (ဥပမာ - သဘာဝဘေးအန္တရာယ်များ၊ သို့မဟုတ် အခြား အနှောင့်အယှက် အဖျက်အဆီးများ) ပိုမို မြန်ဆန် လွယ်ကူပြီး၊ ပိုမို cost effective (ထိရောက်မှုရှိသော ကုန်ကျစရိတ်) ဖြစ်စေသည်။

အခန်း (2) : အသုံးအနှုန်း အဓိပ္ပါယ်ဖွင့်ဆိုချက်များ

ဤအခန်းသည် cloud computing နှင့် ဆက်စပ်သည့် အဓိက အကြောင်းအရာ အများအပြားကို ခြုံငုံထားသည်။

Cloud Computing ဆိုသည်မှာ အဘယ်နည်း။

Cloud Computing သည် စီစဉ်အသုံးချ၍ရသော computing အရင်းအမြစ် အစုအဝေး (ဥပမာ - ကွန်ယက်များ၊ ဆာဗာများ၊ သိမ်းဆည်းရန်နေရာများ၊ အသုံးချ application များနှင့် ဝန်ဆောင်မှုများ) ကို ဝေမျှသုံးစွဲရန်၊ စီမံခန့်ခွဲမှု အနည်းငယ် (သို့) ဝန်ဆောင် တုန့်ပြန်မှုပေးသူ (service provider interaction) အနည်းငယ်ဖြင့် လျင်မြန်စွာ ဖြည့်ဆည်းခြင်း၊ ရယူခြင်း ပြုလုပ်နိုင်သည့် နေရာအနှံ့တွေ့ရသော၊ အဆင်ပြေသော၊ လိုအပ်ချက်ပေါ်မူတည်၍ အသုံးပြုနိုင်သော ကွန်ယက် (on-demand network) ပုံစံတစ်ခု ဖြစ်သည်။ ဤ cloud model သည် လက္ခဏာရပ် (၅) ခု၊ အသုံးချမှု ပုံစံ (၅) ခုနှင့် အချို့သော အာမခံချက်များနှင့် ဖွဲ့စည်းထားသည်။

အဓိက လက္ခဏာရပ်များ[9]

- **လိုအပ်ချက်ပေါ်မူတည်၍ အသုံးပြုနိုင်သော ကိုယ်တိုင်ပေး ဝန်ဆောင်မှု။** သုံးစွဲသူသည် ဆာဗာအချိန်နှင့် ကွန်ယက်တွင် သိမ်းဆည်းမှု (server time and network storage) ကဲ့သို့ computing စွမ်းဆောင်မှုများကို service provider တစ်ယောက်စီထား၍ လူကိုယ်တိုင် တုန့်ပြန်ဝန်ဆောင်မှုပေးရန် မလိုဘဲ၊ မိမိဘာသာ လိုအပ်သလို အလိုလျောက် ဖြည့်ဆည်းနိုင်သည်။
- **ကျယ်ပြန့်သော ကွန်ယက် သုံးစွဲနိုင်မှု။** စွမ်းဆောင်ရည်များကို ကွန်ယက်များ၊ အမျိုးစုံ ရောနှောနေသော သုံးစွဲသူများ၏ လွယ်ကူသော၊ ခက်ခဲသော (thin & thick) platform များ (ဥပမာ - မိုဘိုင်းလ်ဖုန်းများ၊ တက်ဘလက်များ၊ လက်ပ်တော့များနှင့် Workstation များ) ဖြင့် အသုံးပြုခြင်းကို မြှင့်တင်ထားသော စံပြု လုပ်ဆောင်ချက်များကို အသုံးပြုခြင်းအားဖြင့် အသင့်ရရှိနိုင်သည်။
- **အရင်းအမြစ် အစုအဝေး။** ဝန်ဆောင်မှုပေးသူ၏ computing အရင်းအမြစ်များသည် အမျိုးမျိုးသော သုံးစွဲသူများကို ဝန်ဆောင်မှုပေးရန် စုဝေးထားသည်။ အမျိုးမျိုးသော ရုပ်ပိုင်းနှင့် virtual အရင်းအမြစ်များကို သုံးစွဲသူ၏ လိုအပ်ချက်အရ သတ်မှတ်ခွဲဝေခြင်းနှင့် ပြန်လည် သတ်မှတ်ခွဲဝေခြင်းကို အင်တိုက်အားတိုက် ပြုလုပ်နိုင်သည်။ ပေးထားသည့် အရင်းအမြစ်များ၏ တိကျသော တည်နေရာအတွက် ထိန်းချုပ်မှုနှင့် သိနားလည်ခြင်း မရှိသော သုံးစွဲသူအတွက် လွတ်လပ်သည့် တည်နေရာရှာဖွေနိုင်ခြင်း အသိ (sense of location) ရှိနိုင်ပါသည်။ သို့သော် တည်နေရာ ခန့်မှန်းရ ပိုခက်သည့် အနေအထား (higher level of abstraction) (ဥပမာ - တိုင်းပြည်၊ ပြည်နယ်နှင့် အချက်အလက် ဌာန (data center)) တွင် တည်နေရာကို သတ်မှတ်နိုင်ပါလိမ့်မည်။ သိမ်းဆည်းခြင်း၊ တွက်ချက်ဆောင်ရွက်ခြင်း၊ မှတ်ဉာဏ်နှင့် ကွန်ယက် bandwidth အပါအဝင် အရင်းအမြစ်များ၏ ဥပမာများ။
- **လျင်မြန်သော ပြောင်းလွယ်ပြင်လွယ်ခြင်း။** စွမ်းဆောင်ရည်များ ဖြည့်ဆည်းခြင်းနှင့် ထုတ်ယူခြင်းကို ပြောင်းလွယ်ပြင်လွယ် ပြုလုပ်နိုင်သည်။ အချို့ကိစ္စများတွင် လိုအပ်ချက်အတိုင်း အချိုးကျ အလိုလျောက် ပြောင်းလဲနိုင်သည်။ သုံးစွဲသူများအတွက် ရရှိနိုင်သော စွမ်းဆောင်ရည် ဖြည့်တင်းမှုသည် တခါတရံတွင် အကန့်အသတ်မရှိ ဖြစ်နိုင်ပြီး၊ မည်သည့်အချိန်၊ မည်သည့် အရေအတွက် အတွက်မဆို သတ်မှတ်ခွဲဝေနိုင်သည်။

[9] http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

- **ပုံမှန် ဝန်ဆောင်မှုများ** Cloud စနစ်သည် ဝန်ဆောင်မှု အမျိုးအစားများ (ဥပမာ - သိမ်းဆည်းခြင်း၊ တွက်ချက်ဆောင်ရွက်ခြင်း၊ bandwidth နှင့် အသုံးပြုသူများ၏ အသက်ဝင်နေသော အကောင့်တ်များ (active user accounts)) အတွက် သင့်လျော်သည့် အချို့သော အယူအဆ အဆင့် (level of abstraction) တွင် တိုင်းတာနိုင်စွမ်း (metering capability) တစ်ခုကို မြှင့်တင်ခြင်းဖြင့် အရင်းအမြစ်များ အသုံးပြုခြင်းကို အလိုလျောက် ထိန်းချုပ်ပြီး အသင့်လျော်ဆုံးဖြစ်အောင် အလိုလျောက် ဆောင်ရွက်သည်။ အသုံးပြုသည့် ဝန်ဆောင်မှုများ၏ ဝန်ဆောင်မှုပေးသူနှင့် သုံးစွဲသူ နှစ်ဘက်စလုံးကို ပွင့်လင်းမြင်သာမှုရှိအောင် ပြုလုပ်ပေးခြင်းဖြင့် အရင်းအမြစ် အသုံးပြုခြင်းကို စောင့်ကြည့်အကဲဖြတ်၊ ထိန်းချုပ်၊ အစီရင်ခံခြင်းများ ပြုလုပ်နိုင်သည်။

Cloud အသုံးပြုခြင်း ပုံစံ

- **ပုဂ္ဂလိက** Cloud အခြေခံအဆောက်အအုံကို အမျိုးမျိုးသော သုံးစွဲသူများဖြင့် ဖွဲ့စည်းထားသည့် အဖွဲ့အစည်းတစ်ခု၏ သဟဇာတဖြစ်သော တပေါင်းတစည်းတည်း အသုံးပြုမှုအတွက် ဖြည့်ဆည်းထားသည်။ (ဥပမာ - စီးပွားရေး ယူနစ်များ) ၎င်းကို အဖွဲ့အစည်း၊ ပြင်ပလူ/အဖွဲ့အစည်း (သို့) ၎င်းတို့၏ အခြားသော ပူးပေါင်းမှုများမှ ပိုင်ဆိုင်၊ စီမံခန့်ခွဲ၊ လုပ်ကိုင်လည်ပတ်နိုင်သည်။ ၎င်းသည် အသုံးပြုသည့် တည်နေရာ (သို့) အသုံးပြုသည့်တည်နေရာ၏ ပြင်ပ တွင် တည်ရှိနိုင်သည်။
- **Virtual private** cloud အခြေခံအဆောက်အအုံကို အဖွဲ့အစည်း (organisation) တစ်ခု၏ တပေါင်းတစည်းတည်း အသုံးပြုမှုအတွက် တကမ္ဘာလုံးဆိုင်ရာ လုံခြုံမှုနှင့် လိုက်လျောညီထွေရှိမှု စံနှုန်းများကို တိုးမြှင့်ပြီး ဖြည့်ဆည်းထားသည်။ ၎င်းက ခိုင်မာ၍ သီးခြားဖြစ်သည့် အသုံးပြုသည့်တည်နေရာ၏ ပြင်ပ virtual private cloud environment ကို ပေးနိုင်သည်။ အဖွဲ့အစည်းတစ်ခု၏ တပေါင်းတစည်းတည်း အသုံးပြုမှုအတွက် သီးခြား အခြေခံအဆောက်အအုံကိုလည်း ပေးနိုင်သည်။
- **အဖွဲ့အစည်း** cloud အခြေခံအဆောက်အအုံကို ဝေမျှရန် အကြောင်းအရာများ (ဥပမာ - တာဝန်များ၊ လုံခြုံရေး လိုအပ်ချက်များ၊ မူဝါဒများ၊ လိုက်လျောညီထွေ တွေးဆချက်များ) ရှိသော အဖွဲ့အစည်းများမှ သုံးစွဲသူများ၏ သီးခြားအဖွဲ့အစည်း (specific community) တစ်ခုအားဖြင့် တပေါင်းတစည်းတည်း အသုံးပြုမှုအတွက် ဖြည့်ဆည်းထားသည်။ ၎င်းကို အသိုင်းအဝန်းအတွင်းရှိ

တခု (သို့) တခုထက်ပိုသော အဖွဲ့အစည်းများ၊ ပြင်ပလူ/အဖွဲ့အစည်း (သို့) ၎င်းတို့၏ အခြားသော ပူးပေါင်းမှုများမှ ပိုင်ဆိုင်၊ စီမံခန့်ခွဲ၊ လုပ်ကိုင်လည်ပတ်နိုင်သည်။ ၎င်းသည် အသုံးပြုသည့် တည်နေရာ (သို့) အသုံးပြုသည့်တည်နေရာ၏ ပြင်ပ တွင် တည်ရှိနိုင်သည်။

- **စီးပွားရေး** cloud အခြေခံအဆောက်အအုံကို လူထု လွတ်လပ်စွာ အသုံးပြုနိုင်ရန် ပြင်ဆင်ထားပြီးဖြစ်သည်။ ၎င်းကို စီးပွားရေးလုပ်ငန်းတစ်ခု၊ (သို့) ပညာရေးဆိုင်ရာ အဖွဲ့အစည်း (သို့) အစိုးရအဖွဲ့အစည်း (သို့) ၎င်းတို့၏ အခြားသော ပူးပေါင်းမှုများမှ ပိုင်ဆိုင်၊ စီမံခန့်ခွဲ၊ လုပ်ကိုင်လည်ပတ်နိုင်သည်။ ၎င်းသည် အသုံးပြုသည့် တည်နေရာ (သို့) အသုံးပြုသည့်တည်နေရာ၏ ပြင်ပ တွင် တည်ရှိနိုင်သည်။ ၎င်းသည် cloud ဝန်ဆောင်မှုပေးသူ၏ နေရာပေါ်တွင် တည်ရှိသည်။
- **နှစ်မျိုးစပ်** cloud အခြေခံအဆောက်အအုံသည် နှစ်ခု (သို့) ထို့ထက်ပိုသော ထင်ရှားသည့် cloud အခြေခံအဆောက်အအုံများ (ပုဂ္ဂလိက၊ အဖွဲ့အစည်း (သို့) ပြည်သူလူထု) ပေါင်းစပ်ထားခြင်းဖြစ်သည်။ သီးခြားဖြစ်သော အဆောက်အအုံများ၊ သို့သော်လည်း စံနှုန်းသတ်မှတ်ခြင်း (သို့) ဝန်ကျဉ်းသယ်ဆောင်ရလွယ်စေသော အချက်အလက်နှင့် application (ဥပမာ - cloud များကြားတွင် load များ ထိန်းညှိခြင်းအတွက် cloud ကျိုးပေါက်ခြင်း - cloud bursting for load balancing between clouds) များဖြစ်စေသည့် နည်းပညာ ပိုင်ဆိုင်မှုအားဖြင့် အတူတကွ ပေါင်းစည်းထားသော အဆောက်အအုံများအဖြစ် တည်ရှိစေသည်။
- အစိုးရ Cloud ပြည်သူ့ဝန်ဆောင်မှု cloud အခြေခံအဆောက်အအုံကို အစိုးရအေဂျင်စီများ အသုံးပြုရန်အတွက် အစိုးရမှ ဖြည့်ဆည်းသည်။ ၎င်းတွင် Cloud အသုံးပြုခြင်း ပုံစံအမျိုးမျိုး (ပြည်သူလူထု၊ ပုဂ္ဂလိက၊ အဖွဲ့အစည်း၊ နှစ်မျိုးစပ်) ပါဝင်သည်။ တခုချင်းစီသည် outsource (ဝန်ဆောင်မှု/ လုပ်ဆောင်ချက်ကို ပြင်ပ ကုမ္ပဏီသို့ လွှဲပြောင်း လုပ်ခိုင်းခြင်း) လုပ်ခြင်း (သို့) အစိုးရမှ ပိုင်ဆိုင်ခြင်း ဖြစ်နိုင်သည်။ အစိုးရ cloud ဝန်ဆောင်မှုပေးသူများသည် အစိုးရပိုင် ကော်ပိုရေးရှင်းများနှင့် ပညာရေးအဖွဲ့အစည်းများ အပါအဝင် ဝန်ကြီးဌာနများ၊ အေဂျင်စီများ၊ ဌာနခွဲများကို ဝန်ဆောင်မှုများပေးရန် ကြိုတင်၍ တရားဝင် အသိအမှတ်ပြုမှုကို ရရှိထားသင့်ပါသည်။ အစိုးရ cloud ဝန်ဆောင်မှုပေးသူများသည် အစိုးရအေဂျင်စီများကို ဝန်ဆောင်မှုများပေးရန် အနိမ့်ဆုံးသတ်မှတ်ချက် စံနှုန်းများကို ပြည့်မီသင့်ပါသည်။ (တရားဝင် အသိအမှတ်ပြု လုပ်ငန်းစဉ်ကို ကြည့်ပါ။)

အာမခံ ချဉ်းကပ်ခြင်း လမ်းကြောင်းများ : ခွဲဝေထားသော တာဝန်များ

cloud ဝန်ဆောင်မှုများ ဖြည့်ဆည်းခြင်း အကြောင်းအရာတွင်၊ သုံးစွဲသူတစ်ယောက်က ကွန်ပြူတာအချက်အလက်များ (သို့) systems/applications ကို cloud computing ဝန်ဆောင်မှုသို့ ရွှေ့ပြောင်းသည့်အခါ၊ CSP နှင့် သုံးစွဲသူကြားတွင် တာဝန် ခွဲဝေယူရမည်။ ဤ အကြောင်းအရာတွင် သုံးစွဲသူသည် အစိုးရအေဂျင်စီနှင့် စာချုပ်ချုပ်ဆိုထားလိမ့်မည်။ အစိုးရအေဂျင်စီသည် အေဂျင်စီ၏ ထိန်းချုပ်မှုအောက်မှ အချက်အလက်များ စီမံခန့်ခွဲခြင်းကို တာဝန်ယူဆောင်ရွက်ရန် အစိုးရ အချက်အလက် မန်နေဂျာတစ်ယောက်ကို ခန့်ထားလိမ့်မည်။ (အချက်အလက် အမျိုးအစားခွဲခြားခြင်း စနစ်နှင့် လုံခြုံရေး ထိန်းချုပ်မှု မူဘောင်များကို ကြည့်ပါ။)

အချို့သော လုံခြုံရေး၊ အချက်အလက် ကာကွယ်ရေးနှင့် လိုက်လျောညီထွေရှိရေး ကဏ္ဍများကို အစိုးရအေဂျင်စီက လုပ်ဆောင်ပြီး၊ အခြားသော ကဏ္ဍများကို CSP မှ တာဝန်ယူသည်။

- cloud သုံးစွဲသူသည် အချက်အလက် စုဆောင်းသူအဖြစ် ဆောင်ရွက်သည်။ ၎င်း၏ အကြောင်းအရာကို ထိန်းချုပ်သည်။ မည်သူက ၎င်းကိုယ်စား ထိုအကြောင်းအရာကို ဆက်လက်လုပ်ဆောင်မည်ဆိုသည့်အချက် အပါအဝင် အကြောင်းအရာ၏ တင်ပြပုံ (treatment) ကို ဆုံးဖြတ်သည်။ အစိုးရအေဂျင်စီများ/ မိတ်ဖက်များက တာဝန်များနှင့် guest operating system (ပြင်ဆင်ဖြည့်စွက်ခြင်းနှင့် လုံခြုံရေးလုပ်ပိုင်ခွင့်များ အပါအဝင်) အခြားသော ပေါင်းစပ်ပါဝင်သည့် application software, configuration of security group firewalls နှင့် အခြားသော လုံခြုံရေး၊ ပြောင်းလဲမှု စီမံခန့်ခွဲခြင်းနှင့် logging feature များ၏ စီမံခန့်ခွဲမှုများကို လုပ်ဆောင်သည်။
- cloud ဝန်ဆောင်မှုပေးသူသည် အချက်အလက် တွက်ချက်ဆောင်ရွက်သူအဖြစ် လုပ်ဆောင်သည်။ ဝန်ဆောင်မှုပေးသူသည် သုံးစွဲသူတစ်ဦးချင်းစီမှ ရွေးချယ်သော ဝန်ဆောင်မှုများပေးရန်သာ သုံးစွဲသူ၏ အကြောင်းအရာများကို အသုံးပြုသည်။ သုံးစွဲသူ၏ အကြောင်းအရာများကို အခြားသော ရည်ရွယ်ချက်များအတွက် အသုံးမပြုပါ။ CSP သည် ပုံမှန်အားဖြင့် cloud သုံးစွဲသူ၏ အချက်အလက်များကို ဝင်ရောက်အသုံးပြုနိုင်ခြင်း (သို့)

ထိန်းချုပ်နိုင်ခြင်း မရှိပါ။ CSP သည် အခြေခံအဆောက်အအုံ အစိတ်အပိုင်းများကို host operating system နှင့် virtualisation layer မှနေ၍ ဝန်ဆောင်မှု လုပ်ဆောင်လည်ပတ်သည့် facilities ၏ ရုပ်ပိုင်း လုံခြုံရေးအထိ လုပ်ဆောင်လည်ပတ်၊ စီမံခန့်ခွဲ၊ ထိန်းချုပ်သူ ဖြစ်သည်။

cloud solution တစ်ခု၏ လုံခြုံရေးကို စိစစ်အကဲဖြတ်သည့်အခါ အစိုးရဌာနဆိုင်ရာများအတွက် -

- CSP မှ အကောင်အထည်ဖော် လုပ်ဆောင်သည့် လုံခြုံရေး လုပ်ဆောင်ချက်များ : cloud ၏ လုံခြုံရေး နှင့်
- သုံးစွဲသူမှ အကောင်အထည်ဖော် လုပ်ဆောင်သည့်၊ cloud ဝန်ဆောင်မှုများကို အသုံးပြုသည့် သုံးစွဲသူ၏ အကြောင်းအရာ၊ application များနှင့် သက်ဆိုင်သည့် လုံခြုံရေး လုပ်ဆောင်ချက်များ : cloud အတွင်း လုံခြုံမှုရှိရေးတို့ နှစ်မျိုးကြားတွင် နားလည်ရန်နှင့် ခွဲခြားသိမြင်ရန် အရေးကြီးသည်။

ပုံမှန်အားဖြင့် CSP သုံးစွဲသူသည် logical လုံခြုံရေး ထိန်းချုပ်မှုကို ဆောင်ရွက်ပြီး၊ CSP သည် အချက်အလက် ဌာန (data centre) ၏ ရုပ်ပိုင်းလုံခြုံရေး ထိန်းချုပ်မှုအတွက် တာဝန်ရှိသည်။ မည်သို့ပင်ဖြစ်စေ၊ နှစ်ဘက်စလုံးအပေါ်ရှိ တာဝန်ယူမှု အဆင့်နှင့် သဘောသဘာဝသည် cloud အသုံးပြုခြင်းပုံစံပေါ်တွင် မူတည်သည်။ အစိုးရအေဂျင်စီများ (သုံးစွဲသူများ) သည် ပုံစံတစ်မျိုးစီတွင် ၎င်းတို့၏ တာဝန်ကို ရှင်းလင်းစွာ နားလည်သင့်ပါသည်။

အခန်း (3) : လုံခြုံမှုနှင့် စံနှုန်း သတ်မှတ်ခြင်း

အစိုးရ၏ အလုပ်များနှင့် အချက်အလက်များကို commerical cloud ပေါ်သို့ ရွှေ့ပြောင်းခြင်း၏ အကျိုးကျေးဇူးမှာ အချက်အလက်များ၏ အထွေထွေ လုံခြုံမှုကို တိုးမြှင့်နိုင်စွမ်းပင်ဖြစ်သည်။ Cloud ဝန်ဆောင်မှုပေးသူသည် (ငွေချေကဒ်လုပ်ငန်း (PCI), အချက်အလက် လုံခြုံရေး စံနှုန်းများ (DSS) ကဲ့သို့) နိုင်ငံတကာ လုံခြုံရေးစံနှုန်းများကို ပြည့်မီပါလိမ့်မည်။ သင့်လျော်စွာ အသိအမှတ်ပြုခြင်း ခံရလိမ့်မည် (ISO9001, ISO27001 ကဲ့သို့)။ သင့်လျော်သော လုပ်ငန်းစံနှုန်းများအားလုံးကို လိုက်နာရမည်။

၎င်း၏ ကိုယ်ပိုင် အချက်အလက်များ ထိန်းချုပ်မှု လိုအပ်ချက်များ (အချက်အလက်များ အမျိုးအစားခွဲခြားခြင်း မူဘောင်များကို ကြည့်ပါ။) အတွက် အန္တရာယ် စီမံခန့်ခွဲမှု ချဉ်းကပ်ခြင်းနည်းလမ်းကို

အသုံးပြုထားသော၊ အကာအကွယ်ပေးနိုင်သော လုံခြုံရေး မူဝါဒကို အသုံးပြုသည့် အစိုးရဌာနဆိုင်ရာများကို ထောက်ခံပါသည်။ ၎င်းလုံခြုံရေး ထိန်းချုပ်မှု မူဘောင်များကို နိုင်ငံတကာ စံနှုန်းများ၊ အသိအမှတ်ပြုခြင်းများ၊ လုပ်ငန်းစံနှုန်းများနှင့် ကိုက်ညီစေရမည်။ စာချုပ်ချုပ်ဆိုထားသော cloud ဝန်ဆောင်မှုများအတွက် လုံခြုံရေး လိုအပ်ချက်များ၏ တိကျသောအဆင့်ကို အချက်အလက်များ၏ အန္တရာယ်များ စိစစ်အကဲဖြတ်ချက်ပေါ် မူတည်၍ စာချုပ်အေဂျင်စီက ဆုံးဖြတ်သင့်ပါသည်. သတ်မှတ်ပြဋ္ဌာန်းထားသော လုံခြုံရေး ထိန်းချုပ်မှုများတွင် အောက်ပါအချက်များထဲမှ တစ်ခု (သို့) တစ်ခုထက်ပို၍ ပါဝင်နိုင်သည်။

- ရုပ်ပိုင်းနှင့် သဘာဝပတ်ဝန်းကျင်ဆိုင်ရာ လုံခြုံရေး
- စီးပွားရေး အလျင်မပြတ်ရန် စီမံခန့်ခွဲခြင်းနှင့် အဖြစ်အပျက်များကို တုန့်ပြန်ခြင်း
- စစ်တမ်းများနှင့် အစီအစဉ်ချထားမှုများ (configuration) အား စီမံခန့်ခွဲခြင်း
- အချက်အလက်များကို ကုဒ် အဖြစ်သို့ပြောင်းခြင်း
- သုံးစွဲမှုကို ထိန်းချုပ်ခြင်း၊ စောင့်ကြည့်စစ်ဆေးခြင်းနှင့် ဝင်ရောက်ခြင်း
- ကွန်ယက် လုံခြုံမှုနှင့် စောင့်ကြည့်စစ်ဆေးခြင်း

Cloud First environment အတွက် သင့်လျော်သော လုံခြုံရေး ထိန်းချုပ်မှု မူဘောင်များကို အကောင်အထည်ဖော်ရန် cloud အတွင်းမှ လုံခြုံရေးအတွက် စာချုပ်ချုပ်ထားသော အစိုးရအေဂျင်စီများနှင့် CSP ကြားတွင် တာဝန်ခွဲဝေယူရမည်ဖြစ်ကြောင်း အစိုးရအေဂျင်စီများအနေဖြင့် ဦးစွာ နားလည်ထားသင့်ပါသည်။

အချက်အလက်များအပေါ် သက်ရောက်သော ဥပဒေ (Data Sovereignty)

အချက်အလက်များပေါ်တွင် နေထိုင်ခွင့် ကန့်သတ်ချက် မရှိသည့်အတွက် cloud ၏ အကျိုးကျေးဇူးများကို အကောင်းဆုံး သဘောပေါက်နိုင်သည်။ ဤကန့်သတ်ထိန်းချုပ်မှုများသည် ထုတ်လုပ်မှုများပြားခြင်းကြောင့် ကုန်ကျစရိတ် သက်သာမှု (economies of scale) နှင့် ဝေမျှသုံးစွဲသည့် computing အခြေခံအဆောက်အအုံမှ ရရှိသော လုံခြုံရေး အကျိုးကျေးဇူးများကို လျော့ပါးစေသည်။ cloud အတွင်းရှိ အချက်အလက်များကို အသုံးပြုခြင်းသည် လုံခြုံရေး ထိန်းချုပ်မှုများပေါ်တွင် မူတည်သည်။ အစိုးရပိုင်

အချက်အလက်များကို နိုင်ငံကျော်၍ အသုံးပြုခြင်းနှင့် သက်ဆိုင်သည့် အေဂျင်စီများသည် သင့်လျော်သော လုံခြုံရေး စံနှုန်းထိန်းချုပ်မှုများရှိသည့် cloud vendor (cloud ရောင်းချသူ) များကို ရွေးချယ်သင့်ပါသည်။

လုံခြုံရေး မူဘောင်

စာချုပ်ချုပ်ဆိုထားသော cloud ဝန်ဆောင်မှုများအတွက် လုံခြုံရေး စီမံခန့်ခွဲခြင်းသည် စာချုပ်ချုပ်ဆိုသော အေဂျင်စီနှင့် cloud ဝန်ဆောင်မှုပေးသူ ကြားတွင် ခွဲဝေယူရမည့် တာဝန်ဖြစ်သည်။ စာချုပ်ချုပ်ဆိုထားသော အေဂျင်စီသည် cloud အတွင်းရှိ လုံခြုံရေး ထိန်းချုပ်မှုများကို သတ်မှတ်ရမည်ဖြစ်ပြီး၊ cloud ဝန်ဆောင်မှုပေးသူက cloud ၏ လုံခြုံရေးအတွက် တာဝန်ရှိသည်။
အချက်အလက်များ လုံခြုံရေးသည် - (၁) အချက်အလက် အမျိုးအစားခွဲခြားခြင်း အဆင့်တစ်ခုစီအတွက် လုံခြုံရေးလိုအပ်ချက်များကို ပြည့်မီခြင်း (၂) စံနှုန်းသတ်မှတ်ချက် tool များကို အသုံးပြုခြင်းနှင့် စာရင်းစစ်ခြင်းလုပ်ငန်းစဉ်များ ပေါ်တွင် မူတည်သည်။

commercial cloud ပေါ်သို့ ပြောင်းရွှေ့နိုင်သော အချက်အလက်များသည် တရားဝင် အသိအမှတ်ပြုမှုအတွက် လုံခြုံရေး လိုအပ်ချက်များကို ပြည့်မီရန်လိုအပ်ပြီး၊ နိုင်ငံတကာ cloud လုံခြုံရေး စံနှုန်းများအားဖြင့် အတည်ပြု စစ်ဆေးရန် လိုအပ်သည်။ လက်ခံပြီး နိုင်ငံတကာ လုံခြုံရေး စံနှုန်းများတွင် ISO 27001, ဝန်ဆောင်မှု အဖွဲ့အစည်း ထိန်းချုပ်မှုများ အစီရင်ခံစာ (SOC) ၁ နှင့် ၂၊ ငွေချေကဒ်လုပ်ငန်း အချက်အလက် လုံခြုံရေး စံနှုန်း (PCI DSS), Cloud လုံခြုံရေး အဖွဲ့အစည်း (CSA), အသိအမှတ်ပြုခြင်းနှင့် စာရင်းစစ်ခြင်း (သို့) ၎င်းတို့၏နောက်ပိုင်း ဆက်ခံသည့်အရာများ (successors) ပါဝင်သည်။ AES (128 bits and higher), TDES (minimum double-length keys), RSA (1024 bits or higher), ECC (160 bits or higher), and ElGamal (1024 bits or higher) (သို့) ၎င်းတို့၏နောက်ပိုင်း ဆက်ခံသည့်အရာများ (successors) ကဲ့သို့ လုပ်ငန်း စမ်းသပ်ခြင်းနှင့် လက်ခံခြင်း စံနှုန်းများ (industry-tested and accepted standards) နှင့် လုပ်ဆောင်ရန် နည်းလမ်းများ (algorithms) ကို အသုံးပြုပြီး အချက်အလက်များကို ကုဒ်အဖြစ် ပြောင်းလဲလိမ့်မည်။

Commercial cloud ဝန်ဆောင်မှု ပေးသူသည် ညွှန်ကြားထားသော လုံခြုံရေးနှင့် ကိုယ်ရေးကိုယ်တာ လိုအပ်ချက်များကို ပြည့်မီကြောင်း သေချာစေရန်၊ အချက်အလက်များ အသုံးပြုခြင်းအတွက် စာရင်းစစ်မှတ်တမ်းများ (logs and audit trails) အပါအဝင် logical လုံခြုံရေး စာရင်းစစ်ခြင်း ပြုလုပ်ပေးရမည်။

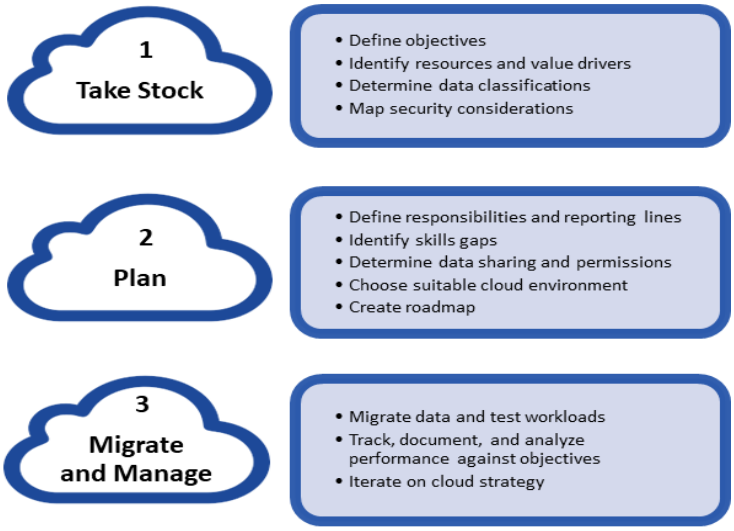
အစိုးရဌာနဆိုင်ရာများအနေဖြင့် cloud ဝန်ဆောင်မှုများသည် သဘောတူသတ်မှတ်ထားသော အချက်အလက်များ လုံခြုံစိတ်ချရခြင်းနှင့် မှန်ကန်မှုရှိခြင်း စသည့်အချက်များ ပြည့်မီကြောင်း၊ အချက်အလက်များ အခွင့်မရှိဘဲ ခိုးယူသုံးစွဲခံရခြင်း (data breaches) မရှိကြောင်းနှင့် အချက်အလက်များနှင့် အလုပ်များ အဆက်မပြတ် အသင့်ရှိနေကြောင်း သေချာစေရန် logical စာရင်းစစ်ခြင်းနှင့် အဆက်မပြတ် လုံခြုံရေး ကြည့်ရှုစစ်ဆေးမှုများပေါ်တွင် ယုံကြည်စိတ်ချမှု ရှိသင့်သည်။

နောက်ထပ် အသေးစိတ်အချက်အလက်များအတွက် အေဂျင်စီများသည် အချက်အလက် အမျိုးအစားခွဲခြားခြင်း မူဘောင်များကို ကိုးကားသင့်ပါသည်။

အခန်း (၄) : နေရာရွှေ့ပြောင်းခြင်း မူဝါဒ

အချက်အလက်များနှင့် အလုပ်တာဝန်များကို cloud သို့ ရွှေ့ပြောင်းခြင်းသည်ဝန်ဆောင်မှုများကို အသုံးချနိုင်မှုနှင့် လုပ်ငန်းလည်ပတ်လုပ်ဆောင်နိုင်မှုတို့ကို မြှင့်တင်ပေးပြီး ဌာနတွင်းလုပ်ငန်းလည်ပတ်နိုင်စွမ်းကို တိုးတက်ကောင်းမွန်စေသည်။ Cloud သို့ နေရာရွှေ့ပြောင်းခြင်းသည် အမျိုးမျိုးသော လုပ်ငန်းဆောင်ရွက်ရေး လိုအပ်ချက်များရှိသည့် လုပ်ငန်းဖြစ်စဉ်များအတွက် ကွန်ပြူတာရင်းမြစ်များ၏ အသုံးပြုနိုင်မှုနှင့် လျှင်မြန်မှုတို့ကို မြှင့်တင်ကာ အချို့သော လုပ်ငန်းဖြစ်စဉ်များ၏ အလိုအလျောက် ဆောင်ရွက်မှုတို့ကိုလည်း ပိုမိုလုပ်ဆောင်နိုင်စေသည်။

နေရာရွှေ့ပြောင်းခြင်းကို အဆင့်သုံးဆင့်ပါသော လုပ်ငန်းစဉ်အနေဖြင့် ရှုမြင်နိုင်သည်။ (၁) အချက်အလက်များကို ရယူပါ (၂) ကြိုတင်ပြင်ဆင်ပါ (၃) နေရာရွှေ့ပြောင်းခြင်းနှင့် စီမံခန့်ခွဲမှုကို ပြုပါ။



(၁) အချက်အလက်များကို ရယူပါ

IT ရင်းမြစ်များကို ဦးတည်ချက်များနှင့် ကိုက်ညီစေရန် မည်သို့ ပြုလုပ်ထားကြောင်းနှင့် ကုန်ကျစားရိတ်များကို မည်သို့ အကျိုးအရှိဆုံးဖြစ်အောင်အသုံးပြုမည်ကို ခွဲခြားဖော်ထုတ်ပါ။ သက်ဆိုင်ရာကိစ္စ၏ ဒေတာအချက်အလက် အမျိုးအစားများနှင့် သက်ဆိုင်ရာ လုံခြုံရေးကိစ္စများ၊ အချက်အလက်လုံခြုံမှု၊ အရည်အသွေးပကတိအတိုင်းတည်ရှိမှု နှင့် အသုံးပြုနိုင်မှုတို့နှင့် သက်ဆိုင်မှုရှိသော အန္တရာယ်များအထိပါဝင်သော အချက်အလက်များကို ရယူပါ။ ထိရှလွယ်မှုမရှိသော အလုပ်ကိစ္စများနှင့် လုံခြုံရေးပိုင်း စိုးရိမ်ဖွယ်ရာ သိပ်မရှိသည့် အရာများကို ပထမဆုံးနေရာရွှေ့ပြောင်းရေးအတွက် ဦးစားပေးသင့်သည်။ အစိုးရဂက်ဘ်ဆိုက်များ၊အများပြည်သူဆိုင်ရာ သိုမှီးအချက်အလက်များ၊ တိုးတက်မှုနှင့် စမ်းသပ်နေသော ပတ်ဂန်းကျင်များသည် cloud သို့ ရွှေ့ပြောင်းရန် ပို၍ အဆင်သင့်ဖြစ်သည်။

Cloud သို့ အလုပ်ကိစ္စများရွှေ့ပြောင်းခြင်း၏တန်ဖိုးကို နည်းပညာ သက်တမ်းစက်ဝန်းနှင့် cloud ကြောင့် တိုးတက်လာသော လုပ်ငန်းလည်ပတ်ဆောင်ရွက်နိုင်စွမ်းဖြင့် ဆုံးဖြတ်သည်။

လက်ရှိနည်းပညာသက်တမ်းစက်ဝန်း ကုန်ဆုံးရန် နီးကပ်နေသော IT ရင်းမြစ်များမှ အလုပ်ကိစ္စများရွှေ့ပြောင်းခြင်းသည် အရင်းအနှီးကြီးသော IT ရင်းမြစ်အသစ်များတွင် ရင်းနှီးမြှုပ်နှံရခြင်းကို ရှောင်ရှားနိုင်သည်။

၂) ကြိုတင်ပြင်ဆင်ပါ

တာဂန်များနှင့် အစီရင်ခံသတင်းပို့ခြင်းအဆင့်ဆင့်တို့အား ဖွင့်ဆိုသတ်မှတ်ခြင်း အပါအဝင် cloud သို့ ရွှေ့ပြောင်းဝန်ဆောင်မှုအတွက် လမ်းပြမြေပုံတစ်ခုကို ရေးဆွဲပါ။ Cloud သို့ အလုပ်ကိစ္စများရွှေ့ပြောင်းခြင်းသည် အဖွဲ့အစည်းအတွင်း လိုအပ်သော ကျွမ်းကျင်မှုများကို ပြောင်းလဲစေနိုင်သည်။ ဥပမာအားဖြင့် developers နှင့် အင်ဂျင်နီယာများ ပိုမိုလိုအပ်လာခြင်း၊ IT အခြေခံအဆောက်အဦးကို စီမံခန့်ခွဲခြင်းအတွက် လိုအပ်သောလူ ပိုမိုနည်းပါးလာခြင်း။ ထို့ကြောင့် cloud providers များနှင့် အလုပ်လုပ်ပါက အလုပ်ကိစ္စများ နေရာရွှေ့ပြောင်းဆဲနှင့် နေရာရွှေ့ပြောင်းပြီးကာလတွင် လိုအပ်သော ဂန်ထမ်းကျွမ်းကျင်မှုများ၊ လေ့ကျင့်သင်ကြားမှုများနှင့် ပညာရေးတို့ကို နားလည်ရန်လိုအပ်သည်ဟု အဓိပ္ပါယ်ရသည်။

- မျှဝေနိုင်သော ဒေတာအချက်အလက်များနှင့် မျှဝေသုံးစွဲခြင်းကြောင့် အကျိုးအမြတ်ရရှိလာနိုင်သော ဒေတာအချက်အလက်များကို ဖော်ထုတ်ပါ။ ထို့နောက် ထိုကဲ့သို့သော ဒေတာအချက်အလက်များအတွက် လုံခြုံရေးနှင့် အသုံးပြုရယူနိုင်ရန်အတွက် လိုအပ်သောခွင့်ပြုချက်များကို သတ်မှတ်ပါ။
- ခေတ်နောက်ကျနေပြီဖြစ်သော IT ပစ္စည်းများကို virtual သက္ကာန်ပြောင်းလဲခြင်း၊ ခေတ်နောက်ကျနေသောIT ပစ္စည်းတို့၏ စွမ်းဆောင်ရည်၊ လုပ်ငန်းဆောင်ရွက်နိုင်ရန်လိုအပ်ချက်များ၊ကုန်ကျစားရိတ်များနှင့် ကိုက်ညီမှုများကဲ့သို့သော သင့်လျော်မှုရှိသော cloud ပတ်ဂန်းကျင်တစ်ခုကို သတ်မှတ်ပါ။
- ရှိရင်းစွဲ applications များကို အသစ်များဖြင့် အစားထိုးမည်လော သို့မဟုတ် အောက်ခြေမှ အထက်သို့ ဂန်ဆောင်မှုအဆင့်ဆင့်ပေးပို့သော စနစ်ပုံစံကို ပြန်လည်ရေးဆွဲရန် ပိုမိုလိုလားသလောဆိုသည်ကို ဆုံးဖြတ်ပါ။

အသုံးပြုရန်ရွေးချယ်ထားသော cloud ဂန်ဆောင်မှုများသည် လက်ရှိဂန်ဆောင်မှုများနှင့် ပေါင်းစည်းနိုင်ရမည်ဖြစ်ပြီး ပြည်တွင်းဖြစ် IT နည်းပညာနှင့် အပြန်အလှန်ပြောင်းလဲ အသုံးပြုနိုင်ရမည်ဖြစ်သည်။ ယင်းတို့အား ကြိုတင်ပြင်ဆင်ထားသော ဒေတာအချက်အလက်နှင့် အလုပ်ကိစ္စနေရာပြောင်းရွှေ့ရန် လိုအပ်ချက်များနှင့် ကိုက်ညီမှုရှိရန် တစ်စုတည်းပေါင်းပြီး အသုံးပြုရန်သဘောတူညီရွေးချယ်ရမည်ဖြစ်သည်။

၃) နေရာချွေ့ပြောင်းခြင်းနှင့် စီမံခန့်ခွဲခြင်း

ကြီးတင်ပြင်ဆင်မှု၏ အခြေအနေတိုးတက်မှုအား မည်သည့်အဆင့်ရောက်နေကြောင်း ဆန်းစစ်မှု၊ မှတ်တမ်းတင်မှုနှင့် သုံးသပ်လေ့လာမှုတို့ကို ရှိရင်းစွဲအချက်အလက်များအပေါ် တဖြည်းဖြည်း ထပ်တိုးဖြည့်ခြင်းနှင့် ပုံသေလုပ်နည်းအတိုင်း ထပ်ကာထပ်ကာလုပ်သောပုံစံဖြင့်လုပ်ပါ။

ရည်ရွယ်ချက်များနှင့် စွမ်းဆောင်မှုများ၊ ဂန်ဆောင်မှု ပေးနိုင်စွမ်းများကို နှိုင်းယှဉ်ကာ စောင့်ကြည့်လေ့လာပါ။ ထို့နောက်နေရာချွေ့ပြောင်းရေးအစီအစဉ်နှင့် ကုန်ကျမည့် ကုန်ကျစားရိတ်များကို ချိန်ထိုးနှိုင်းယှဉ်ပါ။

ဖော်ပြပါ နေရာချွေ့ပြောင်းခြင်း၊cloud ပတ်ဂန်းကျင်အား လုပ်သင့်လုပ်ထိုက်သည့်အတိုင်း ဆောင်ရွက်သော စမ်းသပ်မှုများသည် ရှိရင်းစွဲ နည်းပညာများကို မပယ်ဖျက်ခင် လုပ်ထားရမည်။ စမ်းသပ်ရာတွင် လုပ်ရိုးလုပ်စဉ်ဖြစ်သော/ပုံမှန်ဖြစ်သော အသုံးပြုမှု အခြေအနေများနှင့် သာမာန်ထက်လွန်ကဲသည့် အသုံးပြုမှု/လိုအပ်သော အခြေအနေများ နှစ်ခုစလုံးတွင် စမ်းသပ်ထားရမည်။

cloud ရောင်းချသူများအား ဂန်ဆောင်မှုအဆင့် သဘောတူညီမှုများ(SLAs) မှ တဆင့် cloud ဝန်ဆောင်မှုများကို အသုံးပြုရန် သဘောတူညီမှုရယူခြင်း၊ စီမံခန့်ခွဲခြင်းနှင့် ချွေ့ပြောင်းလိုက်သော အလုပ်ကိစ္စများကို စီမံခန့်ခွဲရန် လိုအပ်သော အရည်အချင်းများ ရှိနေစေရန် ဝန်ထမ်းများအား သင်ကြားပေးထားပါ။

အခန်း (၅) : ဒေတာအချက်အလက်ပိုင်ဆိုင်မှု၊ အချက်အလက်ပြန်လည်ထုတ်ယူခြင်းနှင့် ဌာနတွင်းလုပ်ငန်းလည်ပတ်နိုင်စွမ်း

ဒေတာအချက်အလက် ပိုင်ဆိုင်မှု

အစိုးအဖွဲ့အစည်းများသည် ယင်းတို့၏ ဒေတာအချက်အလက်များကို အပြည့်အဂဂထိန်းချုပ်ပိုင်ခွင့်နှင့် ပိုင်ဆိုင်ခွင့်ရှိသသည်။ အသုံးပြုသူတို့၏ နည်းပညာပစ္စည်းများနှင့် ဒေတာအချက်အလက်များအား ဝင်ရောက်အသုံးပြုနိုင်မှုကို ကန့်သတ်ထားနိုင်သော Cloud Service Provider ၏ ဝင်ရောက်အသုံးပြုသူနှင့် အသုံးပြုမှုကို ထိန်းချုပ်သောစနစ်ကို သုံးခြင်းဖြင့် ထိုသို့ဖြစ်နေစေရန် ဆောင်ရွက်ထားသည် CSP များသည် ၎င်းတို့၏ အသုံးပြုသူများကိုယင်းတို့၏ အချက်အလက်ကို မည်သို့သိမ်းဆည်းမည်၊စီမံခန့်ခွဲမည်၊ကာကွယ်မည် စသဖြင့် ရွေးချယ်ခွင့်အား ရေရှည်စာချုပ် သို့မဟုတ် သီးသန့်တစ်ဦးတည်းအား အသုံးပြုရမည်ဟူသော တောင်းဆိုချက်များ မထားဘဲ ပေးသင့်သည်။

အစိုးရကိုယ်စားလှယ်အဖွဲ့အစည်းများအတွက် cloud ဝန်ဆောင်မှုများကို ပေးခြင်းနှင့် သက်ဆိုင်သော ဝန်ဆောင်မှုစာချုပ်များနှင့် အခြား ဝန်ဆောင်မှုအဆင့်သဘောတူညီမှုများ(SLAs) တွင် cloud သို့ ရွှေ့ပြောင်းလိုက်သော မည်သည့် ဒေတာအချက်အလက်ကို မဆို မည်သူက ပိုင်ဆိုင်၊cloud ကို မည်သူကစီမံခန့်ခွဲ သို့မဟုတ် လည်ပတ်သည်ကို ထည့်သွင်းစဉ်းစားစရာမလိုပဲ စာချုပ်ချုပ်ဆိုထားသောအစိုးရ၏ ပိုင်ဆိုင်မှုအဖြစ်သာရှိနေမည့်အကြောင်း ရှင်းလင်းစွာဖော်ပြပေးသင့်သည်။ စာချုပ်ချုပ်ဆိုသော ဌာနသည် အတည်ပြုခြင်း၊ငြင်းပယ်ခြင်း၊ ပြင်ပလူအဖွဲ့အစည်းများမှ သုံးစွဲခွင့်များကို ပယ်ဖျက်ခြင်း စသည့်အခွင့်အရေးများနှင့် အချက်အလက်၏ ပထဝီတည်နေရာအနေအထားကို ခွဲခြမ်းထုတ်ဖော်ခွင့်တို့အပါအဝင်cloud ဝန်ဆောင်မှုများ၏ ရုပ်ပိုင်းဆိုင်ရာတည်နေရာကို ထည့်သွင်းမတွက်ချက်ပဲ အချက်အလက် ဝင်ရောက်ခွင့်၊ပြန်လည်ဆယ်ယူခွင့်၊အဆင့်မြှင့်တင်ခွင့်နှင့် ပယ်ဖျက်ခြင်းအခွင့်အရေးတို့ကို ရရှိရမည်ဖြစ်သည်။

ဝင်ရောက်အသုံးပြုခွင့်

အချက်အလက်အား ဝင်ရောက်၊ ပြန်လည်ဆယ်ယူ၊အဆင့်မြှင့်တင်ခြင်းနှင့် ဖျက်ခြင်းတို့သည် စာချုပ်ချုပ်ဆိုထားသော အစိုးရဌာန၏ ရပိုင်ခွင့် ဖြစ်ပြီး သက်ဆိုင်ရာ ဝန်ဆောင်မှုစာချုပ်များထဲတွင် ထိုအချက်များပါဝင်နေမည်ဖြစ်သည်။

ဒေတာအချက်အလက်များဝင်ရောက်အသုံးပြုနိုင်ခွင့်နှင့်ပက်သက်သော မူဝါဒများနှင့် သက်ဆိုင်သော လုပ်ငန်းစဉ်များကို စာချုပ်ချုပ်ဆိုထားသော အဖွဲ့အစည်း၏ လိုအပ်ချက်အတိုင်း ဖွင့်ဆိုသတ်မှတ်ပေးရမည် ဖြစ်ပြီး အစိုးရဌာနဆိုင်ရာနှင့် cloud provider တို့ကြားမှ သဘောတူညီချက်စာချုပ်တွင် အသေးစိတ်ဖေါ်ပြထားရမည်ဖြစ်သည်။

ဌာနတွင်း လည်ပတ်ဆောင်ရွက်နိုင်မှု

သုံးရိုးသုံးစည် IT ပစ္စည်းတို့နှင့် နှိုင်းယှဉ်လျှင် Cloud computing ၏ အဓိကကျသော အကျိုးကျေးဇူးသည် အသုံးပြုသူများအနေနှင့် ကြံ့တွေ့မြဲဖြစ်သော ရောင်းချသူတစ်ဦးတည်းကို မှီခိုရသော အခြေအနေမျိုးကို ရှောင်ရှားနိုင်ရန် မိမိစိတ်ကြိုက်ရွေးချယ်နိုင်ခွင့်ရှိခြင်းဖြစ်သည်။ CSPs များအနေဖြင့် အသုံးပြုသူများအား ယင်းတို့၏ cloud ပလက်ဖောင်းများကို လိုအပ်သလို ဒေတာအချက်အလက်များအား တင်ခြင်း၊

ဖြတ်ခြင်းများကို လုပ်ခွင့်ပြုရမည်။ အဆောက်အဦ သို့မဟုတ် နေရာတစ်ခုအတွင်းတပ်ဆင်အသုံးပြုသော ပစ္စည်းတို့ရှိ အစိတ်အပိုင်းများ၏ ချိတ်ဆက်လည်ပတ်နိုင်စွမ်းကိုISO/IEC 17203:2011 Open Virtualisation Format(OVF) တွင်း ဖော်ပြထားသော စွမ်းဆောင်ရည်များအတိုင်း နိုင်ငံတကာစံနှုန်းများအပေါ် အခြေခံပြီး တပ်ဆင်သင့်သည်။

Cloud system တစ်ခု၏ အစိတ်အပိုင်းများသည် အများပြည်သူနှင့် တစ်ဦးပိုင် cloud လုပ်ငန်းများ အပါအဝင် မတူညီသော ရင်းမြစ်များမှ လာခြင်းဖြစ်နိုင်သည်။ ယင်းအစိတ်အပိုင်းများသည် မတူညီသော ဖန်တီးသူတို့ထံမှ လာသော အမျိုးမျိုးသော သို့မဟုတ် အသစ်ဖြစ်သော အစိတ်အပိုင်းတို့နှင့် အစားထိုးနိုင်ရမည်ဖြစ်ပြီး ထိုသို့အစားထိုးပြီးပါက စနစ်တစ်ခုနှင့် တစ်ခုအကြား ဆက်လက်လည်ပတ်နိုင်စွမ်းနှင့် ဒေတာအချက်အလက်ဖလှယ်ခြင်း ဆက်လက်ဆောင်ရွက်နိုင်ရမည်။ CSPs များသည် အချိန်ကြာမြင့်သော ဝယ်ယူမှုနှင့် လုပ်ငန်းအကောင်အထည်ဖော်သည့် လုပ်ငန်းစက်ဝန်များကို ဖြတ်သန်းရန်မလိုဘဲ CSPs များကို အစိုးရဌာနဆိုင်ရာများမှ အလွယ်တကူ ပြောင်းလဲစေနိုင်ရန် မတူညီသောစနစ်များအကြား ချိတ်ဆက်အသုံးပြုနိုင်မှု ဆောင်ရွက်ပေးနိုင်ရမည်။

အခန်း (၆) : CSPs များအတွက် တရားဝင် အသိအမှတ်ပြုခြင်း လုပ်ငန်းစဉ်

တရားဝင်အသိအမှတ်ပြုခြင်း

CSPs များအတွက် တရားဝင် အသိအမှတ်ပြုခြင်းလုပ်ငန်းစဉ်ကို သတင်းအချက်အလက်နည်းပညာနှင့် ဆိုက်ဘာလုံခြုံရေးဌာန(ITCSD) မှ ဆောင်ရွက်ရမည်။ အသိအမှတ်ပြုရေးလုပ်ငန်းစဉ်တွင် အစိုးရ IT နည်းပညာဝယ်ယူမှု အများစုတို့အတွက် အခြေခံမရှိမဖြစ်လိုအပ်သော လိုအပ်ချက်များ ပါဝင်ရမည်ဖြစ်သောကြောင့် အသိအမှတ်ပြုထားသော CSP စာရင်းကိုလည်း ထည့်သွင်းထားရမည်ဖြစ်သည်။ ယင်းသည် CSPs များထံမှ အခြေခံအဆင့် ဂန်ဆောင်မှု ယုံကြည်စိတ်ချရနိုင်စေပြီး ၎င်းတို့အနေနှင့် အစိုးရဌာနဆိုင်ရာများအသုံးပြုနိုင်သော လိုအပ်သည့် လုံခြုံရေးဆိုင်ရာ လုပ်ငန်းဆောင်ရွက်ချက်များပေးနေသည့် လုံခြုံပြီး ထိန်းချုပ်မှုရှိသည့် နေရာတစ်ခုရှိကြောင်းကိုလည်း ခိုင်မာသေချာစေသည်။ အကောင်းဆုံးသော နိုင်ငံတကာလုပ်ထုံးလုပ်နည်းများမှ အသိအမှတ်ပြုခြင်း ကို နည်းလမ်းနှစ်နည်းဖြင့် လုပ်ဆောင်နိုင်ကြောင်းဖော်ပြထားသည်။ (၁) ပြည်တွင်းစံနှုန်းများဖြင့် ပြည်တွင်း

တရားဝင်အသိအမှတ်ပြုချက်၊ သို့မဟုတ်(၂) နိုင်ငံတကာ အသိအမှတ်ပြုလက်မှတ်များကို ရယူခြင်း။ ဌာနဆိုင်ရာများအနေနှင့် တရားဝင်အသိမှတ်ပြုသော CSP စာရင်းတွင် ပါသော ရောင်းချသူများကိုသာ ထည့်သွင်းစဉ်းစားရမည်။

အသိအမှတ်ပြုလက်မှတ်ထုတ်ပေးခြင်း၊ ကနဦးအဆင့်ကာတည်းက ရှိရန်လိုအပ်သော စံချိန်စံနှုန်းများနှင့် လုပ်ဆောင်ရမည့် လုပ်ငန်းစဉ်အဆင့်ဆင့်တို့အတွက် "အခြေခံအဆင့်ထပ်ပေါင်း" မူဘောင်ရှိရမည်

ဌာနဆိုင်ရာများသည် CSP တစ်ခုကို ၎င်းတို့၏ လုပ်ငန်းလိုအပ်ချက်နှင့် ကိုက်ညီသော အခြေခံလိုအပ်ချက်နှင့် ပြည့်မီကြောင်းထောက်ခံချက်များ၊ စံချိန်စံနှုန်းများ သို့မဟုတ် လုပ်ငန်းစဉ်အဆင့်ဆင့်လုပ်ဆောင်ပုံတို့ကို ကြည့်ပြီး ရွေးချယ်သင့်သည်။ ဌာနဆိုင်ရာအဖွဲ့အစည်းတစ်ခု၏ လိုအပ်သော လုပ်ငန်းလည်ပတ်ဆောင်ရွက်မှုနှင့် အခြေခံ အသိအမှတ်ပြုထောက်ခံချက် သို့မဟုတ် လိုအပ်သော လုပ်ငန်းစဉ်အဆင့်ဆင့်တို့နှင့် ကိုက်ညီသောဥပမာတစ်ချို့တွင် အောက်ပါတို့ပါဝင်သည်။

လုပ်ငန်းစဉ်းများ	**အခြေခံအသိအမှတ်ပြု လက်မှတ်နှင့်/သို့မဟုတ် လိုအပ်သော လုပ်ဆောင်ရသည့် လုပ်ငန်းစဉ်အဆင့်ဆင့်**
ထိန်းချုပ်မှုများ	လုပ်ငန်းစဉ်အဆင့်ဆင့် OAuth,Security Assertion Markup Language(SAML) ရွေးချယ်ရန် နည်းလမ်းများ ၎င်းဆောင်မှုအဖွဲ့အစည်းထိန်းချုပ်ရေး(Service Organisation Control-SOC) ၁ နှင့် ၂
သတင်းအချက်အလက်လုံခြုံရေး စီမံခန့်ခွဲမှု	ထောက်ခံချက် ISO/IEC 270001- သတင်းအချက်အလက်လုံခြုံရေး စီမံခန့်ခွဲမှု
ကိုယ်ပိုင် အချက်အလက်	(မြန်မာ နိုင်ငံသားများ၏ ကိုယ်ရေးကိုယ်တာနှင့် လုံခြုံရေး အကာအကွယ်ပေးခြင်းဥပဒေ) နှင့် ကိုက်ညီမှုရှိခြင်း ရွေးချယ်ရန် နည်းလမ်းများ ISO 27018 ထောက်ခံချက်

အီလက်ထရောနစ်ငွေပေးချေမှု (Electronic Payment)	ငွေပေးချေမှုကတ်လုပ်ငန်း (Payment Card Industry - PCI) ဒတာအချက်အလက်လုံခြုံရေးစံနှုန်း (Data Security Standard -DSS)

အခြေခံအသိအမှတ်ပြု ထောက်ခံချက်များနှင့် ပတ်သက်သော ထပ်မံသိရှိရန် လိုအပ်သော အချက်များနှင့် လိုအပ်သော လုပ်ငန်းစဉ်အဆင့်ဆင့်တို့ကို ITCSD မှ ပေးမည်ဖြစ်သည်။

နည်းပညာနှင့် ကဏ္ဍအလိုက် အသိအမှတ်ပြုထောက်ခံချက်များ

တရားဝင်အသိအမှတ်ပြုမှုစနစ်သည် အချို့သော ဌာနဆိုင်ရာများ၊ ကဏ္ဍများ သို့မဟုတ် အချို့သော ဒေတာအချက်အလက်အမျိုးအစားတို့၏ မျှော်မှန်းထားသော မြင့်မားသည့် လိုအပ်ချက်များကို အခြေခံကာ အခြေခံအသိအမှတ်ပြုထောက်ခံချက်ထဲတွင် ပါဝင်သောအရာများထက် ကျော်လွန်ပြီး ကျယ်ပြန့်သွားကောင်း သွားနိုင်သည်။ထို့အတွက်ကြောင့် အချို့သော လိုအပ်ချက် အဆင့်အတန်းတို့နှင့် ကိုက်ညီမှုရှိသော တရားဝင်အသိအမှတ်ပြု အဆင့်ဆင့်တို့ ပါဝင်ရမည်ဖြစ်သည်။

ဥပမာအားဖြင့် တစ်သီးပုဂ္ဂလအခန်းကဏ္ဍများအတွက် တိကျသော အသိအမှတ်ပြုလက်မှတ်များ လိုအပ်လိမ့်မည်။ အသိအမှတ်ပြုလက်မှတ်များအားလုံးသည် တည်ရှိဆဲ နိုင်ငံတကာလုပ်ငန်းစံနှုန်းများနှင့် အသိအမှတ်ပြုလက်မှတ်များပေါ် တွင်အခြေခံရန် အရေးကြီးသည်။ ယင်းတို့သည် အစိုးရဌာန၏ လိုအပ်ချက်များအပေါ် မူတည်၍ လိုအပ်သော အခြေခံ အသိအမှတ်ပြု လက်မှတ်များနှင့်အတူ နှစ်ဖက်လုံးအား ညီတူမျှတူချိန်ထိုး ထည့်သွင်းစဉ်းစားသင့်သည်။ ထင်သာမြင်သာသော ဥပမာများမှာ အမျိုးသားကာကွယ်ရေး သို့မဟုတ် အမျိုးသားသတင်းအချက်အလက်လုံခြုံရေး သို့မဟုတ် ကျန်းမာရေးသတင်းအချက်အလက်တို့ နှင့် သက်ဆိုင်သော ကိစ္စများဖြစ်သည်။[10]

အခန်း (၇) : အစိုးရဌာန၏ ဝယ်ယူရေး လုပ်ငန်းစဉ်

cloud computing ဝန်ဆောင်မှုများကို ဝယ်ယူခြင်းသည် အစိုးရအဖွဲ့အစည်းတစ်လျှောက် ရိုးရှင်း၍ ရှေ့နောက်ညီညွတ်မှုရှိရမည်ဖြစ်ပြီး အစိုးရဌာနဆိုင်ရာများအတွက် အတတ်နိုင်ဆုံး

[10] အမေရိကတွင် အစိုးရ သို့မဟုတ် ပုဂ္ဂလိက အခန်းကဏ္ဍမှ ထိန်းချုပ်ထားသောကျန်းမာရေး သတင်းအချက်အလက်များ အားလုံးသည် ကျန်းမာရေးအာမခံလွယ်ကူအဆင်ပြေမှုနှင့် တာဝန်ခံမှု အက်ဥပဒေ(HIPAA) နှင့် စီးပွားရေးနှင့် ပုဂ္ဂလိက ဆေးရုံဆိုင်ရာကျန်းမာရေးအတွက် သတင်းအချက်အလက် နည်းပညာ (HITECH) ဟူသော အမေရိကန်ဥပဒေနှစ်ရပ်၏ အချက်အလက်ကာကွယ်ရေး ပြဋ္ဌာန်းချက်များ၏ လက်အောက်တွင်ရှိသည်။ HIPAA နှင့် HITECH တို့၏ စည်းကမ်းချက်များနှင့် ကိုက်ညီမှုရှိကြောင်း CSP များအား အသိအမှတ်ပြုသည့် မှ cloud ဝန်ဆောင်မှုများအတွက် လုပ်ငန်းဆိုင်ရာ အသိအမှတ်ပြုထောက်ခံချက်များလည်းရှိသည်။

စွမ်းဆောင်ရည်မြင့်ရန်မှာ cloud ပထမမူဝါဒ အောင်မြင်ရေးအတွက် အလွန်အရေးပါလှသည်။ Cloud ဝန်ဆောင်မှုများကို ရယူအသုံးပြုခြင်းနှင့် ငွေပေးချေမှုတို့ လည်ပတ်လုပ်ဆောင်ရန်အတွက် အသုံးပြုမှုနမူနာပုံစံ မည်သို့ရှိသည်ကို ရိုးရှင်းစွာ ပြသနိုင်ရန်နည်းလမ်းတစ်ခုကိုလည်း စာရင်းသွင်းသင့်သည်။

ဈေးကွက်တစ်ခု- သို့မဟုတ် အစိုးရကိုယ်စားလှယ်အဖွဲ့ဝင်များအားလုံး အသုံးပြုနိုင်သော အများသုံးအွန်လိုင်းပလက်ဖောင်း- cloud ရယူသုံးစွဲခြင်း ဖြစ်စဉ်ကို ရိုးရှင်းအောင် လုပ်ဆောင်ခြင်း။ ဗဟိုချက်ကျသော အွန်လိုင်း-ရယူသုံးစွဲခြင်းမိုဒယ်ကို သေချာစေသည်-

1. ရောင်းချသူများက သမားရိုးကျတရားဝင်အသိအမှတ်ပြုလိုအပ်ချက်များကို လိုက်နာသည်။
2. အစိုးရကိုယ်စားလှယ်အဖွဲ့အစည်းများကို ပုံစံတူသော ဝန်ဆောင်မှုများအကြားရွေးချယ်ရာတွင် ကုန်ကျစားရိတ်နှင့် တရားဝင်အသိအမှတ်ပြုခြင်းတို့တွင် တိုးပွားလာသော ပွင့်လင်းမြင်သာမှု။ ထို့အပြင်
3. ဈေးကွက်တစ်ခုလုံး အကဲဖြတ်ဆန်းစစ်ရန်အတွက် လိုအပ်ချက်ကို ရှောင်ရှားခြင်းဖြင့် ကုန်ကျစားရိတ်များသက်သာစေခြင်း။

အစိုးရကိုယ်စားလှယ်အဖွဲ့များနှင့် ဆွေးနွေးတိုင်ပင်ခြင်းတွင် အစိုးရက တစ်နေရာထဲ အပြီးအစီးဈေးကွက်နေရာကို တည်ထောင်ခြင်း၊ ထိုထဲတွင် လူစွမ်းအားအရင်းမြစ်အဖွဲ့မှ သေချာစီစစ်ထားသော ဈေးရောင်းသူများနှင့် ဝန်ဆောင်မှုများ၏ ကျယ်ပြန့်သော ပမာဏအပါအဝင်ဖြစ်သည်။ ယခုဈေးကွက်ချဉ်းကပ်မှုသည် လုံခြုံရေးမျှော်လင့်ချက်များနှင့် ရယူသုံးစွဲခြင်းစိန်ခေါ်မှုများနှင့်တိကျသောအခန်းကဏ္ဍတစ်စုတစ်စည်းထဲဖြစ်သော အသိအမှတ်ပြုမှုများအားတစ်စုတစ်စည်းထဲဖြစ်အောင် ထည့်သွင်းစဉ်းစားရမည်ဖြစ်သည်။

အများပြည်သူဆိုင်ရာအခန်းကဏ္ဍအတွက် Cloud ဝယ်ယူမှုများတည်ဆောက်ခြင်း။

cloud ကို တိုက်ရိုက် သို့မဟုတ် တစ်ဆင့်ခံ ဝယ်ယူခြင်းကို ကိုယ်စားလှယ်အဖွဲ့များမှတစ်ဆင့် လုပ်ဆောင်နိုင်သည်။

- စီးပွားရေးအရ ရရှိနိုင်သော ဂန်ဆောင်မှုများအတွက် ဒီဇိုင်းရေးဆွဲထားသော CSPs များထံမှတိုက်ရိုက်ဂယ်ယူခြင်း၊ အလုပ်သမားအချိန်မပါပဲ စီးပွားရေးဂန်ဆောင်မှုတစ်ခုဂယ်ယူခြင်း ဖြစ်သည်။
- CSPs လုပ်ဖော်ကိုင်ဖက် သို့မဟုတ် ပြန်လည်ရောင်းချသူထံမှ တစ်ဆင့်ခံ ပြန်လည်ဂယ်ယူခြင်း၊အဆိုပါ အဖွဲ့အစည်းနှင့် သဘောတူညီမှုအတွက် ညှိနှိုင်းဆွေးနွေးခြင်း။

cloud ဂန်ဆောင်မှုများဂယ်ယူခြင်းအတွက် နည်းလမ်းလေးသွယ်ရှိပါသည်။

၁)တရားဂင်အသိအမှတ်ပြုခံထားရသော cloud ရောင်းချသူများနှင့် ဂန်ဆောင်မှုများစာရင်းမှ ဂယ်ယူခြင်း။
ယခုဂယ်ယူမှုသည် တိုက်ရိုက် သို့မဟုတ် တစ်ဆင့်ခံ ဂယ်ယူမှု ဖြစ်နိုင်ပါသည်။ တရားဂင်အသိအမှတ်ပြုခံထားရသော cloud ရောင်းချသူများနှင့် ဂန်ဆောင်မှုများစာရင်းသည် ITCSD မှ ပြုစုထားသော အနည်းဆုံးလိုအပ်ချက်များနှင့် ကိုက်ညီသည်။ဥပမာအားဖြင့် အများပြည်သူနှင့် သက်ဆိုင်သော အခန်းကဏ္ဍတွင် cloud ကို စတင်အသုံးပြုခြင်းအတွက် လွယ်ကူချောမောစေရန်၊အရှိန်မြန်စေရန်အတွက် အခြားနေရာများတွင်လည်း လုပ်ဆောင်နိုင်စေမည့် ချဉ်းကပ်ခြင်းများနှင့် ဆင်တူသည်။

- အစိုးရတစ်ရပ်လုံးအတွက် ဩစတြေးလျ တရားဂင်အသိအမှတ်ပြုထားသော cloud ဂန်ဆောင်မှုများစာရင်း(WoG) ရယူသုံးစွဲခြင်းစာချုပ်များ၊စီစဉ်ခြင်းများနှင့် အစပြုခြင်းများ- cloud services panel[11]
- စင်ကာပူ MTCS လုံခြုံရေးစံနှုန်းအောက် အများပြည်သူများကို ဂန်ဆောင်မှုပေးနေသော CSP တစ်ခုခုကို စင်ကာပူက လိုအပ်သည်။[12]
- ဗြိတိန်၏ အစိုးရ cloud စျေးကွက်သည် အများပြည်သူဂန်ဆောင်မှုပေးသူများအဖြစ် စာရင်းသွင်းမခံရမီတွင် ယင်းတို့၏ဒစ်ဂျစ်တယ်စျေးကွက်အခြေခံမူဘောင်[13]အောက်တွင် အရည်အချင်းပြည့်မီမှုနှင့် အဆင့်အတန်းပြည့်ဂမှုကို လျှောက်ထားရန် ဒစ်ဂျစ်တယ်ရောင်းချသူများအားလုံးက လုပ်ဆောင်ရန် လိုအပ်သည်။

[11] http://www.finance.gov.au/policy-guides-procurement/cloud-services-panel/
[12] Singapore Infocomm Development Authority (IDA)၊ ၁၃ နိုဂင်ဘာ ၂၀၁၃။ အဖွဲ့ပေါင်းစုံပါဂင်သော cloud လုံခြုံရေး အသစ်(MTCS) စံနှုန်းများကို စင်ကာပူတွင် စတင်ခဲ့သည်။ https://www.ida.gov.sg/About-Us/Newsroom/Media-Releases/2013/New-Multi-Tier-Cloud-Security-MTCS-Standard-Launched-In-Singapore
[13] ဗြိတိန်,n.d.,ဒစ်ဂျစ်တယ်စျေးကွက်နေရာ https://www.digitalmarketplace.service.gov.uk

၂) တည်ရှိဆဲ ရောင်းချသူ စာချုပ်ကို အရှိန်အဝါရှိစေမှု(တစ်ဆင့်ခံ ဂယ်ယူမှု)

အစိုးရကိုယ်စားလှယ်အဖွဲ့များသည် အခြားသော ကိုယ်စားလှယ်အဖွဲ့နှင့် ညှိနှိုင်းပြီးနှင့်ဖြစ်သော သဘောတူစာချုပ်ကို 'မျဉ်း'ကြသည်။ ကိုယ်စားလှယ်အဖွဲ့များသည် အသုံးပြုနိုင်ပါက အဆိုပါတည်ရှိဆဲ သဘောတူညီမှုများကို ဖော်ထုတ်ခွင့်ရှိသည်။

CSP တစ်ဆင့်ခံပြန်လည်ရောင်းချသူမှ ဂယ်ယူခြင်း(တစ်ဆင့်ခံဂယ်ယူခြင်း)

အစိုးရကိုယ်စားလှယ်များသည် CSPs တစ်ဆင့်ခံ ပြန်လည်ရောင်းချသူများ သို့မဟုတ် ပူးပေါင်းဆောင်ရွက်သူထံမှာ တိုက်ရိုက်ဂယ်ယူသည်။ အစိုးရကိုယ်စားလှယ်အဖွဲ့များသည် CSP ထံမှ တိုက်ရိုက် ဂယ်ယူလေ့မရှိပါ။ ယင်းသည် CSP တစ်ဆင့်ခံပြန်လည်ရောင်းချသူထံမှ ဖြည့်ဆည်းပေးသော စုဝေးထုပ်ပိုးထားသောဂန်ဆောင်မှု သို့မဟုတ် ဂန်ဆောင်မှုများကြောင့် ဂယ်ယူရန်ဆန္ဒရှိခြင်းဖြစ်နိုင်သည်။

၄) ရည်ညွှန်းစကားစုများကို ထုတ်ပေးခြင်း(TOR) သို့မဟုတ် အဆိုပြုချက် တောင်းဆိုခြင်း(RFP) (တစ်ဆင့်ခံဂယ်ယူမှု)

အလွယ်တကူအသုံးပြု၍ရအောင်ဖန်တီးထားသောအဖြေရှာမှုများသို့မဟုတ် နှစ်ဖက်အဖွဲ့အစည်းကြားဆက်သွယ်ရန်ငစေရေးကို ချက်ချင်းရန်ငစေရေးအတွက် အစဉ်အလာရယူသုံးစွဲနိုင်ရေးချဉ်းကပ်မှု၊ ကိုယ်စားလှယ်အဖွဲ့များသည် ရည်ညွှန်းစကားစုများ သို့မဟုတ် စျေးပြိုင်ကမ်းလှမ်းခြင်းများမှတစ်ဆင့် ယင်းတို့၏ လိုအပ်ချက်များကို စာရင်းပြုစုနိုင်ပြီး CSPs များကို ရရှိနိုင်သကဲ့သို့ ဂယ်ယူမှုအတွက် အဖြေများကို systems ပူးပေါင်းဆောင်ရွက်သူများ၏ အဖြေများကို လည်းရရှိနိုင်သည်။

အခြေခံအဆောက်အဦတည်ဆောက်ခြင်း vs ဂင်ရောက်သုံးစွဲခွင့်ငှားရမ်းခြင်း အသုံးဂင်မှုအခြေပြု စျေးနှုန်းသတ်မှတ်ခြင်း မိုဒယ်ပုံစံများ

Cloud computing သည် အရင်းအနှီးကုန်ကျစားရိတ်(CapEx) ထက် လုပ်ငန်းလည်ပတ်ကုန်ကျစားရိတ်(OpEx) အဖြစ် IT ဂန်ဆောင်မှုများ၏အကျိုးအမြတ်ကို ယူဆောင်လာပေးသည်။ အရင်းအနှီးကုန်ကျစားရိတ်သည် အချိန်နှင့်အမျှ တန်ဖိုးကျဆင်းနေစဉ်မှာ cloud အခြေပြု OpEx ဘတ်ဂျတ်သည်သည် ပိုမိုး၍ များစွာအားကောင်းသော၊ပြုလွယ်ပြင်လွယ်ရှိသော ဘတ်ဂျတ် ထိန်းသိမ်းမှုကို ခွင့်ပြုကာ နစ်မြုပ်နေသော ကုန်ကျစားရိတ်များကို ဖယ်ရှားပေးသည်။

CSPs များကို ရွေးချယ်ရာတွင် ကိုယ်စားလှယ်အဖွဲ့အစည်းများအတွက် အစိတ်အပိုင်းလေးရပ်မှာ အဓိကကျသည်။ (၁) ဈေးနှုန်းသတ်မှတ်ရာတွင် ပွင့်လင်းမြင်သာမှုရှိခြင်း၊(၂)မတူညီသော ဝန်ဆောင်မှုများအတွက် အမျိုးမျိုးသော ဈေးနှုန်းများ၊ (၃)ကိုယ်စားလှယ်အဖွဲ့များကို ယင်းတို့အဖွဲ့၏ လိုအပ်ချက်များနှင့် နှိုင်းယှဉ်၍ CSPအကဲဖြတ်ဆန်းစစ်ရန်ခွင့်ပြုသော အမျိုးမျိုးသော ဈေးနှုန်းသတ်မှတ်ခြင်းမိုဒယ်များကို ခွင့်ပြုခြင်း၊နှင့် (၄) တစ်ခါသုံးတစ်ခါပေး အသုံးပြုမှု မိုဒယ်ပုံစံ။

CSP ဈေးနှုန်းသတ်မှတ်ခြင်းမိုဒယ်ပုံစံသည် ကြိုက်သလောက်သုံး၊ကျသလောက်ပေး မိုဒယ်ပုံစံ ဖြစ်သင့်သည်။ ဝန်ဆောင်မှုများအတွက် အနည်းဆုံးကုန်ကျစားရိတ်နှင့် သီးခြားအမျိုးအမည်များကဲ့သို့ စာရင်းရှိသော ထပ်ဆောင်းရင်းမြစ်များအသုံးပြုမှုအတွက်လည်း ဈေးနှုန်းသက်သာသင့်သည်။ CSPs များသည် ဖောက်သည်များကို ယင်းတို့၏ဈေးနှုန်းသတ်မှတ်မှုများ အကဲဖြတ်နိုင်စေရန် ပွင့်လင်းမြင်သာမှု၊အများပြည်သူအသုံးပြုနိုင်မှု၊ပေါက်ဈေးသတ်မှတ်မှု၊ကိရိယာတန်ဆာပလာများကို ဖြည့်ဆည်းပေးသင့်သည်။ ယင်းတို့သည် လိုအပ်ချက်များနှင့်ကိုက်ညီမှုရှိရန်အတွက် အသုံးပြုမှုအတွက် ကုန်ကျစားရိတ်ပေးဆောင်ခြင်းအစီရင်ခံစာ(လိုင်း-အမျိုးအစား စက်ချုတ်ယွင်းမှုနှင့်အတူ) အသေးစိတ်ထုတ်လုပ်နိုင်ရန် ကိရိယာတန်ဆာပလာများနှင့်အတူ ဖောက်သည်များကို ဖြည့်ဆည်းပေးသင့်သည် အသုံးချအခြေပြု ချဉ်းကပ်ချက်အတွက် တစ်လိုင်းထဲအမျိုးအစားအဆောက်အဦအတွက် ဈေးနှုန်းသတ်မှတ်ခြင်းနမူနာမှာ အောက်ပါအတိုင်းဖြစ်သည်။

အမျိုးအစား နံပါတ်	**ပေးပို့ခြင်းများ/ဝန်ဆောင်မှုများ**	**ပမာဏ**	**ယူနစ်**	**ယူနစ်ဈေးနှုန်း**	**ပမာဏ**
၁၀၀၁	CSP Cloud ဝန်ဆောင်မှုများ	၁,၀၀၀	တစ်ခုချင်းစီ	အမေရိကန်ဒေါ်လာ ၁.၀၀	အမေရိကန်ဒေါ်လာ ၁၀၀၀

အချက်အလက်ခွဲခြားဖော်ပြခြင်း အခြေခံမူဘောင်

နိဒါန်း

ပြည်ထောင်စုမြန်မာနိုင်ငံတော် အစိုးရသည် ထိရောက်မှုမြင့်တက်ရန်၊လုပ်ငန်းဆောင်ရွက်မှုများ ကို ခေတ်မီစေရန်နှင့် ပြည်သူများသို့ ခေတ်မီဆန်းသစ်သော ဝန်ဆောင်မှုများပေးအပ်ရန်အတွက် ICTs နည်းပညာများကို အကောင်အထည်ဖော်ရန် လမ်းခုလတ်ပေါ်တွင် ရှိနေပြီဖြစ်သည်။ ယခုစပ်ဆက်အခြေအနေအရ၊ cloud အခြေပြု ဝန်ဆောင်မှုများ၏ ထူးခြားလှသော ဂုဏ်သတ္တိများအတွက် ကျယ်ပြန့်လှသေ အသိအမှတ်ပြုမှုများတွင် စီးပွားရေးတစ်ခု သို့မဟုတ် စနစ်တစ်ခုကို ကြီးထွားတိုးတက်လာအောင် လုပ်နိုင်စွမ်း၊သေးနိုင်ကျုံ့နိုင်အောင်လုပ်နိုင်စွမ်း၊ကုန်ကျစားရိတ် စီမံခန့်ခွဲမှု(အသုံးပြုသောအခါတွင်မှ အသုံးပြုမှုအတွက် ပေးချေရခြင်း)နှင့် မကြာခဏဆိုသလို အကောင်းဆုံး ရွေးချယ်စရာများပေးသော လုံခြုံရေးအမြင့်စားများကို ပေးအပ်ခြင်းတို့ပါဝင်သည်။ အလားတူစွာပင်၊လိုအပ်နေသော လုပ်ငန်းဆောင်ရွက်မှုနှင့်သိုလှောင်မှုအတွက်အချက်အလက် ဆတိုးပွားများနေခြင်းပမာဏ၊အရှိန်အဟုန်မြင့်လာနေသော ဆိုက်ဘာခြိမ်းခြောက်မှုများ၊ ကုန်ကျစားရိတ်များလျော့ချရန်နှင့် စွမ်းဆောင်ရည်များမြင့်တက်စေရန် တွန်းအားများ၊ပြည်သူတို့၏လိုအပ်ချက်များကို နည်းလမ်းသစ်များဖြင့် ဖြည့်ဆည်းပေးလိုသော အစိုးရ၏ ဆန္ဒများ အစရှိသဖြင့် အစိုးရတစ်ရပ်အနေဖြင့် ရင်ဆိုင်နေရသော စိန်ခေါ်မှုများကို cloud ဝန်ဆောင်မှုများက ပြုလွယ်ပြင်လွယ်သောအဖြေများနှင့် အတူ ကူညီပေးနိုင်မည်ဖြစ်သည်။

cloud computing၊ မိုဘိုင်းကိရိယာများ၊data analytics နှင့် ဉာဏ်ပညာအတု(artificial intelligent) ကဲ့သို့သော ICT နည်းပညာသစ်များနှင့်အတူ အခွင့်အလမ်းအသစ်များရှိလာသကဲ့သို့၊ လုံခြုံရေးစိန်ခေါ်မှုများလည်းရှိလာသည်။ အစိုးရသည် ပြည်သူမြောက်မြားစွာကို လိုအပ်လျှင် လိုအပ်သလို အခြေခံမူဖြင့် ချက်ခြင်း ဝန်ဆောင်မှုများရအောင် ယခင်က တစ်ကြိမ်မှ မလုပ်ဖူးပါ။ ယခု အခွင့်အရေးများနှင့်အတူ သတင်းအချက်အလက်များလုံခြုံရေးကို ပို၍ ဒူပေနာပေ ခံနိုင်၊မွမ်းမံပြင်ဆင်နိုင်၊ထိရောက်မှုရှိနိုင်စေရန် လုပ်ဆောင်ရန် လိုအပ်ချက်များရှိလာပြီဖြစ်သည်။ ယင်းဦးတည်ချက်များကို ပြည့်မှီစေရန် အစိုးရများသည် ခေတ်ပေါ်နည်းပညာများနှင့် အရေးကြီးသော အချက်အလက်များကို လုံခြုံအောင်ဆောင်ရွက်သည့် နည်းပညာများ၏ အကျိုးအမြတ်များကို အသုံးချရင်း ဂရုတစိုက်စဉ်းစားရန် လိုအပ်ပေသည်။

ပြည်ထောင်စုမြန်မာနိုင်ငံတော် အစိုးရသည် ရည်မှန်းချက်ပန်းတိုင်များကို ရှင်းလင်းစွာချမှတ်နိုင်ပြီး ယင်းရည်မှန်းချက်ပန်းတိုင်များကို ရရှိနိုင်မည့် အခြေအနေများကို ဖန်တီးနိုင်သော Cloud-First မူဝါဒ ခရီးစဉ်ကို စတင်ခဲ့ပြီဖြစ်သည်။ ယခုမူဝါဒတွင် ကာကွယ်မှုရှိသော လုံခြုံရေးမူဝါဒ၊ လုံခြုံရေးထိန်းချုပ်မှုအခြေခံမူဘောင် ကို အစိုးရမှ တိုးတက်စေရန် တိုက်ရိုက်စပ်ဆိုင်မှုပါဝင်သည်။ လုံခြုံရေးထိန်းချုပ်မှု အခြေခံမူဘောင်သည် ရုပ်ပိုင်းဆိုင်ရာနှင့် ကျိုးကြောင်းဆီလျော်သော သတင်းအချက်အလက်လုံခြုံရေး နှစ်ခုစလုံး ကိုထည့်သွင်းစဉ်းစားသည်။ မည်သို့သော နားလည်မှုလွယ်ကူသော လုံခြုံရေးမူဝါဒမဆို အရေးကြီးသော အစိတ်အပိုင်းသည် အချက်အလက်များခွဲခြားခြင်း၊ အစိုးရ အချက်အလက် မန်နေဂျာများကို မတူညီသော အချက်အလက်ပုံစံများကို မတူညီသော နည်းလမ်းများဖြင့် သင့်လျော်သလို ကာကွယ်စေနိုင်ရန်ခွင့်ပြုပေးပြီး၊လိုအပ်မှုမရှိသော၊ထိလွယ်ရှလွယ် သိပ်မရှိသော သတင်းအချက်အလက်များအတွက် ငွေကုန်ကြေးကျများသော လုံခြုံရေးထိန်းချုပ်မှုများအတွက် ရင်းမြစ်များကို ဖြုန်းတီးခြင်းများကို လျော့ချရင်း လုပ်ဆောင်ရမည့်မူဝါဒဖြစ်သည်။

အချက်အလက်ကို ကာကွယ်ရန် အချက်အလက် အမျိုးအစားခွဲခြားသတ်မှတ်ခြင်း၊လိုအပ်သော လုံခြုံရေးထိန်းချုပ်မှုများကိုနားလည်ခြင်းနှင့်အတူ သက်ဆိုင်ရာ အစိုးရသည် သီးသန့် ခွဲခြားထုတ်ဖော်မှုအတွက် လုံခြုံရေးအဆင့်များနှင့် သင့်လျော်သော ထိန်းချုပ်မှုများကို အကောင်အထည်ဖော်ရန် သို့မဟုတ် ခွဲခြားဖော်ထုတ်ရန်နှင့် လက်ရှိလုပ်ဆောင်နေသော အခြေခံ လုပ်ဆောင်မှုများတွင် ထိရောက်စွာ လည်ပတ်ဆောင်ရွက်မှုများရှိနေစေရန် ကို သေချာစေနိုင်သည်။ ကောင်းမွန်စွာတည်ဆောက်ထားသောဒူပေနာပေခံသောဆန်းစစ်အကဲဖြတ်ချက် အခြေခံမူဘောင်သည် လုံခြုံရေးထိန်းချုပ်မှုများနှင့်အတူ ထိလွယ်ရှလွယ်သည့် အချက်အလက်များကို ထိန်းညှိပေးမည်ဖြစ်ပြီး လုံခြုံရေးထိန်းချုပ်မှုများ၏ တရားဝင်ဖြစ်မှုကို ထိန်းသိမ်းပေးလိမ့်မည်ဖြစ်သည်။

အချက်အလက်အမျိုးအစား ခွဲခြားသတ်မှတ်ခြင်း အခြေခံမူဘောင် မူဝါဒ ခြုံငုံသုံးသပ်ချက်

အချက်အလက်များအားလုံးသည် တူညီမှုမရှိနိုင်ပါ။ သတင်းအချက်အလက် လုံခြုံရေးစီမံခန့်ခွဲမှုသည် အဖွဲ့အစည်းတစ်ခုအနေဖြင့် သတင်းအချက်အလက်များအားလုံးကို တစ်သမတ်တည်းလုံခြုံအောင်

ပြုလုပ်ရာတွင် အလွန်အကျွံသုံးစွဲခြင်းနှင့် ငွေကြေးမတတ်နိုင်မှုများဖြစ်လာနိုင်သည်။ အချို့သော သတင်းအချက်အလက်များမှာ ထိလွယ်ရှလွယ်နိုင်သည်၊ သို့မဟုတ် တရားမဝင် သို့မဟုတ် အန္တရာယ်များသော ဦးတည်ချက်များ ရှိကောင်းရှိနိုင်သည်။ အခြားသော သတင်းအချက်အလက်မှာ ယင်း၏ ကျယ်ပြောစွာ ပြန့်နှံ့နိုင်မှုနှင့်အတူ မည်သည့် အန္တရာယ်မျိုးမှမရှိပါ။ *အချက်အလက်အမျိုးအစား ခွဲခြားသတ်မှတ်ခြင်းသည် သတင်းအချက်အလက်တစ်ခု၏ တရားမဝင် ပြန့်နှံ့မှုနှင့် သတင်းအချက်အလက်အချို့မှ ဆွဲဆောင်နိုင်သော ခြိမ်းခြောက်မှုများအန္တရာယ် တို့နှင့်သက်ဆိုင်သော အန္တရာယ်များအရ သတင်းအချက်အလက်များကို ခွဲခြားဖော်ထုတ်သောနည်းလမ်းတစ်ရပ်ဖြစ်သည်။* အန္တရာယ်အပေါ်မူတည်၍ သတင်းအချက်အလက်ကို ခွဲခြားဖော်ထုတ်ခြင်းခြင့် စီမံကိန်းတစ်ခုသည် လုံခြုံရေးအတိုင်းအတာများကို အန္တရာယ်နှင့်အချိုးတူ လုပ်ဆောင်သွားနိုင်မည်ဖြစ်သည်။ တကယ့်အရှိတရားမှာ အများစုသော အစိုးရအဖွဲ့အစည်းများသည် ထိလွယ်ရှလွယ်နှုန်း မြင့်မားသည့် သတင်းအချက်အလက်များကို ကိုင်တွယ်မှု နည်းပါးလွန်းကြခြင်းဖြစ်သည်။ ဥပမာအားဖြင့် ဗြိတိန်အစိုးရကအစိုးရ၏ သတင်းအချက်အလက် ၉၀ ရာခိုင်နှုန်းသည် ယင်းတို့၏ အချက်အလက်အတွက် လုံခြုံရေး အနည်းဆုံးအမျိုးအစားအတွင်း ကျရောက်နေသည်ဟု ခန့်မှန်းတွက်ချက်ထားသည်။

ပုံမှန်အားဖြင့် အမျိုးအစားခွဲခြားသတ်မှတ်ခြင်း နည်းလေလေ၊အဆင့်များအကြားကွာခြားမှု ရှင်းရှင်းလင်းလင်းရှိလေလေ၊ ပို၍ ထိရောက်သော အမျိုးအစားခွဲခြားသတ်မှတ်မှု စနစ်သင့်လျော်ကောင်းမွန်စွာ ရှိနေမည်ဖြစ်ပြီး ထိလွယ်ရှလွယ် အဖြစ်ဆုံး သတင်းအချက်အလက်များကို လုံခြုံစေလိမ့်မည်ဖြစ်သည်။ အစိုးရအတွက် အများပြည်သူအကျိုးစီးပွားအတွက် အဓိကကျသော နည်းလမ်းနှစ်ရပ်ကို ဖြစ်စေသည်။ ပထမအချက်မှာ အမှန်တကယ် ထိလွယ်ရှလွယ်သော သတင်းအချက်အလက်သည် သင့်လျော်စွာ လုံခြုံမှုရှိသည်။ ဒုတိယအချက်မှာ အစိုးရသတင်းအချက်အလက်၏ ကြီးမားသောပမာဏကို ပွင့်လင်းမြင်သာမှုနှင့် ပွင့်လင်းသော အစိုးရနှင့်အတူ ပြည်သူထံ အမြဲရရှိစေနိုင်သကဲ့သို့ အစိုးရက ဂန်ဆောင်မှုများ ပေးခြင်းထက် ယင်းတို့အတွက် ထုတ်လုပ်မှုရှိသော ဒုတိယ အသုံးပြုခြင်များကို ရရှိစေခြင်း သို့မဟုတ် အများပြည်သူကောင်းကျိုးကို ရရှိစေခြင်းတို့ကိုဖြစ်စေနိုင်သည်။

အဖွဲ့အစည်းတစ်ခုက ယင်း၏ သတင်းအချက်အလက်များကို အမျိုးအစားခွဲခြားသောအခါ အမျိုးအစားခွဲခြားမှု လွန်ကဲခြင်း၊ပိတ်သိမ်း ကာကွယ်ရန်မလိုအပ်သော သတင်းအချက်အလက်များကို လုံခြုံမှုပြုထားခြင်း၏ အန္တရာယ်ရှိလာနိုင်သည်မှာ အမှန်ပင်ဖြစ်သည်။ အမျိုးအစားခွဲခြားမှု လွန်ကဲခြင်းသည် အာရုံစိုက်ရာ နေရာ ကျယ်ပြန့်လာခြင်းဖြင့် လုံခြုံရေးကာကွယ်မှုတွင် အလုံးစုံ အားနည်းလာခြင်း၊အချက်အလက်လုံခြုံရေးအတွက် ပိုမိုများပြားသော စနစ်အစုအဝေးအတွက် ဘတ်ဂျက်နှင့် အချက်အလက်အတွက် အမှန်တကယ်လိုအပ်သည်ထက် ပိုမိုကုန်ကျခြင်းမျိုးများကို ဖြစ်စေနိုင်ပါသည်။ အခြားတစ်ဖက်တွင်လည်း အမျိုးအစားခွဲခြားမှု နည်းပါးခြင်းသည် သတင်းအချက်အလက်နှင့် စနစ်များကို ကာကွယ်မှု မသင့်တော်မလုံလောက်ခြင်း က ပိတ်သိမ်းခြင်းနှင့် သက်ဆိုင်သော အန္တရာယ်များ သို့မဟုတ် မလိုမုန်းထား ပုံဖျက်မှုများကို ဖြစ်စေသည့် ခြိမ်းခြောက်မှုများ သို့မဟုတ် သတင်းအချက်အလက်ဖျက်ဆီးမှုများနှင့် အချိုးညီသည်။ ထို့အတွက်ကြောင့် အချက်အလက် အမျိုးအစားခွဲခြားခြင်းစနစ်တစ်ခုကို အကောင်အထည်ဖော်သောအခါ အမျိုးအစားများကို ရှင်းလင်းစေရန် အရေးကြီးပြီး အမျိုးအစားခွဲခြားရေးအတွက် တာဂန်ရှိသူများသည် အမျိုးအစားများနှင့် အမျိုးအစားခွဲခြားခြင်း၏ အဓိကကျသော ပန်းတိုင်များကြား ကွာခြားမှုများကို နားလည်သဘောပေါက်ရန်မှာ အလွန်အရေးကြီးသည်။

ယခုမူဝါဒ ချဉ်းကပ်မှုအတွက် ချိတ်ဆက်နေသော လိုအပ်ချက် နှစ်ချက်ရှိသည်။

- အချက်အလက် အမျိုးအစားခွဲခြားမှု- တစ်စုံတစ်ရာသော အစိုးရအချက်အလက်နှင့် ပက်သက်သော အန္တရာယ်ကို ခွဲခြားထုတ်ဖော်ခြင်း။
- လုံခြုံရေး အခြေခံမူဘောင်- တစ်စုံတစ်ရာသော အစိုးရ အချက်အလက်နှင့် ဆက်နွယ်နေသော အန္တရာယ်အဆင့်အတန်းနှင့် ကိုက်ညီသော ရှင်းလင်းသည့် လုံခြုံရေးထိန်းချုပ်မှု လိုအပ်ချက်များကို သေချာစေခြင်းနှင့် ယင်းတို့ကို အစိုးရတစ်ဖွဲ့မှ အသုံးပြုစေခြင်း။

ယခုမူဝါဒသည် ဆက်နွယ်နေသော အမြင်ရှုထောင့်နှစ်ခုကို ခွဲခြားထားသည်။ ပထမအချက်မှာ အစိုးရအချက်အလက်မန်နေဂျာများက IT systems များတွင် လုံခြုံစွာ သိုလှောင်ထားနိုင်ရန်အတွက် ယင်းတို့၏ အချက်အလက်များကို ယင်းတို့၏ အချက်အလက်များကို ပြင်ဆင်နိုင်စေရန် အချက်အလက်အမျိုးအစာခွဲခြားခြင်း ရှုထောင့်မှ အချက်အလက်လုံခြုံရေးကိုစဉ်းစားခြင်းဖြစ်သည်။

ဒုတိယအပိုင်းသည် အစိုးရအချက်အလက်၏ ထိလွယ်ရှလွယ်ဖြစ်မှု အဆင့်အတန်းအတွက် လုံခြုံရေး ထိန်းချုပ်မှုများကို ချိန်ညှိရန် အစိုးရ အချက်အလက်မန်နေဂျာများက Cloud Service Providers(CSPs) နှင့် အလုပ်လုပ်ဆောင်နိုင်ခြင်းဖြင့် လုံခြုံရေး အခြေခံမူဘောင်ကို စီစဉ်ပေးသည်။

အစိုးရအဖွဲ့အစည်းတစ်ခုချင်းစီ၊တစ်သီးပုဂ္ဂလတစ်ဦးချင်းစီအတွက် ဤနေရာတွင် အဖွဲ့အစည်းအတွင်းမှ အသင်းကို ဦးဆောင်ရန် "အစိုးရ အချက်အလက်မန်နေဂျာ" ဟုရည်ညွှန်းသည်။ အဆိုပါ အဖွဲ့အစည်းသည် အချက်အလက်အမျိုးအစား ခွဲခြားခြင်းဖြစ်စဉ်များကို ဦးဆောင်ပြီး ယခု မူဝါဒနှင့် အညီ လုံခြုံရေး ထိန်းချုပ်မှုများ အကောင်အထည်ဖော်သည်။ အစိုးရအချက်အလက်မန်နေဂျာသည် ဖန်တီးထားသော၊ထိန်းသိမ်းထားသော အချက်အလက် သို့မဟုတ် ယင်းတို့၏သက်ဆိုင်ရာ အစိုးရအဖွဲ့အစည်းမှ စီမံခန့်ခွဲသော သတင်းအချက်အလက်တို့၏ လုံခြုံရေးအတွက် တာဝန်ရှိသည်။

အချက်အလက်အမျိုးအစားခွဲခြားခြင်း မိတ်ဆက်

အဖွဲ့အစည်းတစ်ခုစီတိုင်းသည် ယင်းအဖွဲ့အစည်းအတွက် အချက်အလက်စီမံခန့်ခွဲမှုနှင့် ထိန်းချုပ်မှုများအတွက် တာဝန်ရှိသူ တစ်ဦးကို ခွဲခြားဖော်ထုတ်ရန်မှာ အရေးကြီးလှသည်။ ဤနေရာတွင် "အစိုးရအချက်အလက်မန်နေဂျာ" ဟု ရည်ညွှန်းသော အဆိုပါတာဝန်ရှိသူသည် ယခုမူဝါဒနှင့်အညီ အချက်အလက်အမျိုးအစား ခွဲခြားခြင်းနှင့် လုံခြုံရေးထိန်းချုပ်မှုများအကောင်အထည်ဖော်ခြင်း ဖြစ်စဉ်များကို ဦးဆောင်ရန် တာဝန်ရှိသည်။ အစိုးရအချက်အလက်မန်နေဂျာသည် ဖန်တီးထားသော၊ထိန်းသိမ်းထားသော အချက်အလက် သို့မဟုတ် ယင်းတို့၏သက်ဆိုင်ရာ အစိုးရအဖွဲ့အစည်းမှ စီမံခန့်ခွဲသော သတင်းအချက်အလက်တို့၏ လုံခြုံရေးအတွက် တာဝန်ရှိသည်။

အစိုးရများသည် ထိလွယ်ရှလွယ်ဖြစ်နိုင်မှု မြင့်မားသော သတင်းအချက်အလက်ကို ထိလွယ်ရှလွယ်ဖြစ်နိုင်မှု နည်းပါ သို့မဟုတ် ထိလွယ်ရှလွယ် မရှိ ဆိုသည်တို့မှ ခွဲခြားရန်လိုအပ်လာခဲ့သည်မှာကြာပြီဖြစ်သည်။ လိုအပ်သောလုံခြုံရေးပိုမိုကောင်းမွန်သောအနေအထား၏ မြင့်မားသော အဆင့်များအချက်အလက်ကို ရှင်းလင်းစွာ ထုတ်ဖော်ပြသချက်သည် အစိုးရအား ICT နှင့် cloud ရင်းနှီးမြှုပ်နှံမှုများထံမှ အကျိုးအမြတ်ရရှိစေပြီး အများပြည်သူများထံ နည်းပါးသော အဖိုးအခဖြင့် ပိုမိုကောင်းမွန်သော ဝန်ဆောင်မှုကို ပေးနိုင်စေသည်။ မည်သည့်လုံခြုံရေးထိန်းချုပ်မှု အခြေခံမူဘောင်မဆို

အချက်အလက်သစ်၏ ထိရောက်သော အမျိုးအစားခွဲခြားမှုတွင် မူတည်သည်။ အချက်အလက်သစ် အမျိုးအစားခွဲခြားခြင်းအတွက် တာဂန်ရှိသော လူပုဂ္ဂိုလ် သို့မဟုတ် အသင်းသည် အဆိုပါ အဖွဲ့အစည်းမှ လည်ပတ်နေသော အချက်အလက်အတွက် အန္တရာယ်ရှိသောအကဲဖြတ်ဆန်းစစ်ချက်ကို ဆောင်ရွက်သည်။ အချက်အလက်၊တန်ဖိုး၊အချက်အလက်၏ထိလွယ်ရှလွယ်ဖြစ်နိုင်မှု၊အရေးပါမှုတို့နှင့်အတူ ဆက်နွယ်နေသော အဖွဲ့အစည်းဆိုင်ရာ အန္တရာယ် အပေါ်မူတည်ပြီး အဆိုပါ သတင်းအချက်အလက်ကို သင့်လျော်သောအမျိုးအစားအတွင်း ထည့်သွင်းနိုင်သည်။ ၎င်ရောက်ခွင့် ထိန်းချုပ်မှုများနှင့် အနည်းဆုံး-လုံခြုံရေးလိုအပ်ချက်များသည် အချက်အလက်ခွဲခြားမှု တစ်ခုချင်းစီအတွင်း အချက်အလက် ကိုင်တွယ်ခြင်း၊စီမံခန့်ခွဲမှုတို့အတွက် အခြေပြုတည်ဆောက်ရန် လိုအပ်သည်။

အစိုးရ အဖွဲ့အစည်းအများစုသည် ထိလွယ်ရှလွယ်ဖြစ်နိုင်ချေ မြင့်မားမှု နည်းနည်း ရှိသော သတင်းအချက်အလက်များကို ကိုင်တွယ်ကြသည်။ ယင်းအချက်က ပြည်ထောင်စုမြန်မာနိုင်ငံတော် အစိုးရအပါအဝင် အစိုးရအများစုသည်အဘယ့်ကြောင့် ICT ရယူသုံးစွဲခြင်းအတွက် "cloud-first" မူဝါဒကို အသုံးပြုရသနည်းဆိုသည်ကို အခြေခံဖြစ်စေသည်။ သို့ရာတွင် အန္တရာယ်နည်းပါးသည့် အတွက် သင့်လျော်သော လုံခြုံရေးရှိရမည်ဆိုစေကာမူ အရေးကြီးသော သတင်းအချင်အလက်အတွက် သင့်လျော်သော လုံခြုံရေးရှိကိုရှိရမည်ဖြစ်သည်။ **ယခု မူဝါဒလမ်းညွှန်ချက်များအရ အစိုးရသည် သတင်းအချက်အလက်များအား ခွဲခြားသတ်မှတ်ခြင်းကို စီစစ်စိတ်စိတ်ဖြာရာတွင် စံအားဖြင့် သတင်းအချက်အလက်များကို ကာကွယ်ပေးရန်သာဖြစ်ပြီး သင့်လျော်သော လုံခြုံရေး အဆင့်အတန်းတွင် သတင်းအချက်အလက်ကို ကာကွယ်ပေးရမည်ဖြစ်သည်။**

အချက်အလက်အမျိုးအစားခွဲခြားဖော်ထုတ်ခြင်းစနစ် တစ်ခု၏ အခြေခံကျသော စည်းမျဉ်းများ

အမျိုးအစားခွဲခြားသတ်မှတ်ခြင်းအတွက် ကိုယ်စားလှယ်အဖွဲ့တစ်ခု၏ သိပ္ပံနည်းကျ မျိုးခွဲခြင်းသိပ္ပံနည်းပညာအရ စတင်အမှတ်သည် သတင်းအချက်အလက်ကို အတန်းအစားခွဲခြားသတ်မှတ်နိုင်သည်။ သိပ္ပံနည်းကျ ခွဲခြားသတ်မှတ်မှုသည် တစ်သီးပုဂ္ဂလများ အမျိုးအစားခွဲခြားသတ်မှတ်ခြင်းတစ်ခုချင်းစီအတွက် လိုအပ်ချက်များနှင့်အတူ လုံခြုံရေးလိုအပ်ချက်များသင့်လျော်စွာ ချိန်ညှိနိုင်ရန်အလို့ငှာ ထိရောက်မှုရှိသော လမ်းညွှန်ချက်နှင့်အတူ ပုံမှန်အားဖြင့် အကောင်အထည်ဖော်နိုင်ရန်ဖြစ်သည်။ ထုံးစံအားဖြင့် ခွဲခြားဖော်ထုတ်မှု အဆင့်

နည်းပါးလေလေ၊အဆင့်များအကြား ကွာခြားမှုများ ရှင်းလင်းလေလေ၊ အမျိုးအစားခွဲခြားသတ်မှတ်ခြင်း စနစ်သည် ပို၍ ထိရောက်လေလေဖြစ်ကာ ထိလွယ်ရှလွယ်အဖြစ်နိုင်ဆုံးသော သတင်းအချက်အလက်ကို သင့်လျော်စွာ လုံခြုံမှု ပေးထားကြောင်း သေချာစေသည်။[14] ယင်းသည် အများပြည်သူအကျိုးစီးပွားကို အဓိကကျသော နည်းလမ်းနှစ်သွယ်ကို လုပ်ဆောင်ပေးသည်။ (၁)အမှန်တကယ်ထိလွယ်ရှလွယ်သော သတင်းအချက်အလက်သည် သင့်လျော်စွာ လုံခြုံမှုရှိသည် နှင့် (၂) ရင်းမြစ်များသည် အခြားသတင်းအချက်အလက်များကို လုံခြုံစေခြင်းဖြင့် အလဟသ ဖြုန်းတီးမှု မရှိပါ။

အမျိုးအစားခွဲခြားသတ်မှတ်မှု လွန်ကဲခြင်းသည် အဖွဲ့အစည်းတစ်ခု၏ အချက်အလက်ကာကွယ်ရေး ခုခံမှုများကို စနစ်အစုအဝေးနှင့် လိုအပ်သောအချက်အလက်များထက် ကျယ်ပြန့်စေခြင်းဖြင့် အလုံးစုံအားဖြင့် အင်အားယုတ်လျော့စေသည်။ အခြားတစ်ဖက်တွင် အမျိုးအစားခွဲခြားသတ်မှတ်မှုလျော့ပါးခြင်းသည် အချက်အလက်ဆုံးရှုံးရခြင်း သို့မဟုတ် အချက်အလက်ကို မလိုမုန်းထား ပုံဖျက်ခြင်းတို့ကို ကောင်းမွန်စွာ ကာကွယ်နိုင်ခြင်းမရှိပါ။ ထို့အတွက်ကြောင့် အချက်အလက်ခွဲခြားဖော်ထုတ်မှုစနစ်တစ်ခုကို စတင်သောအခါ အမျိုးအစားများသည် ရှင်းလင်းရန်နှင့် အမျိုးအစားခွဲခြားသတ်မှတ်ခြင်းအတွက် စည်းမျဉ်းစည်းကမ်းများနှင့် ရည်မှန်းချက်ပန်းတိုင် များကို အပြည့်အဝ ရှင်းလင်းစွာ နားလည်နိုင်ရန်မှာ အရေးကြီးလှသည်။

ရှေ့နောက်ညီညွတ်မှုသည် အစိုးရတစ်ဖှဲ့မ်းလုံးအတွက် အရေးကြီးသည်။ အစိုးရတစ်ဖှဲ့မ်း ရှေ့နောက်ညီညွတ်မှု ပိုမိုကောင်းမွန်လေ၊ သတင်းအချက်အလက်လုံခြုံရေး လိုအပ်ချက် များ အတွက် cloud ဝန်ဆောင်မှုများက ပိုမိုထိရောက်စွာ ထိန်းညှိဆောင်ရွက်ပေးနိုင်လေဖြစ်သည်။[15] အစိုးရတစ်ဖှဲ့မ်းမှ ရှင်းလင်းသော၊ရှေ့နောက်ညီညွတ်မှုရှိသော အမျိုးအစားခွဲခြားသတ်မှတ်မှုသည် အစိုးရအတိုင်းအတာတစ်ခုလုံး ရှေ့နောက်ညီညွတ်မှုကို ဖြစ်စေနိုင်သည်။ Cloud ပထမမူဝါဒအရ သတင်းအချက်အလက်နည်းပညာနှင့် ဆိုက်ဘာလုံခြုံရေး ဌာန(ITCSD) သည် CSP အသိအမှတ်ပြုခြင်းနှင့်

[14] အစိုးရကခြောက်မျိုးမှာ သုံးမျိုးအထိ အမျိုးအစား ခွဲခြားသတ်မှတ်ခြင်းကို အရှိန်အဟုန်ဖြင့်လုပ်ဆောင်ခြင်းနှင့် တစ်ခုချင်းစီတိုင်းအတွက်စရိုက်လက္ခဏာများကို ရှင်းလင်းစေခြင်းဖြင့် ပြီတိန်တွင် ပြုလုပ်ခဲ့သော မကြာသေးခင်က အပြောင်းအလဲများအရ သက်သေအထောက်အထားရှိသည်။

[15] ဥပမာအားဖြင့် အမေရိကန်သည် အမျိုးသားစံနှုန်းများနှင့်နည်းပညာ(NIST)မှ ကြီးကြပ်မှုနှင့် သတင်းအချက်အလက်နှင့် သတင်းအချက်အလက်စနစ်များဆိုထားရန် ပြဋ္ဌာန်းချက်များအရ အချက်အလက်ခွဲခြားသတ်မှတ်ခြင်းတွင်တွင် ပိုမိုများများပြားသော ရှေ့နောက်ညီညွတ်မှုများကို ဖန်တီးရန် အတိုင်းအတာများပြုလုပ်ခဲ့ပြီးဖြစ်သည်။ အဆိုပါစံနှုန်းများကို အစိုးရတစ်ဖှဲ့မ်းလုံးမှ အသုံးပြုနိုင်ပြီး၊ အမျိုးသားမော်ကွန်းတိုက်နှင့် မှတ်ပုံတင်ဌာန(NARA)ကိုယ်စားလှယ်တစ်ဖွဲ့ထဲမှ ကြီးကြပ်နိုင်သည်။ အစိုးရတစ်ဖှဲ့မ်းလုံး အသိအမှတ်ပြုမှုများကို the US FedRAMP cloud ရယူသုံးစွဲခြင်း အသိအမှတ်ပြု အစီအစဉ်မှ ရေးဆွဲသည်။ FedRAMP သည် cloud service provider မှ လုံခြုံရေးလိုအပ်ချက်များနှင့် ကိုက်ညီအောင် လုပ်ပေးနိုင်ကြောင်း အသိအမှတ်ပြုသည်။ ထို့နောက် ဖက်ဒရယ်ကိုယ်စားလှယ်အဖွဲ့တစ်ဖွဲ့သည် သက်ဆိုင်ရာ service provider သည် FedRAMP လိုအပ်ချက်များနှင့် ကိုက်ညီကြောင်းပို့လျှဲနေသည်များကို လျော့ချနိုင်ကြောင်း သိရှိပြီး မိမိအဖွဲ့အစည်းလိုအပ်ချက်များနှာင့် လုံခြုံရေးလိုအပ်ချက်များအတွက် သင့်လျော်ကြောင်း သိရှိသည့်အတွက် ဝန်ဆောင်မှုများကို ရယူနိုင်လိမ့်မည်ဖြစ်ကာ ကုန်ကျစားရိတ်များကို လျော့ချနိုင်လိမ့်မည်ဖြစ်သည်။

အစိုးရကိုယ်စားလှယ်အဖွဲ့များကို အသိအမှတ်ပြုခံထားရသော cloud ဝန်ဆောင်မှု များကို သင့်လျော်စွာရယူရန် အွန်လိုင်းစျေးကွက်နေရာတစ်ခုရှိစေရန် အခြေပြုနိုင်သည်။

အစိုးရတစ်ရပ်က တိုးတက်လာသည်နှင့် အမျိုးအစားခွဲခြားဖော်ထုတ်ထားသော အစီအစဉ်တစ်ခုကို အကောင်အထည်ဖော်နေချိန်တွင် အဆိုပါ သတင်းအချက်အလက်မှာ သင့်လျော်စွာ လုံခြုံအောင်ထားရှိခံထားရကြောင်း ကိုသေချာစေရန်၊အဆိုပါ ရည်မှန်းချက်ကို အလေးစိုက်နေစေရန် အာရုံစူးစိုက်နေစေရန် အရေးကြီးသည်။ အဆိုပါရည်မှန်းချက်ပန်းတိုင်ကို ရောက်ရှိရန် အမျိုးအစားခွဲခြားသတ်မှတ်ခြင်းဖြစ်စဉ်သည် သီးသန့် သတင်းအချက်အလက်နှင့် ဆက်နွယ်သော အန္တရာယ်ကို အမျိုးအစားခွဲခြားဖော်ထုတ်ရန်၊ နည်းပါးသောသို့မဟုတ် ထူးထူးခြားခြားလုံခြုံရေး မလိုအပ်ကြောင်းမှ မြင့်မားသောလုံခြုံရေး အဆင့်ကို ခွဲခြားပေးသင့်ပြီး အဆိုပါသတင်းအချက်အလက်ကို ကောင်းမွန်စွာ ကာကွယ်ပေးနိုင်ရန် သင့်လျော်သော လုံခြုံရေးကို ချမှတ်ရမည်။ ယင်းအတွက်ရလဒ်မှာ မြင့်မားသော ထိရောက်မှုနှင့် အချိုးညီသော ကုန်ကျစားရိတ် သက်သာမှုများကို ဖြစ်ပေါ်စေလိမ့်မည်။

အစိုးရအချက်အလက်မန်နေဂျာ တစ်ဦး၏ အဓိက တာဝန်များ

ယခုမူဝါဒအောက်တွင် အချက်အလက်ခွဲခြားသတ်မှတ်ခြင်း၏ ရည်မှန်းချက်ပန်းတိုင်သည် အစိုးရအချက်အလက်မန်နေဂျာက အစိုးရ၏ Cloud-First မူဝါဒကို အကောင်အထည်ဖော်နိုင်ရန်ဖြစ်သည်။ Cloud computing ကို အသုံးပြုရန် စဉ်းစားသော အခါ အစိုးရအချက်အလက်မန်နေဂျာတွင် တာဝန်သုံးရပ်ရှိလာသည်။

- သီးခြား အစိုးရအချက်အလက်နှင့် ဆက်နွယ်သော အန္တရာယ်ကို ခွဲခြားဖော်ထုတ်ခြင်းဖြင့် အချက်အလက်ကို အမျိုးအစားခွဲခြားသတ်မှတ်ခြင်း။
- သီးခြား အစိုးရအချက်အလက်နှင့်သက်ဆိုင်သော အန္တရာယ်အဆင့်နှင့်အညီ ရှင်းလင်းသော လုံခြုံရေး ထိန်းချုပ်မှုလိုအပ်ချက်များနှင့် အဆိုပါလိုအပ်ချက်များကို အစိုးရ အဖွဲ့အစည်းတစ်လျှောက် အသုံးပြုခြင်းတို့ကို ဖြည့်ဆည်းပေးသော လုံခြုံရေး အခြေခံမူဘောင်ကိုအကောင်အထည်ဖော်ခြင်း။

- အစိုးရအဖွဲ့အစည်းက cloud ပန်ဆောင်မှုများကို ရယူခြင်းနှင့် cloud ပန်ဆောင်မှုပေးသူက လုံခြုံရေးနှင့် အွန်လာရယ်စီမံခန့်ခွဲမှုတို့နှင့်အတူ ယင်းတို့၏ တာဝန်များကို နားလည်ကြောင်းသေချာစေခြင်း။

အချက်အလက်ခွဲခြားဖော်ပြခြင်း

သတင်းအချက်အလက် ခွဲခြားသတ်မှတ်ခြင်းစနစ်အတွက် အလွှာသုံးလွှာချဉ်းကပ်ချက်သည် အစိုးရကဏ္ဍကွက်အတွင်း ရရှိနိုင်သော cloud compiting ကဲ့သို့ modem ICT နည်းပညာများကို အသုံးပြုနေချိန်တွင် အစိုးရသတင်းအချက်အလက်အတွက် သင့်လျော်သော လုံခြုံရေးအဆင့်ကို သေချာစေနိုင်သည်။ ပြည်ထောင်စုမြန်မာနိုင်ငံတော်အစိုးရသည် အောက်ဖော်ပြပါ အလွှာသုံးလွှာ လုံခြုံရေးခွဲခြားသတ်မှတ်မှုကို အသုံးပြုသည်။

- ထိပ်တန်းလျှို့ဝှက်ချက်- ကာကွယ်ရေးအမြင့်ဆုံး အတိုင်းအတာကို လိုအပ်ခြင်း။ အမြင့်ဆုံးသော ကာကွယ်မှုကို လိုအပ်သည်။ ယခု သတင်းအချက်အလက်ကို ညှိနှိုင်းအပေးအယူလုပ်ခြင်းသည် ခြွင်းချက်မရှိ စိုးရိမ်ဖွယ်အနေအထား သို့မဟုတ် အမျိုးအစားခွဲခြားဖော်ထုတ်ရေး အာဏာပိုင်က ဖော်ပြခဲ့သည့်အတိုင်း အမျိုးသားအကျိုးစီးပွား၊အဖွဲ့အစည်းများ သို့မဟုတ် တစ်ဦးတစ်ယောက်ချင်းစီများအတွက် ကြီးမားပြင်းထန်သော ထိခိုက်မှုဖြစ်စေနိုင်ကြောင်းမျှော်လင့်ရသည်။
- လျှို့ဝှက်ချက်- အဆိုပါ အချက်အလက်ကို ညှိနှိုင်းအပေးအယူလုပ်သောအခါ အမျိုးအစားခွဲခြားဖော်ထုတ်ရေး အာဏာပိုင်က ဖော်ပြခဲ့သည့်အတိုင်း အမျိုးသားအကျိုးစီးပွား၊အဖွဲ့အစည်းများ သို့မဟုတ် တစ်ဦးတစ်ယောက်ချင်းစီများအတွက် ပြင်းထန်သော ထိခိုက်မှုများရှိလာနိုင်သည့်အခါ အသုံးပြုသည်။
- အထွေထွေ - အဆိုပါ အချက်အလက်ကို ညှိနှိုင်းအပေးအယူလုပ်သောအခါ အဖွဲ့အစည်းဆိုင်ရာလုပ်ငန်းများ၊အဖွဲ့အစည်းဆိုင်ရာ ပိုင်ဆိုင်မှုများ သို့မဟုတ် တစ်ဦးတစ်ယောက်ချင်းစီအတွက် အသေးစားထိခိုက်မှုများသာ ဖြစ်လာမည်ဟုမျှော်လင့်ထားသောအခါ အသုံးပြုသည်။ ယခုအချက်အလက်တွင်

သတင်းအချက်အလက်သည် စီးပွားရေးလိုအပ်ချက်များ သို့မဟုတ်
လုပ်ငန်းဆောင်ရွက်မှုများအတွက် အရေးမကြီးသည့်ထဲတွင်ပါဝင်နိုင်သည်။[16]

အထွေထွေသည် လုံခြုံမှုရှိသော အစိုးရသတင်းအချက်အလက်၏ကြီးမားသော ပမာဏအတွက် အသုံးပြုသော အမျိုးအစားခွဲခြားသတ်မှတ်ခြင်းဖြစ်သည်။ အထွေထွေ အမျိုးအစား ခွဲခြားသတ်မှတ်ခြင်းကို အသုံးပြုရန်၊မပြုရန် တန်ဖိုးတွက်ချက်လိုက်သောအခါ ခွဲခြားစီစစ်ခြင်း၏ ပထမအဆင့်သည် သက်ဆိုင်ရာ အဖွဲ့အစည်းအတွက် အန္တရာယ်ကို ကြည့်ခြင်းဖြစ်သည်။ ဒုတိယအဆင့်သည် အဆိုပါသတင်းအချက်အလက်အတွက် လုံခြုံရေးဦးစားပေးချက်များကို စဉ်းစားရန် လိုအပ်သည်။

အထွေထွေ အဆင့်အလွှာကို တန်ဖိုးဖြတ်ရာတွင် အောက်ပါတို့ကို စဉ်းစားခြင်းဖြင့် အဆိုပါအဖွဲ့အစည်းအတွက် ကျရောက်နိုင်သော အန္တရာယ်ကို စဉ်းစားရမည်။

1. အသုံးပြုနိုင်သော ဥပဒေများ၊ အစိုးရမူဝါဒများနှင့် ကိုက်ညီရမည်။
2. မလိုမုန်းထားဝင်ရောက်မှု သို့မဟုတ် သက်ဆိုင်ရာ ကိုယ်စားလှယ်အဖွဲ့ သို့မဟုတ် အစိုးရ သို့မဟုတ် အခြားသော အမျိုးသားအကျိုးစီးပွားကို ထိခိုက်စေသော သတင်းအချက်အလက်ကို ဖြန့်ဖြူးခြင်း အန္တရာယ်နှင့်
3. မလိုမုန်းထားလုပ်ဆောင်သူတစ်ဦးအတွက် အဆိုပါ သတင်း၏ အလားအလာရှိသော တန်ဖိုး
    a. မလိုမုန်းထားလုပ်ဆောင်သူတစ်ဦးအတွက် အဆိုပါ သတင်းအချက်အလက်၏ ငွေကြေးဆိုင်ရာ သို့မဟုတ် အခြားတိုက်ရိုက်ရှိသော တန်ဖိုး
    b. ဖီလာဆန့်ကျင်ပြုသော လူ့အဖွဲ့အစည်းဆိုင်ရာ ဂယက်များ (ဥပမာ- စီးပွားရေးထိခိုက်စေမှုဥပဒေအခွင့်အရေးများကို ရေရှည်ရှိအောင်လုပ်ခြင်း သို့မဟုတ် နိုင်ငံရေးတည်ငြိမ်မှု)

အမျိုးအစားခွဲခြားထားသောသတင်းအချက်အလက် အလွှာသုံးလွှာ အပြင် အစိုးရသတင်းအချက်အလက်အများစုသည် သတင်းအချက်အလက်ဝင်ရောက်ရယူနိုင်မှု သို့မဟုတ် ဖြန့်ဖြူးခံရနိုင်မှု မရှိပါပဲ(သို့မဟုတ် ဖြစ်နိုင်တရာတစ်စုံတစ်ရာ)အမျိုးအစားမခွဲခြားပဲထားရှိလိမ့်မည်။

[16] အချို့သော သတင်းအချက်အလက်ကို တစ်ချို့သော ပရိသတ်ကို ကန့်သတ်ထားကို ထားသင့်သည်။ ယင်းအကြောင်းပြောရလျှင် အမျိုးအစားခွဲခြားသတ်မှတ်မှုတွင် "မဖတ်ခင်စဉ်းစားရန်များ" ပါဝင်နိုင်သည်။ ဥပမာအားဖြင့် "သိရန်လိုအပ်" အခြေခံအတွက် ဂင်ရောက်ရန်ကန့်သတ်ခြင်းဖြစ်သော "PROTECTED-SENSITIVE" နှင့် အဆိုပါသတင်းအချက်အလက်အတွက် (ဥပမာ- တစ်သီးပုဂ္ဂလ၊အစိုးရယူနစ်တစ်ခု သို့မဟုတ် နိုင်ငံခြားအစိုးရတစ်ခုမှ ကိုယ်စားလှယ်တစ်ဦး) "PROTECTED-EYES-ONLY"

ယခုသတင်းအချက်အလက်အတွက် လုံခြုံရေးပူပန်စရာရှိကောင်းရှိနေဆဲဖြစ်သည်။ သို့ရာတွင် သင့်လျော်အများပြည်သူသုံး cloud သတင်းအချက်အလက်စနစ်အတွက် စံချိန်မီ လုံခြုံရေးအတိုင်းအတာများနှင့်အတူ ထုံးစံအတိုင်း ယင်းပူပန်စရာများကို ဖော်ပြနိုင်သည်။ အချို့သော အမျိုးအစားမခွဲခြားရသေးသော သတင်းအချက်အလက်အတွက် အဆိုပါ သတင်းအချက်အလက်လုံခြုံရေးကို တာဝန်ရှိသူသည် လုံခြုံရေး အတိုင်းအတာများကို ဖော်ပြရင်း ဝန်ဆောင်မှုအဆင့် သဘောတူညီချက်(SLA) တွင် သတ်မှတ်ချက်များရယူခြင်းနှင့်အတူ သင့်လျော်သော အတိုင်းအတာများကို ညှိနှိုင်းဆောင်ရွက်လိုပေလိမ့်မည်။

လုံခြုံရေးထိန်းချုပ်မှု အခြေခံမူဘောင်

မည်သည့်ICT ပတ်ဝန်းကျင်အတွက်မဆို ထိန်းချုပ်မှုအခြေခံမူဘောင်သည် ရုပ်ပိုင်းဆိုင်ရာနှင့် လော့ဂျစ်ကယ်ဆိုင်ရာလုံခြုံရေးထိန်းချုပ်မှုများတွင်မူတည်သည်။

ရုပ်ပိုင်းဆိုင်ရာ လုံခြုံရေးကို အမြင်ရှုထောင့် သုံးခုဖြင့် ဖွဲ့စည်းထားသည်။

1. ICT အခြေခံအဆောက်အဦတွင်းသို့ သင့်လျော်သော ဝင်ရောက်ခွင့်များနှင့် တာဝန်ရှိသူများကို ဝင်ရောက်ခွင့်ပြုရန် ကန့်သတ်ခြင်း။
2. ICT အခြေခံအဆောက်အဦသည် ရေကြီးခြင်းကဲ့သို့ သဘာဝဘေးအန္တရာယ်များနှင့်ရုပ်ပိုင်းဆိုင်ရာ အန္တရာယ်မှ ဘေးကင်းကာ ဥပမာအားဖြင့် မီးပျက်နေလျှင်ပင် ဆက်လက် လုပ်ငန်းဆောင်ရွက်နေစေလိမ့်မည်(သို့မဟုတ် လက်ခံထားသော နောက်ကျ အချိန်အတိုင်းအတာတစ်ခုအတွင်း ပြန်လည် လည်ပတ်မည်)
3. ICT ရင်းမြစ်များက အချိန်တိုင်းတောင်းဆိုသော လိုအပ်ချက်များနှင့် ကိုက်ညီမှုရှိစေရန် လုံလောက်သော ရင်းမြစ်များကို စီစဉ်ခြင်း၊ဆောင်ရွက်ခြင်း။

လော့ဂျစ်ကယ်ဆိုင်ရာ လုံခြုံရေးထိန်းချုပ်မှုကို အချက်အလက်ဝင်ရောက်ရယူနိုင်မှုကို ကန့်သတ်ရန် လုပ်ထုံးလုပ်နည်းကျင့်ဝတ်များနှင့် ကိရိယာတန်ဆာပလာများပါဝင်သည်။ ယင်းတို့ထဲတွင်

1. အန္တရာယ်အရ အချက်အလက်အမျိုးအစားခွဲခြားခြင်း

2. မတူညီသော အချက်အလက် အမျိုးအစားခွဲခြားမှုများအတွက် လုံခြုံရေးရှင်းလင်းမှုများကို အဓိပ္ပါယ်ဖွင့်ဆိုခြင်း
3. လုံခြုံရေးစံနှုန်းများနှင့် အသုံးပြုသူ အခွင့်အာဏာပေးအပ်မှု အဆင့်များကို အဓိပ္ပါယ်ဖွင့်ဆိုခြင်း
4. အချက်အလက်အမျိုးအစားခွဲခြားမှုအရ အချက်အလက် စီမံခန့်ခွဲခြင်း
5. အကျိုးဂင်မှုကို အကောင်အထည်ဖော်ခြင်းနှင့် လုံခြုံရေး ထိန်းချုပ်မှုများနှင့်ကိုက်ညီမှုရှိခြင်းသေချာစရေန် စည်းမျဉ်းစည်းကမ်းများကို စာရင်းစစ်ခြင်း

ယင်းတို့ထဲမှမြောက်များလှစွာသော တာဂန်ယူများကို အကောင်အထည်ဖော်ခြင်း၊ ဆော့ဖ်ဝဲလ်အနက်ဖွင့် အမျိုးအစားခွဲခြားဖော်ထုတ်ခြင်းကိုလည်ပတ်ဆောင်ရွက်ခြင်းနှင့် တစ်သီးပုဂ္ဂလများ အချက်အလက်ရယူခြင်းတို့ကို လုပ်ဆောင်ခြင်းဖြင့် ပြီးမြောက်နိုင်သည်။

Cloud အခြေပြု လုံခြုံရေးထိန်းချုပ်မှု အခြေခံမူဘောင်

Cloud အခြေပြု ICT ပတ်ဂန်းကျင်နှင့်အတူ အချက်အလက်လုံခြုံရေးသည် မျဖေထားသော တာဂန်ဖြစ်သည်။ အစိုးရအချက်အလက်မန်နေဂျာသည် ယင်းတို့၏ CSP အတွက် ရုပ်ပိုင်းဆိုင်ရာ လုံခြုံရေး ထိန်းချုပ်ရန် အတွက် တာဂန်အမြောက်အများထမ်းဆောင်ရန် ပြင်ပ ရင်းမြစ်ရှာဖွေရကောင်းနိုင်သည်။ CSPs များသည် ထုံးစံအားဖြင့် မြောက်များစွာသော ဖောက်သည်များကို ကြီးမားသော အတိုင်းအတာဖြင့် အထောက်အပံ့ပေးမှုများကို လည်ပတ်ဆောင်ရွက်သည်။ စီးပွားရေးအတိုင်းအတာသည် CSPs များကို ရှိရင်းစွဲ ICT အဆောက်အဦအတွက် အကောင်အထည်ဖော်နိုင်ရန် အလားအလာများသော ကန့်သတ်ချက်ပိုများသည့် ရုပ်ပိုင်းဆိုင်ရာ ဂင်ရောက်ထိန်းချုပ်မှုကို အကောင်အထည်ဖော်စေနိုင်သည်။ CSP ၏ အချက်အလက်ဌာနများသည် သဘာဂပတ်ဂန်းကျင်အန္တရာယ်ခြိမ်းခြောက်မှုများနှင့် လူသားအမှားများကို ကြံ့ကြံ့ခံနိုင်သကဲ့သို့ ရင်းမြစ်ကွန်ယက်တစ်ခုခု ပျက်သွားခဲ့ပါက ပိုလျှံနေသော ရင်းမြစ်များက အလိုအလျောက်အလုပ်လုပ်ဆောင်ကာ failover ခလုတ်များပွင့်လာလိမ့်မည်။

CSPs များသည် စက်ရုံတွင်း ICT စနစ်ကို တိုင်းတာရန် ရက်များ၊ရက်သတ္တပတ်များ၊လများ ကြာမြင့်တတ်သော ICT ရင်းမြစ်များ၏ အရေးပေါ်လိုအပ်ချက်များကို တိုင်းတာခြင်းအား အချိန်တိုတွင်းဆောင်ရွက်ပေးနိုင်သည်။ အကျိုးဆက်အားဖြင့် cloud အခြေပြု စနစ်တစ်ခုတွင်

ရုပ်ပိုင်းဆိုင်ရာ လုံခြုံရေးထိန်းချုပ်မှုများသည် ပုံမှန်အားဖြင့် ICT ပတ်ဝန်းကျင်များရှိ ဆော့ဖ်ဝဲနှင့် နည်းပညာထက် ပို၍ အကြမ်းခံသည်။

ဖောက်သည် အချက်အလက်ဒ ရုပ်ပိုင်းဆိုင်ရာ လုံခြုံရေးသည် နိုင်ငံတကာစံနှုန်းများကို ရည်ညွှန်းခြင်းဖြင့် တရားဝင်ကြောင်းသက်သေ ပြနိုင်သည်။ ယခုအဆုံးသတ်တွင် အစိုးရ အချက်အလက်မန်နေဂျာတစ်ယောက်သည် Cloud Security Alliance's Cloud Controls Matrix v3.0(CSA CCM v3.0)[17] သို့မဟုတ် စံချိန်စံညွှန်းသတ်မှတ်ပေးရေး နိုင်ငံတကာ အဖွဲ့အစည်း၏ ISO/IEC 2770001[18] ကဲ့သို့ နိုင်ငံတကာ cloud နှင့် သတင်းအချက်အလက်စံနှုန်းများ လိုက်လျောမှုရှိ၊မရှိ ကြည့်နိုင်သည်။ နိုင်ငံတကာစံနှုန်းများနှင့် CSP လိုက်လျောညီထွေမှုကို လွတ်လပ်သော တတိယအဖွဲ့များတွင် စစ်ဆေးကြည့်ရှုနိုင်သည်။

နိုင်ငံတကာစံနှုန်းများနှင့် တတိယအဖွဲ့အစည်းများနှင့် ကိုးကားကြည့်ခြင်းဖြင့် အစိုးရ အချက်အလက်မန်နေဂျာတစ်ယောက်သည် ယင်းတို့ စာချုပ်ချုပ်ဆိုထားသော cloud ဝန်ဆောင်မှုများသည် လုံခြုံရေးနှင့် စိတ်ချယုံကြည်ရမှု ရှိသည့်အပေါ် ယုံကြည်လာနိုင်သည်။
အစိုးရအချက်အလက်မန်နေဂျာသည် ဝန်ဆောင်မှုရရှိနိုင်သော တာဝန်ယူမှုများအပါအဝင် မည်သည့် cloud SLAs များကို သေချာစေရန်စစ်ဆေးသင့်သည်။

ဖောက်သည်မှ တတိယအဖွဲ့အစည်းကို မယုံကြည်နိုင်သော သတင်းအချက်အလက်အချို့လည်း ရှိသည်။ ယင်းမှာ ပြင်ပရင်းမြစ်ဖြစ်သော ရုပ်ပိုင်းဆိုင်ရာလုံခြုံရေးထိန်းချုပ်မှု၊ ဥပမာ TOP SECRET အချက်အလက်။ ယခုနမူနာများတွင် cloud ဝန်ဆောင်မှုများသည် သင့်လျော်သော အဖြေမဖြစ်နိုင်ပါ။

လုံခြုံရေးထိန်းချုပ်မှုများကို အဓိပ္ပါယ်ဖွင့်ဆိုခြင်း

Cloud ပတ်ဝန်းကျင်တစ်ခုတွင် အစိုးရအချက်အလက်မန်နေဂျာတစ်ယောက်၏ ထိန်းချုပ်မှု အခြေခံမူဘောင်သည် လော့ဂျစ်ကယ်ထိန်းချုပ်မှုများအတွက် တာဝန်ရှိသည်။ ယင်းတို့မှာ

- အချက်အလက်အမျိုးအစားခွဲခြားခြင်း

[17] https://cloudsecurityalliance.org/download/cloud-controls-matrix-v3/
[18] http://www.iso.org/iso/home/standards/management-standards/iso27001.htm

- Cloud ပလက်ဖောင်းများနှင့် အက်ပလီကေးရှင်းများအတွက် အဓိပ္ပါယ်ဖွင့်ဆိုခြင်းနှင့် ဂင်ရောက်ထိန်းချုပ်မှုကို စောင့်ကြည့်ခြင်း
- သင့်လျော်သော အချက်အလက်စီမံခန့်ခွဲမှုနှင့် ပုက်စာသွင်းခြင်းကို အကောင်အထည်ဖော်ခြင်းနှင့် စောင့်ကြည့်လေ့လာခြင်း
- ဆော့ဖ်ဝဲလ်လုံခြုံရေးနှင့် ပက်သက်သော အန္တရာယ်များကို ကာကွယ်ခြင်း
- ပုဂ္ဂလိက လုံခြုံရေးကို စီမံခန့်ခွဲခြင်း
- Cloud စွမ်းဆောင်ရည်ကို စောင့်ကြည့်ခြင်း
- အစီအစဉ်ရေးဆွဲမှု ဆက်တိုက်လုပ်ခြင်း၊အဖြစ်အပျက် ထိန်းချုပ်ခြင်းနှင့် event logging ဆောင်ရွက်ခြင်း။

အသုံးများသော လော့ဂျစ်ကယ်လုံခြုံရေးထိန်းချုပ်မှု အသုံးများသော ဥပမာများမှာ အောက်ပါအတိုင်း ဖြစ်သည်။

- ပုက်စာသွင်းခြင်း အခြေခံကျသောလုံခြုံရေးထိန်းချုပ်မှုမှာ ပုက်စာသွင်းခြင်းဖြစ်သည်။ ပုက်စာသွင်းခြင်းကို အချက်အလက်က နားနေသည်ဖြစ်စေ၊ ရွှေ့ပြောင်းနေသည်ဖြစ်စေ အသုံးပြုသည်။ အမျိုးအစားသတ်မှတ်ချက်အရ တစ်သီးပုဂ္ဂလဖြစ်သော ဖိုင်များ သို့မဟုတ် ဖိုင်များအားလုံ သိုလှောင်ထားသော drive ကိုပုက်စာသွင်းခြင်းဖြင့် အချက်အလက် 'နားနေ'သည့်အခါ ပုက်စာသွင်းခြင်း ပိုမိုသင့်တော်သည်။ နေရာကူးပြောင်းနေသော အချက်အလက်ကို ပုက်စာသွင်းခြင်းဖြင့် 'လှုပ်ရှားနေသောဖိုင်' ကို ပုက်စာသွင်းရန်မှာလည်း အကောင်းဆုံးအလေ့အကျင့်ဖြစ်သည်။ ပုက်စာသွင်းထားသော"လှုပ်ရှားနေသော" အဓိပ္ပါယ်မှာ နေရာလွှဲပြောင်းနေသော အချက်အလက်အတွက် ပုက်စာသွင်းထားသော ချန်နယ်များကို အသုံးပြုခြင်းဖြစ်သည်။ [19]
- ပုက်စာဂင်ရောက်မှုထိန်းချုပ်ရေး အသုံးအများဆုံးဖြစ်သောဂင်ရောက်မှု ထိန်းချုပ်ရေးသည် အချက်အလက်ဂင်ရောက်မှု လုံခြုံရေးမြှင့်တင်ရန်အတွက် ပုက်စာအပေါ် အားထားရခြင်းဖြစ်သည်။
  - မည်သို့ဆိုစေ ရှည်လျားပြီး ရှုပ်ထွေးသောပုက်စာများကို ပြဋ္ဌာန်းခြင်းနှင့် မကြာခဏ ပုက်စာများ

[19]

ပြောင်းခြင်းသည် အန္တရာယ်ဖြစ်စေနိုင်သည်။ ယင်းအန္တရာယ်မှာ အသုံးပြုခွင့်ရှိသော အသုံးပြုသူများက ယင်းတို့၏ ပုဂ္ဂိုလ်ကို ကောင်းမွန်စွာမထိန်းသိမ်းခြင်း၊ ဥပမာ ပုဂ္ဂိုလ်ကို ချရေးထားခြင်း သို့မဟုတ် မလုံခြုံသော နေရာတွင် ထိန်းသိမ်းထားခြင်းများ ဖြစ်သည်။ ယင်းတို့၏ ရည်ရွယ်ထားသော ဦးတည်ချက်ကို ထမ်းဆောင်ရန် လုံခြုံရေးထိန်းချုပ်မှုအဖြစ် ပုဂ္ဂိုလ်၏ စွမ်းဆောင်မှုကို လျော့ကျစေသည်။

- • အဆင့်မြင့်တင်ထားသော ဝင်ရောက်မှုထိန်းချုပ်ရေး • ရှုပ်ထွေးသော ပုဂ္ဂိုလ်အစည်အလာများသို့ လူကြိုက်များသော အပြောင်းအလဲအဖြစ် ကဏ္ဍများ စွာပါသောမှန်ကန်ကြောင်း စစ်ဆေးပေးမှုများပေါ် ပေါက်လာခဲ့ပြီဖြစ်သည်။ ယင်းတွင် အသုံးပြုသူ၏ သီးခြားလက္ခဏာကို အတည်ပြုရန် အစိတ်အပိုင်းနှစ်မျိုးသို့မဟုတ် နှစ်မျိုးထက်ပိုသောဝင်ရောက်အသုံးပြုရန် စစ်ဆေးပေးမှုများ ပေါ် ပေါက်လာခဲ့ပြီဖြစ်သည်။ • အသုံးများသော ပုံစံများတွင်မရွေ့မပြောင်းသော PIN ကုဒ်၊ အသုံးပြုသူကို SMS မှပေးပို့သော ကုဒ်တစ်ခု၊ သို့မဟုတ် မိုဘိုင်းအက်ပလီကေးရှင်းမှဆောင်ရွက်ပေးသော ရွေ့လျားနေသော ပုဂ္ဂိုလ်စာတစ်ခု၊ သို့မဟုတ် တာဝန်ယူဆောင်ရွက်ပေးသော လုံခြုံရေးပစ္စည်း ကဲ့သို့ နှစ်ခု သို့မဟုတ် နှစ်ခုထက်ပိုသော အကြောင်းအရာများ ပေါင်းစပ်ခြင်းတို့ပါဝင်သည်။
- ဝင်ရောက်မှု(Log-in) စောင့်ကြည့်ခြင်း • အချက်အလက်မန်နေဂျာများသည် ဝင်ရောက်မှုများ၊စစ်မှန်ကြောင်းသက်သေပြမှုများ(authentication) ကို တက်ကြွစွာ စောင့်ကြည့်နေရမည်ဖြစ်ပြီး သုံးစွဲခွင့်မရှိသူများက ဝင်ရောက်ရန်ကြိုးပမ်းခြင်းများကို စစ်ဆေးရန် အလိုအလျောက်၊အန္တရာယ်အခြေပြု လုပ်ငန်းလည်ပတ်စေမှုများကို အကောင်အထည်ဖော်ရမည်ဖြစ်သည်။ အခြားလုံခြုံရေးထိန်းချုပ်မှုများတွင်ဝင်ရောက်မှု အခန်းကဏ္ဍများကိုကန့်သတ်ခြင်း၊ အသုံးပြုမှု မရှိသည့် ကြိုတင်သတ်မှတ်အချိန်အရောက်တွင်အလိုအလျောက် ပြန်ထွက်(log out)ခြင်းနှင့် အချိန်ပြည့် ဝင်ရောက်ထားခြင်း(login) ကို ခွင့်မပြုခြင်းတို့ပါဝင်သည်။
- ဝင်ရောက်မှုစစ်ဆေးခြင်း အချက်အလက်သို့ဝင်ရောက်မှု စစ်ဆေးခြင်းသည် ရည်ရွယ်ချက်နှစ်ခုကို ထမ်းဆောင်နိုင်သည်။ ပုံမှန်စစ်ဆေးမှုများသည် ကျိုးပေါက်သည့်ရင်းမြစ်သို့မဟုတ် ထုတ်ဖော်ချက်ကို ခွဲခြားဖော်ထုတ်ရန် မူခင်းဆေးပညာကိရိယာတန်ဆာပလာတစ်ခုကဲ့သို့ မကြာသေးခင်ကဖြစ်ခဲ့သည့် အမျိုးအမည်ခွဲခြားမရနိုင်သော ကျိုးပေါက်သည့်နေရာကို

ရှာဖွေရာတွင် အကူအညီပေးခြင်းနှင့် ကျိုးပေါက်ခြင်း၏ တိကျသော ဖြစ်ရပ်များကို ရှာဖွေရာတွင် အကူအညီပေးသည်။

သင့်လျော်သော အတိုင်းအတာများကို ဆုံးဖြတ်ခြင်းသည် ၎နှင့်ဆောင်မှုအသုံးပြုခြင်းအပေါ် အနှုတ်သဘောဆောင် သက်ရောက်မှုမရှိကြောင်းသေချာစေသင့်သည်။ [20]

လုံခြုံရေးထိန်းချုပ်မှု အခြေခံမူဘောင်နှင့် ဆွေးနွေးခဲ့သကဲ့သို့ လုံခြုံရေးထိန်းချုပ်မှုသည် အမျိုးအစားနှစ်ခုတွင် ကိုက်ညီရမည်။ ရုပ်ပိုင်းဆိုင်ရာနှင့် လော့ဂျစ်ကယ် ထိန်းချုပ်မှုများ ရုပ်ပိုင်းဆိုင်ရာထိန်းချုပ်မှုများသည် CSP ၏တာ၎နှင်ဖြစ်ပြီး အစိုးရ အချက်အလက်မန်နေဂျာနှင့် CSP ကြားမှ ၎နဆောင်မှု သဘောတူညီချက်အဆင့် (SLA) တွင်ဖော်ပြရမည်။

အချက်အလက်အမျိုးအစားခွဲခြားခြင်းနှင့် လုံခြုံရေးထိန်းချုပ်မှုများကို ချိန်ညှိခြင်း

ယခုအကြောင်းအရာကို ယခုမူဂါဒ၏ အခန်း ၅ တွင်ဆွေးနွေးခဲ့ပြီးဖြစ်သည်။ လျှို့ဝှက် သို့မဟုတ် ထိပ်တန်းလျှို့ဝှက် အချက်အလက်သည် ပို၍ တင်းကြပ်သော လုံခြုံရေးစံနှုန်းများလိုအပ်ပြီး အထွေထွေ အဖြစ် အမျိုးအစားခွဲခြားသတ်မှတ်ခံထားရသော အချက်အလက်မှာ အခြေခံလုံခြုံရေးထိန်းချုပ်မှုများသာ လိုအပ်သည်။ [2122] အချက်အလက်အမျိုးအစားခွဲခြားသတ်မှတ်ခြင်းတစ်ခုစီတိုင်းအတွက် အနည်းဆုံး လုံခြုံရေးလိုအပ်ချက်၏ အဓိပ္ပါယ်ဖွင့်ဆိုချက်တွင် နိုင်ငံတကာစံနှုန်းများကို ရည်ညွှန်းခြင်းသည် ဖောက်သည်အား သတင်းအချက်အလက်နှင့် လိုအပ်သော ထိန်းချုပ်မှု အဆင့်အတန်း ကိုက်ညီမှုရှိသော cloud ၎နဆောင်မှုများကို အလွယ်တကူ ရရှိစေရန် ကူညီနိုင်သည်။

အချက်အလက်ခွဲခြားသတ်မှတ်ခြင်း အခြေပြု လုံခြုံရေးလိုအပ်ချက်များကို ချိန်ညှိခြင်းသည် အချက်အလက်စီမံခန့်ခွဲမှုကို လျော့ကျစေကာ အဖွဲ့အစည်းတစ်ခုအတွင်း၊ မတူညီသော အဖွဲ့အစည်းများအကြား သတင်းအချက်အလက်များ မျှဝေခြင်းနှင့် ပိုမိုထိရောက်စွာ အသုံးပြုခြင်းဖြစ်စေကာ အချက်အလက်ကို သင့်လျော်စွာ လုံခြုံစေရန်ကူညီပေးသည်။

[20] UK Cloud Service Security Principles (Beta) မှဖြည့်စွက်ချက်။ အောက်တွင်ရှုပါ။ https://www.gov.uk/government/publications/cloud-service-security-principles/cloud-service-security-principles

[21] http://www.iso.org/iso/home/standards/management-standards/iso27001.htm

[22] http://www.iso27001security.com/html/27017.html

Cloud Platforms

Cloud အခြေခံအားဖြင့် အချက်အလက်များအား ဖတ်ရှုနိုင်ခွင့်၊ ပြုပြင်နိုင်ခွင့် သို့မဟုတ် ဖျက်သိမ်းနိုင်ခွင့် စသော ရယူနိုင်ခွင့် အမျိုးအစားများအား အချက်အလက်ဆိုင်ရာ ရယူခွင့် မူဝါဒ (Data access policy) အရ အစိုးရ၏ အချက်အလက်ဆိုင်ရာ စီမံခန့်ခွဲသူသည် ခွင့်ပြုချက်များအား ရယူလုပ်ဆောင်နိုင်သည်။

အစိုးရ၏ အချက်အလက်ဆိုင်ရာ စီမံခန့်ခွဲသူသည် လိုအပ်သလို အချက်အလက်ရယူပိုင်ခွင့်များအား ပေးအပ်၊စီမံ၊ ရုပ်သိမ်းနိုင်ခွင့်ရှိပြီး လုပ်ဆောင်ခွင့်များအား အချိန်နှင့် တပြေးညီ ထိန်းသိမ်းထားခြင်းအတွက် တာဝန်ရှိသည်။ အစိုးရ၏ အချက်အလက်ဆိုင်ရာ စီမံခန့်ခွဲသူသည် အချက်အလက်များအား မည်သို့အသုံးပြုနေသည် သာမက Cloud အတွင်းရှိ အချက်အလက်များအား စီမံရန်အတွက် မည်သည့် လုပ်ဆောင်မှုစနစ်များ (Operation systems) နှင့် ဆော့ဖ်ဝဲလ်များ အသုံးပြုသည်ကိုလည်း ထိန်းချုပ်နိုင်မည်။

အစိုးရ၏ အချက်အလက်ဆိုင်ရာ စီမံခန့်ခွဲသူသည် ခွင့်ပြုချက်များအတွက် တာဝန်ရှိပြီး အလုပ်တာဝန်များ လုပ်ဆောင်ရန် သို့မဟုတ် ပြည်သူလူထု သတင်းအချက်အလက် ရယူပိုင်ခွင့် စသော အခြေအနေများတွင် အချက်အလက်လိုအပ်နေသော သူများအား အချက်အလက်အရင်းအမြစ်များ ရရှိစေရန်အတွက် အချက်အလက်ရယူခွင့် စာရင်းများ(Data access lists)အား အမြဲမပြတ် စီမံလုပ်ဆောင်ရန်မည်ဖြစ်သည်။ လူထုအနေဖြင့် တားမြစ်ထားသော အချက်အလက်များအား ရယူနိုင်ခြင်းမရှိစေရန်နှင့် တချို့သော အချက်အလက်များအား မရယူစေရန်အတွက်လည်း စာရင်းများအား စီမံခန့်ခွဲရမည်ဖြစ်သည်။

ကုတ်အဖြစ်ပြောင်းလဲခြင်း (Encryption) ကဲ့သို့သော သင့်လျော်ရာ အချက်အလက်စီမံခန့်ခွဲမှု စနစ်များအား အသုံးချခြင်းနှင့် လုပ်ဆောင်ခြင်း
အစိုးရ၏ အချက်အလက်ဆိုင်ရာ စီမံခန့်ခွဲသူသည် အချက်အလက်များ လွှဲပြောင်းခြင်း၊ သိမ်းဆည်းခြင်းနှင့် ရယူခြင်းများ လုပ်ဆောင်စဉ်အတွင်း လုံခြုံရေးဆိုင်ရာလုပ်ဆောင်ချက် ထိန်းချုပ်ခြင်းများအား ရွေးချယ်နိုင်မည်။ ထို ထိန်းချုပ်မှုများအား မတူညီသော အချက်အလက် အမျိုးအစားခွဲခြားမှုများအတွက် မတူညီသော လုံခြုံရေး သတ်မှတ်ချက်များနှင့် အညီ ပြဋ္ဌာန်းဖော်ပြထားပါသည်။
အမျိုးအစားခွဲခြားမှုများပေါ်တွင်မူတည်၍ ထိုထိန်းချုပ်မှုများတွင် ဖိုင်တစ်ခုချင်းစီကို

ကုတ်အဖြစ်ပြောင်းလဲကာ "တည်ငြိမ်သောအခြေအနေ" (At rest) ရှိအချက်အလက်များအား ကုတ်အဖြစ်ပြောင်းလဲခြင်း (Encrypting) သို့မဟုတ် ဖိုင်များ သိမ်းဆည်းထားသော Drive တစ်ခုလုံးနှင့် "ရွှေ့လျားအခြေအနေ" (At motion) ရှိ ဖိုင်များအားအား ကုတ်အဖြစ်ပြောင်းလဲခြင်း ၊ အကူးအပြောင်းလုပ်ဆောင်နေသော အချက်အလက်များအား ကုတ်အဖြစ်ပြောင်းလဲခြင်း (Encrypting) နှင့် မူလအခြေအနေသို့ ပြန်လည်ပြောင်းလဲခြင်း (Decrypting) တို့ပါဝင်ပါသည်။

အစိုးရ၏ အချက်အလက်ဆိုင်ရာ စီမံခန့်ခွဲသူသည် အချက်အလက်များ မည်သည့်နေရာတွင် ထားရှိသွားမည်ဟူသော ဆုံးဖြတ်ခွင့်ကို ရွေးချယ်ခြင်းအပါအဝင် အချက်အလက်များ သိမ်းဆည်းသောနေရာအား ရွေးချယ်နိုင်သည်။ အချက်အလက်များလွှဲပြောင်းရာနေရာ (Cross broder data transfers) ရှိ ကန့်သတ်မှုများအဖြစ် ယူဆနိုင်သော ပုဂ္ဂိုလ်ရေးဆိုင်ရာ သတင်းအချက်အလက်များ သို့မဟုတ် တခြား အချက်အလက်များအား လွှဲပြောင်းသည့် Cloud အသုံးပြုသူများအတွက် ထိုအချက်အလက်များအား CSP တွင် သိမ်းဆည်း၍ စနစ်တကျလုပ်ဆောင်ကာ လိုအပ်သော စည်းမျည်းစည်းကမ်းများ၊ဖော်ပြချက်များနှင့် ကိုက်ညီမှုရှိစေရမည်ဖြစ်သည်။ ဥပမာအားဖြင့် Cloud အသုံးပြုသူတစ်ယောက်အနေဖြင့် ဥရောပသမဂ္ဂမှ စင်ကာပူသို့ အချက်အလက်များလွှဲပြောင်းသည့်အခါတွင် ထိုသူတို့၏ CPS သည် ဥရောပသမဂ္ဂ၏ စည်းမျည်းစည်းကမ်းများနှင့် ကိုက်ညီမှုရှိကြောင်းသာမက လိုအပ်သည့်အလျောက် ဥရောပသမဂ္ဂမှ ဥရောပသမဂ္ဂမဟုတ်သော နိုင်ငံများသို့ ပုဂ္ဂိုလ်ရေးအချက်အလက်လွှဲပြောင်းခြင်းဆိုင်ရာ ဆုံးဖြတ်ချက်အတွက် ဥရောပသမဂ္ဂ၏ အချက်အလက်ကာကွယ်ရေးဆိုင်ရာ တာဝန်ရှိသူ၏ ထောက်ခံချက်ပါ ဖော်ပြရမည်ဖြစ်သည်။

အစိုးရ၏ အချက်အလက်ဆိုင်ရာ စီမံခန့်ခွဲသူသည် အချက်အလက်များ သိမ်းဆည်းမည့်၊ စနစ်တကျလုပ်ဆောင်မည့်၊ စီမံခန့်ခွဲမည့် နေရာအား ထုတ်ဖော်ရန်အတွက် လိုအပ်သော CPS များအားရွေးချယ်ရန်လိုအပ်ပါသည်။ ထိုမှသာ Cloud အသုံးပြုသူက သူတို့၏ အချက်အလက်များသည် မည်သည့်ဆုံးဖြတ်ချက်အရ သတ်မှတ်ထားသည်၊ အစိုးရတာဝန်ရှိသူကဲ့သို့သော ပုဂ္ဂိုလ်များက

သူတို့၏ခွင့်ပြုချက်မပါရှိဘဲ မည်သည့်အချက်အလက်များအားရယူနိုင်သည်ဟူသော စည်းမျဉ်းများအား သဘောပေါက်နားလည်နိုင်မည်ဖြစ်သည်။[23]

အစိုးရ၏ အချက်အလက်ဆိုင်ရာ စီမံခန့်ခွဲသူသည် အချက်အလက်များ မည်သို့လွှဲပြောင်းမည်နှင့် သိမ်းဆည်းမည်ကို ထိန်းချုပ်နိုင်သည်။ ထိုအပိုင်းတွင် အချက်အလက်များ အစမှအဆုံးအထိ ကုတ်အဖြစ်ပြောင်းလဲရန် သို့မဟုတ် သိမ်းဆည်းမှသာ ကုတ်အဖြစ်ပြောင်းလဲရန် လိုအပ်ခြင်းရှိမရှိ ၊ မူလအချက်အလက်များ မလွှဲပြောင်းမီနှင့် လုပ်ဆောင်ခြင်းမပြုမီ တူညီသော မူလပုံစံမဟုတ်သည့် ပုံစံအားဖြစ်စေသော အချက်အလက်အကာအကွယ် (data masking) လိုအပ်ခြင်းရှိမရှိနှင့် အချက်အလက်များ မလွှဲပြောင်းမီ သို့မဟုတ် လုပ်ဆောင်ခြင်းမပြုမီ ပုဂ္ဂိုလ်ဆိုင်ရာ ဖော်ပြချက်များအားလုံးအား ဖယ်ထုတ်ကာ အချက်အလက်များအား အမည်မဖော်ပြခြင်းလုပ်ဆောင်ရန် လိုအပ်ခြင်းရှိမရှိ စသည့် ဆုံးဖြတ်ခြင်းများ ပါဝင်သည်။

လွှဲပြောင်းသော အချက်အလက်များအတွက် ကုတ်အဖြစ်ပြောင်းလဲသော နည်းလမ်းများအား အသုံးပြုကာ အချက်အလက်များအား ရွှေ့လျားအခြေအနေ (In motion) ၌ ကုတ်အဖြစ်ပြောင်းလဲသွားမည်ဖြစ်သည်။ ဂက်ဆိုက်အခြေပြုကူးပြောင်းမှုများအတွင် ယုံကြည်စိတ်ချရသော ရောင်းချသူထံမှ တတိယအဖွဲ့အစည်း အသိအမှတ်ပြုလက်မှတ်ကို အသုံးပြုပြီးအကောင်အထည်ဖော်ပုက်စာသွင်းခြင်းကို ပေါ်လွင်စေသည်။[24] အချက်အလက်များလွှဲပြောင်းရန်အတွက် လုံခြုံစိတ်ချသော၊ ကုတ်အဖြစ်ပြောင်းလဲသော လမ်းကြောင်းအား အသုံးပြုမှုများ တိုးတက်လာသဖြင့် လုပ်ဆောင်မှု၏ အကျိုးဆက်များအား လျစ်လျူနိုင်ကာ အချက်အလက်များသည်လည်း ပိုပြီးလုံခြုံလာပါသည်။ နိုင်ငံသားများ၏ အချက်အလက်လွှဲပြောင်းသည့် နက်ဂေါ့ခ်များအား စမ်းသပ်ခိုးယူခြင်းနှင့် ကြားဖြတ်ရယူခြင်းများ မဖြစ်စေရန် နက်ဂေါ့ခ်အကာအကွယ်များနှင့် ကုတ်အဖြစ်ပြောင်းလဲခြင်းတို့အား ပေါင်းစပ်ကာ လုံလောက်စွာ ကာကွယ်ထားရမည်ဖြစ်သည်။ အကယ်၍ ယခုစည်းမျဉ်းအား မဖော်ဆောင်နိုင်ပါက ကူးပြောင်းရာတွင် အချက်အလက်များ၏ ပြည့်စုံမှု သို့မဟုတ် လုံခြုံစိတ်ချမှုအား ထိခိုက်စေမည်ဖြစ်သည်။[25]

[23] ဗြိတိန်နိုင်ငံ၏ "Cloud လုံခြုံရေး စည်းမျဉ်းများ" (Cloud Security Principles) တွင် ထိုသဘောတရားကို အကြံပြုဖော်ပြထားပါသည်။ ကြည့်ရှုရန် - https://www.gov.uk/government/publications/cloud-service-security-principles/cloud-service-security-principles

[24] "https" တွင် 's' ရလဒ်များမှာ ဂက်ဆိုက်လိပ်စာများပေါ်တွင် https://www.domain-name.com/ ကဲ့သို့ပေါ်လာမည်။

[25] ဗြိတိန်နိုင်ငံ Cloud ဂန်ဆောင်မှု၏ လုံခြုံရေးစည်းမျဉ်းများ (Beta) မှ ကောက်နှုတ်ထားပါသည်။ ကြည့်ရှုရန် - https://www.gov.uk/government/publications/cloud-service-security-principles/cloud-service-security-principles

ဆော့ဖ်ဝဲလုံခြုံရေးနှင့်ဆက်စပ်နေသည့် အန္တရာယ်များအား ကြိုတင်ကာကွယ်ခြင်း

အစိုးရ၏ အချက်အလက်ဆိုင်ရာ စီမံခန့်ခွဲသူသည် Cloud အသုံးပြုသူအနေဖြင့် Cloud တွင် ထည့်သွင်းထားသော လုပ်ဆောင်မှုစနစ်များ (Operation systems) နှင့် ဆော့ဖ်ဝဲများအတွက် ထိန်းချုပ်မှုနှင့် တာဝန်များအား ထိန်းသိမ်းရမည်ဖြစ်သည်။ ဆော့ဖ်ဝဲလုံခြုံရေးနှင့် ဆက်စပ်နေသည့် အန္တရာယ်များ လျော့နည်းစေရန်အတွက် Cloud တွင် အသုံးပြုနေသော လုပ်ဆောင်မှုစနစ်များ (Operation systems) နှင့် အသုံးချဆော့ဖ်ဝဲများအား အဆင့်မြှင့်တင်ခြင်းနှင့် လုံခြုံရေးအကာအကွယ်များအား ပုံမှန်ထည့်သွင်းခြင်းကို Cloud အသုံးပြုသူသည် ပုံမှန်လုပ်ဆောင်ရမည်ဖြစ်သည်။

အိမ်တွင်းအသုံးပြု ICT စနစ်ရှိ လုပ်ဆောင်မှု စနစ်များနှင့် ဆော့ဖ်ဝဲများရှိ အချက်အလက်များအား တရားဝင်မဟုတ်သော ပြင်ပအဖွဲ့အစည်းများမှနေ၍ ခိုးယူနိုင်သကဲ့သို့ Cloud ၏ ခေတ်မမှီသော လုပ်ဆောင်မှုစနစ်များနှင့် ဆော့ဖ်ဝဲများရှိ အချက်အလက်များသည်လည်း ခိုးယူခံရနိုင်ပါသည်။ Cloud အသုံးပြုသူသည် ဒေသတွင်း ဆာဗာများ (Servers) နှင့် အလုပ်ရုံများတွင် အသုံးပြုသော လုံခြုံရေးနည်းလမ်းများအတိုင်း Cloud တွင်ထည့်သွင်းထားသော အသုံးပြုဆော့ဖ်ဝဲအားလုံးကို စီမံခန့်ခွဲရမည်ဖြစ်သည်။

ပုဂ္ဂိုလ်ရေး လုံခြုံမှု စီမံခန့်ခွဲခြင်း

ICT စနစ်အား တရားဝင်ဝင်ရောက်နိုင်သော အဖွဲ့အစည်းအတွင်းသူ (Trusted Insider) သည် အစိုးရဆိုင်ရာ လုပ်ငန်းများနှင့် စီးပွားရေးလုပ်ငန်းများရှိ အဖွဲ့အစည်းအား အကြီးများဆုံး အန္တရာယ်ပေးနိုင်သော အရာတစ်ခုဖြစ်သည်။ ပြင်ပအဖွဲ့အစည်းမှနေ၍ တရားမဝင် သတင်းအချက်အလက်များရယူရန် ယုံကြည်ရသောဝန်ထမ်းများကို ပစ်မှတ်ထားခံရနိုင်ခြင်း သို့မဟုတ် ငွေကြေးကဲ့သို့ ဆွဲဆောင်မှုကြောင့် ဝန်ထမ်းများကိုယ်တိုင်က ကန့်သတ်ထားသော သတင်းအချက်အလက်များအား ရယူကာ ပြင်ပအဖွဲ့အစည်းများထံသို့ မျှဝေခြင်း ဖြစ်လာနိုင်ပါသည်။

ပုဂ္ဂိုလ်၏ လုံခြုံရေး အန္တရာယ်များအား စီမံရန်အတွက် အစိုးရ၏ အချက်အလက်ဆိုင်ရာတာဝန်ရှိသူသည် တူညီသော လူပုဂ္ဂိုလ်ဆိုင်ရာ စစ်ဆေးမှုများနှင့် အရေးကြီးသော တာဝန်များအား အထူးဝင်ရောက်ခွင့်ရရှိသော ဝန်ထမ်းများကို စောင့်ကြည့်ခြင်းများကို

အလေးထားလုပ်ဆောင်ရမည်ဖြစ်သည်။ ဤအပိုင်းတွင် ပန်ထမ်းအသစ်များအား အဆင့်တစ်ခုထားကာ စောင့်ကြည့်ခြင်း၊ ပန်ထမ်းများ၏ ဆက်လက်လုပ်ကိုင်နေသော အလုပ်များအား ကြည့်ရှုကာ ပန်ထမ်းဆိုင်ရာ ပြန်လည်ဆန်းစစ်ချက်များ လုပ်ဆောင်ခြင်းနှင့် သင့်လျော်ရာ လုံခြုံရေးနှင့် အရေးပေါ်ဆိုင်ရာ အသိပေးချက် လေ့ကျင့်မှုများ ဆောင်ရွက်ပေးခြင်းတို့ ပါဝင်သည်။ ပုဂ္ဂိုလ်ရေး လုံခြုံမှု စီမံခန့်ခွဲခြင်းသည် ပန်ထမ်းများသာမက အဖွဲ့အစည်း၏ သတင်းအချက်အလက်နှင့် အရေးကြီးသော လုပ်ငန်းဆောင်တာများအား ကာကွယ်ရာတွင် ကူညီနိုင်မည်ဖြစ်သည်။ Phishing' တိုက်ခိုက်မှုများအား တားဆီးခြင်းကဲ့သို့သော အွန်လိုင်းလုံခြုံရေးအတွက် အကောင်းဆုံးလုပ်ဆောင်မှုများအား လေ့ကျင့်ပေးရောတွင် အကြံပြုညွှန်ကြားထားသော အကောင်းဆုံးလုပ်ဆောင်မှုများနှင့် ကိုက်ညီမှုရှိစေရန်အတွက် ပုံမှန် လေ့ကျင့်ခန်းများ၊ စမ်းသပ်မှုများ၊ ကျပန်းလေ့ကျင့်ခန်းများ၊ စမ်းသပ်မှုများနှင့်အတူ လေ့ကျင့်ခြင်း။

Cloud ၏ စွမ်းဆောင်ရည်အား စောင့်ကြည့်ခြင်း။

လုံခြုံရေးထိန်းချုပ်မှုများ ဖော်ပြသတ်မှတ်ကာ လုပ်ဆောင်ပြီးသည်နှင့် တစ်ပြိုင်နက် အစိုးရ၏ အချက်အလက်ဆိုင်ရာ စီမံခန့်ခွဲသူ၏ အဖွဲ့သည် အစဉ်မပြတ် ထိရောက်စွာလုပ်ဆောင်နိုင်ခြင်းများအတွက် Cloud ၏ စွမ်းဆောင်ရည်အား စောင့်ကြည့်ရမည်ဖြစ်သည်။

ထိရောက်သောလုပ်ဆောင်မှုလုပ်ဆောင်နိုင်ရန်အတွက် သင့်လျော်ရာ မူဝါဒများနှင့် CSP ရှိ ကိရိယာများအား ပင်ရောက်နိုင်ခွင့်ရှိသ၍ မည်သည့်အစိုးရ အဖွဲ့အစည်းမဆို Cloud အသုံးပြုသူအနေဖြင့် ထိုသူတို့၏ လုံခြုံရေး ထိန်းချုပ်မှုများ၏ ထိရောက်မှုများအား စီမံခန့်ခွဲခြင်းနှင့် စောင့်ကြည့်ခြင်း လုပ်ဆောင်နိုင်မည်ဖြစ်သည်။ အသုံးပြုသူများအတွက် ဆိုလိုသည်မှာ -

1. ပန်ဆောင်မှုအား လုံခြုံစွာ စီမံခန့်ခွဲရန်အတွက် လိုအပ်သော ကိရိယာများအား ထောက်ပံ့ပေးခြင်း
2. ပန်ဆောင်မှု၏ ပြင်ပ သို့မဟုတ် ယုံကြည်စိတ်ချခြင်းမရှိသော စနစ်အားလုံးအား ဖော်ထုတ်သတ်မှတ်ထားပြီး ထိုအခြေအနေများမှတဆင့် တိုက်ခိုက်မှုများအား ကာကွယ်ရန်အတွက် သင့်လျော်သော ကာကွယ်မှုများ လုပ်ဆောင်ထားခြင်းနှင့်
3. သူတို့၏ ပန်ဆောင်မှုနှင့် ထိုအထဲတွင်ပါဝင်သော အချက်အလက်များအား စောင့်ကြည့်ရယူနိုင်ရန်အတွက် လိုအပ်သော စစ်ဆေးမှု မှတ်တမ်းများအား ထောက်ပံ့ပေးခြင်း။

အစိုးရအဖွဲ့အစည်းအတွင်း သတ်မှတ်ဖော်ပြထားသော ဆက်စပ်ကဏ္ဍများတွင် လိုအပ်သည့် ထိရောက်သော စောင့်ကြည့်လေ့လာရေး မူဘောင်အား လုပ်ဆောင်ခြင်း။ ထိန်းချုပ်မှုဆိုင်ရာ မူဘောင်၏ အစိတ်အပိုင်းများအား သတ်မှတ်ဖော်ပြခြင်း၊ လုပ်ဆောင်ခြင်းနှင့် စောင့်ကြည့်ခြင်း ကဏ္ဍတစ်ခုခြင်းစီတွင် သက်ဆိုင်ရာ တစ်ဦးတစ်ယောက်ချင်းစီ သို့မဟုတ် အဖွဲ့အလိုက် တာဝန်များခွဲဝေပေးရန် လိုအပ်သည်။ ရှင်းလင်းစွာ ဖော်ပြရသော် -

- အချက်အလက်အသစ်များအား အမျိုးအစားခွဲခြားသတ်မှတ်ရန်အတွက် မည်သူ တာဝန်ယူလုပ်ဆောင်မည်နည်း။
- အချက်အလက်များအား စီမံခန့်ခွဲရန်အတွက် မည်သူ တာဝန်ယူလုပ်ဆောင်မည်နည်း။
- အချက်အလက်များရယူခွင့်အား စီမံခန့်ခွဲရန်အတွက် မည်သူ တာဝန်ယူလုပ်ဆောင်မည်နည်း။
- Cloud ဝန်ဆောင်မှုဆိုင်ရာ စွမ်းဆောင်ရည်အား စောင့်ကြည့်ရန်နှင့် ပြန်လည်တင်ပြရန်အတွက် မည်သူတာဝန်ယူလုပ်ဆောင်မည်နည်း။

အထက်စီမံခန့်ခွဲမှုရှိ ရှင်းလင်းစွာ သတ်မှတ်ဖော်ပြထားသော ကိုယ်စားလှယ်၊ အဖွဲ့အစည်းအတွက် အစိုးရ၏ အချက်အလက်ဆိုင်ရာတာဝန်ရှိသူ၏ အောက်တွင်ရှိသော သူတို့၏ ယေဘူယျချည်းကပ်နည်းများအတိုင်း သက်ဆိုင်ရာ တစ်ဦးတစ်ယောက်ချင်းစီနှင့် အသင်းများသည် တင်ပြကာ ပေါင်းစည်းလုပ်ဆောင်ရမည်ဖြစ်သည်။ ဝန်ဆောင်မှုရရှိနိုင်မှု၊ နက်ဝေါ်ခ် စွမ်းဆောင်ရည်၊ အချက်အလက်ရရှိနိုင်မှုနှင့် အချက်အလက်များ ပေါက်ကြားနိုင်မှုကဲ့သို့သော Cloud ၏ စွမ်းဆောင်ရည်များ၏ ကဏ္ဍများအား စောင့်ကြည့်ရန်အတွက် Cloud ၏ စွမ်းဆောင်ရည်အတွက် တာဝန်ရှိသော လူပုဂ္ဂိုလ် သို့မဟုတ် အဖွဲ့သည် CSP မှ လိုအပ်သော ကိရိယာများနှင့် မှတ်တမ်းများအား ရယူရမည်ဖြစ်သည်။

စွမ်းဆောင်ရည်အား အဖွဲ့အစည်း၏ တောင်းဆိုမှုများအရ နှိုင်းယှဉ်ကြည့်နိုင်ပြီး လိုအပ်သော ငွေကြေးအခြေခံ၊ ဘဏ္ဍာငွေစာရင်းနှင့် အကဲဖြတ်ခြင်းဆိုင်ရာရှိ တာဝန်ယူအဖွဲ့များဆီသို့ ပုံမှန်တင်ပြရမည်ဖြစ်သည်။ ဤသို့ပြုလုပ်ခြင်းဖြင့် ICT ကဏ္ဍများအား တခြား အသုံးပြုဆော့ဖ်ဝဲ ဝန်ဆောင်မှုများနှင့် လွှဲပြောင်းဝန်ဆောင်မှုများကဲ့သို့ပင် စီမံခန့်ခွဲမှုနှင့် ရယူအသုံးခွင့်ရှိစေရန် လုပ်ဆောင်နိုင်မည်ဖြစ်ပြီး အဖွဲ့အစည်း၏လိုအပ်ချက်များအား ပြည့်မှီစေရန်အတွက် ICT နည်းပညာအား

တဖြည်းဖြည်း အဆင့်မြှင့်တင်နိုင်မည်ဖြစ်သည်။ ဤသို့လုပ်ဆောင်ခြင်းသည် အဖွဲ့အစည်း၏ ICT ကဏ္ဍအသစ်များအသုံးချခြင်းကို အထောက်အကူဖြစ်စေကာ အသစ်အသစ်သော ဝန်ဆောင်မှု သို့မဟုတ် ပိုကောင်းသော ဝန်ဆောင်မှုများအား တိုးတက်စေမည်ဖြစ်သည်။

လုံခြုံရေးထိန်းချုပ်မှု အမျိုးအစားများရှိ အန္တရာယ် စစ်ဆေးခြင်းနှင့် ပေါင်းစည်းမှု အမျိုးအစားခွဲခြားခြင်းများ

အန္တရာယ်စစ်ဆေးခြင်း (Risk assesment)တွင် အစိတ်အပိုင်း (၄) ခုပါဝင်ပေသည်။

1. အဖွဲ့အစည်းတွင်း အန္တရာယ်အား ထည့်သွင်းစဉ်းစားခြင်း - ပုဂ္ဂိုလ်ဆိုင်ရာ၊ လုပ်ဆောင်မှုများဆိုင်ရာ၊ စီးပွားရေး ဆုံးရှုံးမှုဆိုင်ရာ၊ အမျိုးသားလုံခြုံရေးဆိုင်ရာ အန္တရာယ်များ
2. အချက်အလက်များ ပေါက်ကြားခြင်း အန္တရာယ်အား ထည့်သွင်းစဉ်းစားခြင်း - ပြင်ပအဖွဲ့အစည်းတစ်ခုမှနေ၍ အချက်အလက်များ လိုအပ်တောင်းခံခြင်းသည် တခြားပြင်ပအဖွဲ့များမှ ထည့်သွင်းစဉ်းစားထားသော အချက်အလက်များအား ရရှာဖွေရယူခြင်းကဲ့သို့သော မြင့်မားသည့် အန္တရာယ်ကို ဖြစ်စေသည်။
3. လုံခြုံစိတ်ချမှု၊ ပြည့်စုံမှုနှင့် အဆင်သင့်ရရှိနိုင်မှုဟူသော သတ်မှတ်ချက် (၃) ခုအလိုက် အန္တရာယ်အဆင့်များအား အဆင့်မြင့်၊ အလယ်အဆင့်နှင့် အဆင့်နိမ့်ဟူ၍ ခွဲခြားထားရမည်ဖြစ်ပြီး
4. (၁)၊ (၂) နှင့် (၃) အပေါ်အခြေခံ၍ သင့်လျော်ရာ လုံခြုံရေး ထိန်းချုပ်မှုများကို ဆုံးဖြတ်ရမည်။ ဖော်ပြထားသော အန္တရာများအပေါ်အခြေခံ၍ မည်သည်တို့သည် သင့်လျော်သော၊ လက်တွေ့ကျသော လုံခြုံရေး ထိန်းချုပ်မှုများဖြစ်သည်နည်း။

Cloud အဓိကသုံးသည့် ICT အခြေအနေတစ်ခုတွင် Cloud သို့ပြောင်းရွှေ့သည့် နေရာမှစ၍ အန္တရာယ်စစ်ဆေးခြင်းကို လုပ်ဆောင်ရမည်ဖြစ်သည်။ Cloud အသုံးပြုသူသည် Cloud သို့ပြောင်းရွှေ့နေသည့် အချက်အလက်များနှင့် ဆက်စပ်နေသော အန္တရာယ်များအား ဆုံးဖြတ်ရမည်ဖြစ်ပြီး အချက်အလက်ခွဲခြားခြင်းနည်းစနစ် (Data classification taxonomy)ရှိ ရည်ညွှန်းကိုးကားချက်နှင့် အညီ အချက်အလက်များအား အမျိုးအစားခွဲရမည်ဖြစ်သည်။

အချက်အလက်များ Cloud အတွင်းသို့ရောက်ရှိပါက Cloud အသုံးပြုသူသည် ၎င်းတို့၏ ရည်ရွယ်ချက်အား စနစ်အတွင်းရှိ လုံခြုံရေးထိန်းချုပ်မှုများက ဖော်ဆောင်နိုင်ခြင်းရှိမရှိ၊ ၎င်းတို့လုပ်ဆောင်ရန်

စီစဉ်ထားသည့်အရာကို လုပ်ဆောင်နိုင်ခြင်းရှိမရှိနှင့် စနစ်အတွင်းရှိ လုံခြုံရေးထိန်းချုပ်မှုများသည် အလွယ်တကူ သယ်ဆောင်နိုင်ခြင်းရှိမရှိ၊ ကိစ္စအများတွင် ဆက်တိုက်အသုံးခြင်းအတွက် လက်တွေ့အသုံးပြုရန် သင့်တော်ခြင်းရှိမရှိကို ဆုံးဖြတ်ရန်အတွက် လုံခြုံရေးထိန်းချုပ်မှုများ၏ လုပ်ဆောင်မှုအား စောင့်ကြည့်ရမည်ဖြစ်သည်။

အဖွဲ့အစည်းတွင်း အန္တရာယ် (Institutional Risk) အား ဆုံးဖြတ်ခြင်း

လုံခြုံရေး ထိန်းချုပ်မှုများအား ရယူရာတွင် အစိုးရ၏ အချက်အလက်ဆိုင်ရာ တာဝန်ရှိသူသည် ပထမဦးစွာ အဖွဲ့အစည်းတွင်း အန္တရာယ်များအပေါ် အဓိကထားသည့် အချက်အလက်အမျိုးအစားခွဲခြားခြင်း ဖြစ်စဉ်ကိုလုပ်ဆောင်ကာ အချက်အလက်များ၏ လုံခြုံရေးအရ အရေးကြီးမှုကို ထည့်သွင်းစဉ်းစားရမည်ဖြစ်သည်။ အဖွဲ့အစည်းတွင်းအန္တရာယ်ကို ထည့်သွင်းစဉ်းစားထားသည့် အချက်အလက်များအား တရားမဝင်ရယူခြင်းမှ ဖြစ်ပေါ်လာနိုင်သည့် ဆုံးရှုံးမှုအပေါ် တွင်မူတည်ကာ အဓိပ္ပာယ်သတ်မှတ်ထားပါသည်။ အောက်ပါအခြေအနေများ။ *အကယ်၍ အချက်အလက်များ ထိခိုက်မှုရှိပါက နိုင်ငံ၏လုံခြုံရေး ထိခိုက်နိုင်ပါသလား။ အကယ်၍ အချက်အလက်များ ပေါက်ကြားမှုရှိပါက အစိုးရ သို့မဟုတ် ပြင်ပအဖွဲ့အစည်းတစ်ခုတွင် စီးပွားရေးဆုံးရှုံးမှု အန္တရာယ် ဖြစ်စေနိုင်ပါသလား။*

ပညာရပ်ဆိုင်ရာ ဂေါဟာရတွင် တိကျစွာဖော်ပြထားမှုမရှိသည့်အတွက်ကြောင့် ထိခိုက်မှုများအား အမျိုးအစားခွဲခြားမှုအနေဖြင့် "အကန့်အသတ်ရှိသော ဆိုးရွားသည့် အကျိုးဆက်" (Limited adverse effect) ၊ "ပြင်းထန်သော ဆိုးရွားသည့် အကျိုးဆက်" (Serious adver effect) နှင့် "အင်မတန် ပြင်းထန်သော သို့မဟုတ် ကြီးမားသော ဆိုးရွားသည့် အကျိုးဆက်" (Severe or catatstrophic effect) ဟူ၍ အဖွဲ့အစည်းတွင်း အန္တရာယ်အား စစ်ဆေးခြင်းဖြစ်စဉ်တွင် ပါဝင်သော အကြောင်းအရာများ၏ ထင်ရှားသော အဆင့်အား ပုံနှင့်တကွ ဖော်ပြထားပါသည်။[26] ထို့ကြောင့် အစိုးရ၏ အချက်အလက်ဆိုင်ရာ တာဝန်ရှိသူသည် အမျိုးအစားခွဲခြားခြင်းအား ပို၍ သို့မဟုတ် လျော့၍ မလုပ်ဆောင်မိစေရန်အတွက် အမြဲမပြတ် သတိရှိစေရန် အထူးအရေးကြီးပါသည်။

[26] NIST FIPS PUB 199: ဒေသဆိုင်ရာ သတင်းအချက်အလက်များနှင့် သတင်းအချက်အလက်စနစ်များ၏ လုံခြုံရေးဆိုင်ရာ အမျိုးအစားခွဲခြားခြင်းဆိုင်ရာ စံနှုန်းများ http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf တွင်ရယူနိုင်သည်။

အချက်အလက်များ ပေါက်ကြားခြင်း အန္တရာယ်အား ဆုံးဖြတ်ခြင်း

အဖွဲ့အစည်းတွင်း အန္တရာယ်အား လုံခြုံရေးထိန်းချုပ်မှုအဖြစ် အကောင်အထည်ဖော်ရာတွင် ထည့်သွင်းစဉ်းစားချက် (၂) ခု လိုအပ်ပါသည်။ ပထမ တစ်ခုမှာ အချက်အလက်များ ပေါက်ကြားခြင်း အန္တရာယ်ဖြစ်ပြီး ဒုတိယတစ်ခုမှာ အချက်အလက်များ၏ သဘောသဘာဝပင်ဖြစ်သည်။ အချက်အလက်များ ပေါက်ကြားခြင်း အန္တရာယ်သည် တရားမဝင် အဖွဲ့အစည်းများ ထိုထည့်သွင်းစဉ်းစားထားသည့် အချက်အလက်အား မည်မျှအလိုရှိသည်ဟူသော စစ်ဆေးချက်အပေါ် တွင် မူတည်ပါသည်။ ကျူးလွန်ရန် ရည်ရွယ်ထားသူတစ်ယောက်၏ သတင်းအချက်အလက်များ ရယူလိုအပ်ခြင်းအား ထိုသူ့အတွက် သတင်းအချက်အလက်၏ ဖြစ်လာနိုင်သော ငွေကြေး သို့မဟုတ် တခြားတန်ဖိုးနှင့် ဖြစ်လာနိုင်သော လူမှုဝန်းကျင်ဆိုင်ရာ ဆိုးကျိုးသက်ရောက်မှုများ (စီးပွားရေးဆိုင်ရာ နစ်နာမှု၊ ဥပဒေဆိုင်ရာ အခွင့်အရေးများ၏ ကာကွယ်စောင့်ရှောက်မှု သို့မဟုတ် နိုင်ငံရေး တည်ငြိမ်မှုအား ထိန်းသိမ်းထားနိုင်မှု) စသည့် အချက်နှစ်ချက်အပေါ် တွင်မူတည်ကာ တွက်ဆရမည်ဖြစ်သည်။ ထိုအချက်အလက်အား ပို၍လိုချင်လေလေ တရားမဝင်အဖွဲ့အစည်းများသည် ထိုအချက်အလက်အား ရရှိရန် ကြိုးစားမည့် အန္တရာယ် ပိုများလေဖြစ်ပြီး ဤသို့အချက်အလက်အများအား တရားမဝင်ရယူခြင်း အန္တရာယ်အား ပြန်လည်တုံ့ပြန်ရန်အတွက် ပိုမိုမြင့်မားသော သင့်လျော်ရာလုံခြုံရေး နည်းလမ်းများ လိုအပ်လေဖြစ်သည်။ **ပုဂ္ဂိုလ်ရေးဆိုင်ရာ အချက်အလက် သို့မဟုတ် လုံခြုံရေးစနစ် ထိန်းချုပ်မှုများအား တရားမဝင်ရယူခြင်းသည် အစိုးရအတွက်သာမက တခြားပြင်ပအဖွဲ့အစည်းအတွက်ကိုပါ ကြီးမားသော ဆုံးရှုံးမှုအား ဖြစ်ပေါ် စေနိုင်ပါသည်။ ထိုသို့သော အချက်အလက်အမျိုးအစားသည် သတင်းအချက်အလက်များအား တရားမဝင်ရယူသည့် ပုဂ္ဂိုလ်များအတွက် တစ်ခါတစ်ရံ တန်ဖိုးကြီးသော (လိုချင်မှုများသော) အချက်အလက်များဖြစ်သည်။**

အချက်အလက်များပေါက်ကြားခြင်း အန္တရာယ်သည် အဖွဲ့အစည်းတွင်း အန္တရာယ်နှင့် သီးသန့် ကွဲပြားမှုမရှိပေ။ ထို့ကြောင့် အစိုးရ၏ အချက်အလက်ဆိုင်ရာ စီမံခန့်ခွဲသူသည် သင့်လျော်သော လုံခြုံရေး ထိန်းချုပ်မှုများအား ဆုံးဖြတ်ရာတွင် ထိုကဏ္ဍာန်စုံလုံးရှိ အန္တရာယ်များအား ထည့်သွင်းစဉ်းစားရမည်ဖြစ်သည်။

သင့်လျော်သော လုံခြုံရေး ထိန်းချုပ်မှုများအား ဆုံးဖြတ်ခြင်း

အန္တရာယ်စစ်ဆေးခြင်းအား လုံခြုံစိတ်ချမှု၊ ပြည့်စုံမှုနှင့် အဆင်သင့်ရရှိနိုင်မှု စသည့် လုံခြုံးရေးထိန်းချုပ်မှု၏ ဦးတည်ချက် (၃) ခုပေါ်တွင် အလေးထားလုပ်ဆောင်ထားသည်။

လူတစ်ဦးတစ်ယောက်က သတင်းအချက်အလက်တစ်ခုအတွက် ယေဘူယျ (GENERAL) ၊ လျို့ဝှက်ဖိုင် (SECRET) သို့မဟုတ် အထူးလျို့ဝှက်ဖိုင် (TOP SECREAT) ရှိ လုံခြုံရေး အမျိုးအစားများအား ဆုံးဖြတ်သတ်မှတ်ရာတွင် သင့်လျော်သော လုံခြုံရေး ထိန်းချုပ်မှုများ သေချာစီစစ်နိုင်ရန်အတွက် ဖိုင်တစ်ခုချင်းစီ၏ လုံခြုံစိတ်ချမှု၊ ပြည့်စုံမှုနှင့် အဆင့်သင့်ရရှိမှုအပေါ်တွင် ဖြစ်လာနိုင်သော အကျိုးသက်ရောက်မှု အဆင့်အလိုက် ခွဲခြားသတ်မှတ်ရမည်ဖြစ်သည်။[27]

- လုံခြုံစိတ်ချမှု လုံခြုံစိတ်ချမှုဆိုသည်မှာ သတင်းအချက်အလက်များကို တရားမဝင်သော သူများမှ ရယူကြည့်ရှုခြင်းအား ကာကွယ်နိုင်စွမ်းပင်ဖြစ်သည်။
- ပြည့်စုံမှု အချက်အလက်များသည် တိတိကျကျ မှုလရှိလုံခြုံသော သတင်းအချက်အလက်များအား ပြောင်းလဲခြင်းမရှိ သေချာစွာ ဖော်ပြနိုင်စွမ်းပင်ဖြစ်သည်။
- အဆင်သင့်ရရှိမှု သတင်းအချက်အလက်များအား တရားဝင်ခွင့်ပြုထားသောသူမှ အချိန်တိုင်း အမြဲမပြတ် ရရှိအသုံးပြုနိုင်ရမည်ဖြစ်သည်။

အကျိုးသက်ရောက်မှု အဆင့်တစ်ခုစီအလိုက် ဦးတည်ချက် (၃) ခု၏ တစ်ခုချင်းစီကို လုပ်ဆောင်နိုင်ရမည်ဖြစ်သည်။ အနိမ့် (LOW) ၊ အလယ်အလတ် (MODERATE) နှင့် အမြင့် (HIGHT) ရှိသဖြင့် အဆင့်တစ်ခုချင်းစီအတွက် လုံခြုံရေးထိန်းချုပ်မှုများတွင် စံနှုန်းတစ်ခု သတ်မှတ်ရမည်ဖြစ်သည်။ ယခုဖော်ပြထားသည်၏ ရည်ရွယ်ချက်သည် လုံခြုံရေး လုပ်ဆောင်မှုနည်းလမ်းများနှင့် လုံခြုံရေးလိုအပ်ချက်များအား ရှင်းလင်းစွာ တွဲစပ်နိုင်ရန်ဖြစ်သည်။ ပုံအရ အနိမ့် (LOW) အတွက် စနစ်သည် လုံခြုံရေး ထိန်းချုပ်မှု ၁၀၀ ဖြည့်သွင်းလုပ်ဆောင်သွားမည်ဖြစ်ပြီး အလယ်အလတ် (MODERATE) အတွက် လုံခြုံရေး ထိန်းချုပ်မှု ၁၂၀၊ အမြင့် (HIGH) အတွက် ၁၆၀

[27] ထိုနည်းအတိုင်းပင် တူညီစွာ သတ်မှတ်ထားသည့် သတင်းအချက်အလက်စနစ်အား ခွဲခြမ်းလေ့လာကာ လုံခြုံရေး အမျိုးအစား တစ်ခုအား ခွဲခြားသတ်မှတ်ရမည်ဖြစ်သည်။ သတင်းအချက်အလက်စနစ်သည် စနစ်ရှိ သတင်းအချက်အလက်များ၏ လုံခြုံရေးလိုအပ်ချက်များနှင့် ကိုက်ညီစေရန်အတွက် ထိုသို့လုပ်ဆောင်ထားခြင်းဖြစ်သည်။ NIST မှ အထူးထုတ်ပေးသော 800-53 နှင့် ပေါင်းစပ်ထားသည့် အမေရိန်ကန်အစိုးရ FIPS ၏ ထုတ်ပေးချက်ဖြစ်သည့် ဒေသဆိုင်ရာ သတင်းအချက်အလက်နှင့် သတင်းအချက်အလက်စနစ်အတွက် အနိမ့်ဆုံးရှိရမည့် လုံခြုံရေးလိုအပ်ချက်များ ၂၀၀ သည် HIGH ၏ အကျိုးသက်ရောက်မှုရှိသော သတင်းအချက်အလက်နှင့် စနစ်များအပါအဝင် ဒေသဆိုင်ရာ သတင်းအချက်အလက်နှင့် သတင်းအချက်အလက်စနစ်အားလုံးရှိ လုံခြုံရေးလိုအပ်ချက်များနှင့် အသုံးချနိုင်သော ထိန်းချုပ်မှုများကို ဖော်ပြပေးနိုင်မည်ဖြစ်သည်။

လုပ်ဆောင်သွားမည်ဖြစ်သည်။ ဖော်ပြထားသော
မည်သည့်သတင်းအချက်အလက်အမျိုးအစားအတွက်မဆို လုံခြုံစိတ်ချမှု၊ ပြည့်စုံမှုနှင့်
အဆင်သင့်ရရှိမှုအတွက် အကျိုးသက်ရောက်မှု အဆင့်တစ်ခု (LOW, MODERATE,HIGHT) အား
ပေးအပ်သွားမည်ဖြစ်ပြီး လုံခြုံရေးဆိုင်ရာ ခွဲခြမ်းစိတ်ဖြာမှုတွင် ပိုမိုအရေးကြီးမှုအလိုက် သတ်မှတ်မှုများ
ဖော်ပြသွားမည်ဖြစ်သည်။ ဥပမာအားဖြင့် သတင်းအချက်အလက်သည် လုံခြုံစိတ်ချမှုနှင့် ပြည့်စုံမှုအတွက်
အမြင့် (HIGH) အဆင့်ပြသနိုင်ပြီး အဆင်သင့်ရရှိမှုအတွက် အနိမ့် (LOW) အဆင့် ပြသနိုင်ပေသည်။
ထို့ကြောင့် လုံခြုံရေး လိုအပ်ချက်များသည် ယုံကြည်စိတ်ချမှုနှင့် ပြည့်စုံမှုအတွက် ဦးတည်ကာ
လုံခြုံရေးထိန်းချုပ်မှုအများအပြား လုပ်ဆောင်သွားမည်ဖြစ်ပြီး သတင်းအချက်အလက်များ၏
အဆင်သင့်ရရှိမှုအတွက်ကိုမူ ထိန်းချုပ်မှုများ အနည်းငယ်သာလုပ်ဆောင်သွားမည်ဖြစ်သည်။

ယခုစနစ်သည် စီးပွားရေးလုပ်ငန်းကြီးများနှင့် အဖွဲ့အစည်းအများအပြားတွင် အသုံးပြုနေသော စနစ်များနှင့်
မတူညီပေ။ ကောင်းစွာ လည်ပတ်နေသော အဖွဲ့အစည်းတစ်ခုသည် ၎င်းတို့၏ တန်ဖိုးရှိသော
သတင်းအချက်အလက်များကို ကာကွယ်ရန်အတွက် တူညီသော အဆင့်များအား
လုပ်ဆောင်ရမည်ဖြစ်သည်။ ကုန်သွယ်ရေးဆိုင်ရာ လျှို့ဝှက်ဖိုင်ဖြစ်စေ သို့မဟုတ် စီးပွားရေးဆိုင်ရာ လျှို့ဝှက်
သတင်းအချက်အလက် သို့မဟုတ် စီးပွားရေးလုပ်ငန်းလုပ်ဆောင်မှု၏ သတင်းအချက်အလက်များ ဖြစ်စေ
အစိုးရ၏ သတင်းအချက်အလက်အတော်များများသည် စီးပွားရေးလုပ်ငန်း သတင်းအချက်အလက်များနှင့်
နှိုင်းယှဉ်ကြည့်နိုင်ပေသည်။ ထို့ကြောင့် စီးပွားရေးတစ်ခု၏ သတင်းအချက်အလက်ဆိုင်ရာ
လုံခြုံရေးလိုအပ်အမျိုးမျိုးသည်လည်း အစိုးရ၏ လိုအပ်ချက်များနှင့် အလားသဏ္ဌာန်တူပေသည်။ ထို့ကြောင့်
ကောင်းစွာ လည်ပတ်နေသော စီးပွားရေးလုပ်ငန်းကြီးတစ်ခုအတွက် စနစ်အား စီစဉ်ရေးဆွဲထားသော်လည်း
အစိုးရ၏ သတင်းအချက်အလက်ဆိုင်ရာ လုံခြုံရေး ကျွမ်းကျင်သူသည် ထို ICT စနစ်အား အစိုးရ၏
လိုအပ်ချက်များနှင့် ကိုက်ညီစေရန်အတွက် သတ်မှတ်ဖော်ပြနိုင်ပေသည်။ ကောင်းစွာ လည်ပတ်နေသော
စီးပွားရေးလုပ်ငန်းကြီးတစ်ခုခုနှင့်အတူ အစိုးရ၏ အချက်အလက်ဆိုင်ရာ စီမံခန့်ခွဲသူသည်
စီမံလုပ်ဆောင်မှုများတိုးတက်လာစေရန်အတွက် သတင်းအချက်အလက်ဆိုင်ရာ လုံခြုံရေး
ဦးဆောင်အဖွဲ့အစည်းတစ်ခုအား စမ်းသပ်လုပ်ဆောင်ရမည်ဖြစ်ပြီး တူညီသောနည်းလမ်းအတိုင်း
ကောင်းမွန်သော လုံခြုံရေး နည်းလမ်းများအား အစိုးရတွင် ဖော်ဆောင်ရမည်ဖြစ်သည်။

အန္တရာယ် စစ်ဆေးမှု အကဲဖြတ်ခြင်းနှင့် စောင့်ကြည့်ခြင်း

လုံခြုံရေး ထိန်းချုပ်မှုများ၏ ခိုင်မာမှုအား ဆုံးဖြတ်ရန်အတွက် Cloud အသုံးပြုသူသည် စနစ်အတွင်းရှိ လုံခြုံရေးထိန်းချုပ်မှုများ၏ အကျိုးသက်ရောက်မှုအား စောင့်ကြည့်လုပ်ဆောင်ရန်အတွက် လူများ သို့မဟုတ် အဖွဲ့များရှိရမည်ဖြစ်သည်။ အချက်အလက်များ ပေါက်ကြားခြင်း သို့မဟုတ် တိုက်ခိုက်ရန်ကြိုးစားမှုများအား သိရှိထုတ်ဖော်နိုင်ရန်အတွက် စောင့်ကြည့်ခြင်း သို့မဟုတ် စစ်ဆေးခြင်းအား ပုံမှန်လုပ်ဆောင်ရမည်ဖြစ်သည်။

ကောင်းမွန်သော အကဲဖြတ်ခြင်းနှင့် စောင့်ကြည့်ခြင်း လုပ်ဆောင်ရန်အတွက် Cloud အသုံးပြုသူသည် လိုအပ်သော အောက်ပါ အရည်အချင်းများအား သိရှိကာ တိုးတက်စေရန်လုပ်ဆောင်၊ ထိန်းသိမ်းထားရမည်ဖြစ်သည်။

1. Cloud ရှိ ICT အရင်းအမြစ်များနှင့် ၎နှဆောင်မှု လွှဲပြောင်းရာ စနစ်များအား လုပ်ဆောင်ခြင်းနှင့် စီမံခန့်ခွဲခြင်း
2. လုံခြုံရေး လိုအပ်ချက်များနှင့် ကိုက်ညီမှုရှိစေရန်အတွက် လုံခြုံရေး ထိန်းချုပ်မှုများ၊ ထိန်းချုပ်မှု လုပ်ဆောင်ချက်များနှင့် စစ်ဆေးခြင်းများအား သိရှိနားလည်ဖြင်း၊ လက်တွေ့လုပ်ဆောင်ခြင်းနှင့် ဆော့ဖ်ဝဲများအသုံးပြုခြင်း
3. Cloud ၎နှဆောင်မှုရှိ စောင့်ကြည့်ရေးဆိုင်ရာ ကိရိယာများနှင့် မှတ်တမ်းတင် စနစ်များ (Logging systems) အား သတ်မှတ်ဖော်ပြခြင်းနှင့် လက်တွေ့အသုံးချခြင်း[28]

အန္တရာယ်စစ်ဆေးခြင်းအား လုပ်ဆောင်ပြီးသည်နှင့် တစ်ပြိုင်နက် သင့်လျော်သော လုံခြုံရေး ထိန်းချုပ်မှုများအား စနစ်အတွင်းသို့ ထည့်သွင်းရမည်ဖြစ်ပြီး အန္တရာယ် ထိန်းချုပ်မှုများသည် ထိရောက်စွာလုပ်ဆောင်နိုင်ကြောင်း သေချာစေရန်အတွက် အဖွဲ့အစည်းအတွင်းတွင် တိကျသော အရည်အချင်းများ လိုအပ်မည်ဖြစ်သည်။ အိမ်တွင်းသုံး ICT အခြေအနေတွင်မူ အောက်ဖော်ပြပါ အရေးကြီးသော အရည်အချင်း (၃) ခု လိုအပ်ပါသည်။

[28] AWS DevOps ၏ အင်ဂျင်နီယာ စာမေးပွဲ အယူအဆများမှ ပြင်ဆင်ထားသည်။ http://aws.amazon.com/certification/certified-devops-engineer-professional/

1. ကိုယ်တိုင်ဂင်ရောက်ခွင့်တားမြစ်ခြင်းများ (Physical access restrictions) အပါအဂင် ပုဂ္ဂိုလ်၏ လုံခြုံရေး ထိန်းချုပ်မှုများ လုပ်ဆောင်ကြောင်း သေချာမှုရှိစေရန်အတွက် စမ်းသပ်သော ကျွမ်းကျင်ပညာရှင်
2. အဖွဲ့အစည်း၏ လိုအပ်ချက်များနှင့် ကိုက်ညီမှုရှိစေရန်အတွက် လုံလောက်သော ICT အရင်းအမြစ်များ ဖြည့်ဆည်းပေးနိုင်ကြောင်း သေချာမှုရှိစေရန်တွက် စမ်းသပ်သော ICT ကျွမ်းကျင်ပညာရှင်နှင့်
3. အချက်အလက်များရယူခြင်းအတွက် Logical control များ၊ ဆော့ဖ်ဂဲအခြေပြု လုံခြုံရေး ထိန်းချုပ်မှုများနှင့် စောင့်ကြည့်ခြင်းလုပ်ဆောင်မှုများ မည်သို့လုပ်ဆောင်မည်ကို သိရှိသော ကျွမ်းကျင်ပညာရှင်

Cloud အပေါ်တွင်အခြေခံထားသော ICT အခြေအနေတွင်ရှိ ထိရောက်သော အန္တရာယ်ထိန်းချုပ်မှုများသည် ယေျဘူယျအခြေအနေ၊ အိမ်တွင်းသုံး ICT အခြေအနေရှိ လိုအပ်သော အရည်အချင်း အမျိုးမျိုးပေါ်တွင်မူတည်သည်။ ပုဂ္ဂိုလ်၏ လုံခြုံရေးထိန်းချုပ်မှုများအား CSP သို့လွှဲပြောင်းသည့်အခါတွင် Cloud အသုံးပြုသူသည် ထိန်းသိမ်းစောင့်ရှောက်ခြင်း အဆင့်ရှိ Cloud ဂန်ဆောင်မှုများနှင့် ဂန်ဆောင်မှုစီမံခန့်ခွဲခြင်း အဆင့်ရှိ Cloud ဂန်ဆောင်မှုများအား ညှိနှိုင်းလုပ်ဆောင်နိုင်သော စီမံခန့်ခွဲနိုင်သော ကျွမ်းကျင်ပညာရှင်များလိုအပ်မည်ဖြစ်သည်။ ထိုအပိုင်းတွင်

1. Cloud SLAs အား ညှိနှိုင်းလုပ်ဆောင်ခြင်းနှင့် စီမံခန့်ခွဲခြင်းများ လုပ်ဆောင်ရန်အတွက် အင်ဂျိနီယာများ၊ ဆော့ဖ်ဂဲလ်ကျွမ်းကျင်သူများ၏ လုပ်ဆောင်မှုများနှင့်အတူ ဥပဒေရေးရာ ရှုေ့နများ SLAs သည် CSP မှ ICT ဂန်ဆောင်မှု သဘောတူညီချက်များအား Cloud အသုံးပြုသူထံတွင် ထားရှိသွားမည်ဖြစ်ဖြင့် Cloud အသုံးပြုသူသည် သူတို့၏ လိုအပ်ချက်များနှင့် ကိုက်ညီသော ဂန်ဆောင်မှုများရရှိသည်ကို သေချာမှုရှိစေရန်အတွက် လိုအပ်သော အရည်အချင်းများရှိရမည်ဖြစ်သည်။
2. Cloud ၏ သဘောတူညီမှုဆိုင်ရာ စစ်ဆေးချက်များအား စောင့်ကြည့်ရန်နှင့် ဆန်းစစ်ရန်အတွက် ကျွမ်းကျင်ဂန်ထမ်းများ ထိုအပိုင်းတွင် အဖွဲ့အစည်းအတွင်း လူပုဂ္ဂိုလ်များ သို့မဟုတ် ကျွမ်းကျင်စစ်ဆေးခြင်း အဖွဲ့များလည်း ပါဂင်နိုင်ပါသည်။ British Standards Institution ကဲ့သို့သော စစ်ဆေးခြင်း အဖွဲ့များသည် ISO Cloud လုံခြုံရေးစံနှုန်းများနှင့်အတူ CSP ၏ စစ်ဆေးခြင်း

ဂန်ဆောင်မှုများ လုပ်ဆောင်ပေးသော အဖွဲ့များဖြစ်သည်။ Cloud အသုံးပြုသူသည် သူတို့၏ ဂန်ဆောင်မှုပေးသော သူထံမှနေ၍ ထိုကဲ့သို့သော အဖွဲ့များ၏ ထုတ်ပြန်ချက်များအား တောင်းဆိုခြင်း ဆန်းစစ်ခြင်းများ လုပ်ဆောင်ရမည်ဖြစ်သည်။

3. ထိန်းချုပ်ခြင်းဆိုင်ရာ မူဘောင်အား ဒီဇိုင်းဆွဲရန်၊ ရယူခွင့် တောင်းဆိုမှုများအား စီမံခန့်ခွဲရန်၊ လုံခြုံရေးထိန်းချုပ်မှုများ၏ လုပ်ဆောင်ချက်အား စောင့်ကြည့်ရန်နှင့် အသုံးချဆော့ဖ်ဝဲ တစ်ခုမှ နောက်တစ်ခုသို့ ဖြစ်နိုင်သည့် လုံခြုံရေးထိန်းချုပ်မှုများရယူရန်အတွက် စနစ် အော်ပရေတာများနှင့် အင်ဂျီနီယာများ
4. ယေဘူယျအားဖြင့် စနစ် အော်ပရေတာများ၊ အင်ဂျီနီယာများနှင့် တွဲဖက်လုပ်ကိုင်နေသော ဆော့ဖ်ဝဲလ်ကျွမ်းကျင်သူများသည် Cloud အသုံးပြုသူကို "DevOps" လုပ်ဆောင်မှုဝေလေ့အား တိုးတက်စေရန် ရှာဖွေလုပ်ဆောင်ရာတွင် ကူညီလုပ်ဆောင်ပေးနိုင်မည်ဖြစ်သည်။ အဖွဲ့အစည်းတစ်ခုအတွင်းရှိ "DevOps" လုပ်ဆောင်မှုဝေလေ့သည် အဆက်မပြတ်ရှာဖွေလုပ်ဆောင်ခြင်းနှင့် လုပ်ဆောင်မှု အသစ်များ တိုးတက်လာခြင်းမှ ပေါ်ထွက်လာခြင်းဖြစ်ပြီး အဖွဲ့အစည်း၏ ဂန်ဆောင်မှု လွှဲပြောင်းခြင်းအား ဆော့ဖ်ဝဲလ်၏ အလိုအလျောက်လုပ်ဆောင်အဖြစ်ပြောင်းလဲစေခြင်း၊ တိုးမြှင်းပေးခြင်း သို့မဟုတ် တိုးတက်စေခြင်း ဖြစ်စေမည်ဖြစ်သည်။ Cloud မှ ထောက်ပံ့ပေးထားသော ပြောင်းလဲလုပ်ဆောင်နိုင်သည့် ICT အခြေအနေနှင့်အတူ စနစ်အော်ပရေတာများနှင့် အင်ဂျီနီယာများသည် Cloud ၏ အသစ်အသစ်သော အသုံးချဆော့ဖ်ဝဲများနှင့် ဂန်ဆောင်မှုများ တိုးတက်လာခြင်းနှင့် စမ်းသပ်ခြင်းမှတစ်ဆင့် ဖြေရှင်းနည်းအသစ်များကို အဆက်မပြတ်ရှာဖွေရန်အတွက် လိုအပ်သော ကိရိယာများအား ရရှိနိုင်မည်ဖြစ်သည်။

အချက်အလက်များအား လွတ်လပ်စွာ အသုံးပြုခြင်း မူဝါဒမှ (Open Data Policy) တစ်ဆင့် လွတ်လပ်စွာရယူနိုင်ခွင့် ဝိုင်မြှောင်လုပ်ခြင်း (A 5)

အုပ်ချုပ်ရေ တိုးတက်စေလိုသော ရည်ရွယ်ချက်၊ ယုံကြည်မှုတည်ဆောက်ခြင်းနှင့် ပွင့်လင်းမြင်သာမှုရှိခြင်း စသည်တို့နှင့်အတူ မြန်မာနိုင်ငံတော်အစိုးရသည် အစိုးရ၏ အချက်အလက်များအား လွတ်လပ်စွာအသုံးပြုနိုင်ရေးအတွက် ခွန်အားစိုက်ထုတ်လုပ်ဆောင်မှုမနေဖြင့် အချက်အလက်များအား လွတ်လပ်စွာအသုံးပြုခြင်းမူဝါဒ (Open Data Policy) (က ၅) ကို ပြဋ္ဌာန်းသွားမည်ဖြစ်ပါသည်။

နိဒါန်း

လွတ်လပ်စွာအသုံးပြုနိုင်သော အချက်အလက်များ (Open data) ဆိုသည်မှာ မည်သူမဆို၊ မည်သည့်အချိန်၊ မည်သည့်နေရာတွင်မဆို လွတ်လပ်စွာ အသုံးပြုခြင်း၊ ပြန်လည်အသုံးပြုခြင်းနှင့် ပြန်လည်ရောင်းချခြင်းအတွက် လိုအပ်သော နည်းပညာနှင့် ဥပဒေဆိုင်ရာ လက္ခဏာများဖြင့် ဖွဲ့စည်းတည်ဆောက်ထားသော ဒီဂျစ်တယ်ဆိုင်ရာ အချက်အလက်များဖြစ်သည်။[29]

အချက်အလက်များသည် မြန်မာနိုင်ငံတော်အစိုးရ၏ တန်းဖိုးရှိသော အရင်းအမြစ် ပစ္စည်းများပင်ဖြစ်ပေသည်။ နိုင်ငံတော် အစိုးရသည် ထိုသတင်းအချက်အလက်ရင်းမြစ်များမှနေ၍ အကျိုးအမြတ်အပြည့်အဝ ရရှိစေရန်အတွက် ဝန်ကြီးဌာနတစ်ခုချင်းစီနှင့် အဖွဲ့အစည်းများသည် လွတ်လပ်စွာ အချက်အလက်များရယူခြင်းနှင့် ပေါင်းစည်းလုပ်ကိုင်နိုင်ခြင်းအား အထောက်အပံ့ဖြစ်စေသော နည်းလမ်းအတိုင်း အချက်အလက်များအား စီမံခန့်ခွဲရမည်ဖြစ်သည်။ ထိုသို့လုပ်ဆောင်ခြင်းဖြင့် အကျိုးကျေးဇူးများလာခြင်း၊ ကုန်ကျစရိတ် လျော့ချခြင်း၊ ဝန်ဆောင်မှု လုပ်ဆောင်ခြင်းများ တိုးတက်လာခြင်း၊ လူပုဂ္ဂိုလ်ဆိုင်ရာ သတင်းအချက်အလက်များအား ကာကွယ်နိုင်ခြင်းနှင့် အစိုးရ၏ တန်ဖိုးရှိသော သတင်းအချက်အလက်များအား ပြည်သူများရယူနိုင်ခြင်းများ တိုးမြှင့်လာမည်ဖြစ်သည်။

အချက်အလက်အရင်းအမြစ်များအား ပြည်သူအများ ရယူခြင်း၊ ရှာဖွေခြင်းနှင့် အသုံးပြုခြင်းများလုပ်ဆောင်ခြင်းကြောင့် များစွာသော အကျိုးကျေးဇူးများ ဖြစ်ထွန်းလာမည်ဖြစ်သည်။ စီးပွားရေး ရှုထောင့်အရ ထိုသို့လုပ်ဆောင်ခြင်းသည် စွန့်ဦးတီထွင်မှုများနှင့် ဆန်းသစ်မှုများအား အားဖြည့်ပေးနိုင်မည်ဖြစ်ပြီး နိုင်ငံခြားရင်းနှီးမြှုပ်နှံမှုများအား လှုံ့ဆော်စေနိုင်ကာ စီးပွားရေးတိုးတက်စေရန်အတွက် အခွင့်အလမ်းအသစ်များ ဖန်တီးပေးနိုင်မည်ဖြစ်သည်။

ယခု မူဝါဒသည် အချက်အလက်များအား အစိုးရ၏ ဝန်ကြီးဌာနများ၊ အဖွဲ့အစည်းများနှင့် အစိုးရဆိုင်ရာ ဌာနများ (နောက်ပိုင်းတွင် အဖွဲ့အစည်းများ) သည် ရှိထားသောအချက်အလက်များအား

[29] နိုင်ငံတကာ လွတ်လပ်စွာ အသုံးပြုနိုင်သော အချက်အလက်များ၏ လက္ခဏာများ။

မျဖေသုံးစွဲနိုင်သည့် တစ်ခုတည်းသော နည်းလမ်းပေါ်တွင် အခြေခံထားပါသည်။ ထိုမျှသာမက ဤလုပ်ဆောင်မှုသည် မြန်မာနိုင်ငံတော် အစိုးရ၏ အခြေအနေနှင့် အချက်အလက်အရင်းအမြစ်များအား မည်သို့စီရင်ပြုစုမည့် နည်းလမ်းကိုပါ ဖော်ပြနိုင်မည်ဖြစ်သည်။ သတင်းအချက်အလက်တစ်ခုကို ပြည်သူလူထုအား ဖော်ပြသည်ဖြစ်စေ မဖော်ပြသည်ဖြစ်စေ အချက်အလက်အရင်းအမြစ်အားလုံးတွင် ပိုမိုထိရောက်စွာလုပ်ဆောင်နိုင်ရန်နှင့် ပိုမိုတန်ဖိုးရှိစေရန်အတွက် ယခု မူဝါဒတွင် ပါရှိသော ပြဋ္ဌာန်းချက်များနှင့်အညီ အဖွဲ့အစည်းများသည် လျှောက်ထားနိုင်မည်ဖြစ်သည်။

အထူးသဖြင့် နောင်ပိုင်းအဆင့်များရှိ စနစ်တကျလုပ်ဆောင်ခြင်းများနှင့် အချက်အလက်ဖေမျှခြင်းများအား အထောက်အကူဖြစ်စေရန်အတွက် ယခုမူဝါဒသည် အဖွဲ့အစည်းအားလုံးအား အချက်အလက်များ စုစည်းရန် သို့မဟုတ် ဖန်တီးရန်အတွက် လိုအပ်မည်ဖြစ်သည်။ ထိုအပိုင်းတွင် ကွန်ပြူတာတွင်သုံးသော အချက်အလက်များအသုံးပြုခြင်းနှင့် အချက်အလက်အသစ်များအတွက် ပုံစံအသစ်များ လုပ်ဆောင်ခြင်း၊ အချက်အလက်ဆိုင်ရာ စံနှုန်းများလုပ်ဆောင်ခြင်းများ ပါဝင်သည်။ ထိုသို့လုပ်ဆောင်ရာတွင်လည်း လွတ်လပ်စွာအသုံးပြုခွင့်ရသော လိုင်စင်များမှတစ်ဆင့် အချက်အလက်များအား ကောင်းမွန်မှုရှိစေရန်လုပ်ဆောင်ခြင်းနှင့် ပုဂ္ဂိုလ်ရေးဆိုင်ရာအချက်အလက်များ၊ လုံခြုံစိတ်ချရခြင်း၊ လုံခြုံရေး သို့မဟုတ် တခြားကန့်သတ်ချက်များအတွက် အချက်အလက်များအား ပြန်လည်ဆန်းစစ်ခြင်းများလည်း ပါဝင်သည်။ ထပ်မံဖြည့်စွပ်ရသော် အဖွဲ့အစည်းအားလုံးသည် ပေါင်းစည်းလုပ်ကိုင်ခြင်းနှင့် ရယူအသုံးပြုနိုင်ခြင်းများ အကောင်းဆုံးလုပ်ဆောင်နိုင်စေရန်၊ အချက်အလက်ဆိုင်ရာ စာရင်းများအား ထိန်းသိမ်းရန်၊ ကာကွယ်မှုများအား အဆက်မပြတ် တိုးမြှင့်ရန်နှင့် သတင်းအချက်အလက်ဆိုင်ရာ စီမံခန့်ခွဲခြင်း တာဝန်များအား ရှင်းလင်းစွာအဓိပ္ပာယ်သတ်မှတ်ရန်အတွက် အဖွဲ့အစည်းအားလုံးသည် သတင်းအချက်အလက်ဆိုင်ရာ စနစ်များအား တည်ဆောက်ခြင်း သို့မဟုတ် ခေတ်မှီအောင်လုပ်ဆောင်ခြင်းများ လိုအပ်မည်ဖြစ်သည်။

မြန်မာနိုင်ငံတော်အစိုးရသည် ပေါင်းစည်းလုပ်ဆောင်ခြင်းနှင့် လွတ်လပ်စွာရယူနိုင်ခြင်း တိုးမြှင့်စေရန်အတွက် အချက်အလက်အရင်းအမြစ်များ၏ စီမံခန့်ခွဲမှုအား တိုးတက်အောင်လုပ်ဆောင်ရာတွင် သိသာသော တိုးတက်မှုကို လုပ်ဆောင်နိုင်ခဲ့ပြီဖြစ်သည်။ ပွင့်လင်းမြင်သာခြင်းနှင့် ပေါင်းစည်းလုပ်ကိုင်ခြင်း၏ စည်းမျဉ်းများကို အကောင်အထည်ဖော်ရန်နှင့်

သတင်းအချက်အလက်ရယူခြင်းအား တိုးမြှင့်ရန်အတွက် လုပ်ဆောင်မှုများ ဆောင်ရွက်ရန် အဖွဲ့အစည်းအားလုံးအား ညွှန်ကြားရမည်ဖြစ်သည်။ ထိုမျှသာမက ယခုမူဂါဒသည် စုစည်းထားသောအချက်အလက်များနှင့်အတူ ခိုင်မာသော နိုင်ငံတော်ဆိုင်ရာ လွတ်လပ်စွာအသုံးပြုနိုင်သော အချက်အလက် လမ်းညွှန် (Open Data Portal) အား ဖြစ်ပေါ်စေမည့် အစီအစဉ်အားလျာထားခြင်းဖြစ်သလို ဤသည်ကိုလည်း အနာဂါတ်တွင် ဖန်တီးလုပ်ဆောင်သွားမည်ဖြစ်သည်။ အစိုးရ၏ အချက်အလက်များအား ရယူအသုံးပြုခွင့် တိုးမြှင့်လာစေရန်အတွက် ဤအွန်လိုင်း ပလပ်ဖောင်းကိုလည်း ဒီဇိုင်းရေးဆွဲသွားမည်ဖြစ်သည်။ ယခုလမ်းညွှန်မှတစ်ဆင့် ထုတ်ပေးသော အချက်အလက်များသည် ပြည်သူလူထုအား ကောင်းကျိုးဖြစ်စေရန်နှင့် စီးပွားရေးဆိုင်ရာ အခွင့်အလမ်းတိုးတက်မှုများ ဖန်တီးနိုင်ရန်အတွက် ဆက်လက်ဆောင်ရွက်သွားမည်ဖြစ်သည်။

အသုံးအနှုန်း အဓိပ္ပါယ်ဖွင့်ဆိုချက်များ

လွတ်လပ်စွာ အသုံးပြုနိုင်သော အချက်အလက်ဆိုင်ရာ မူဂါဒနှင့် ကိုက်ညီမှုရှိရမည့် သတ်မှတ်ချက်များနှင့် စည်းမျဉ်းများအား ယခုအပိုင်းတွင် ဖော်ပြထားပါသည်။

- အချက်အလက် ယခု စာတမ်း၏ ရည်ရွယ်ချက်အရ မှတ်သားထားခြင်းမဟုတ်သည့် တည်ဆောက်ထားသော သတင်းအချက်အလက်အားလုံး
- အချက်အလက်မှတ်တမ်း ယခု စာတမ်း၏ ရည်ရွယ်ချက်အရ ဇယားပုံစံ သို့မဟုတ် ဇယားပုံစံမဟုတ်သော ပုံစံတွင် ပါဝင်သည့် အချက်အလက်များအား စုစည်းမှု
- တန်ဖိုးမြင့်မားသော အချက်အလက်မှတ်တမ်း များပြားသော အသုံးပြုသူများအတွက် အသုံးဝင်မည့် အချက်အလက်မှတ်တမ်းများ သို့မဟုတ် ရည်မှန်းထားသော အသုံးပြုသူအတွက် ကြီးမားသော တန်ဖိုးကို ဖြစ်စေသော အချက်အလက်မှတ်တမ်း၊ အသုံးပြုမှုများခြင်းနှင့် ပြန်လည်အသုံးပြုနိုင်ချေများခြင်း၊ ပြန်လည်အသုံးပြုရာတွင် ကြီးမားသော လူမှုရေးနှင့် စီးပွားရေးဆိုင်ရာ အကျိုးသက်ရောက်နိုင်မှု ရှိခြင်း။
- **သတင်းအချက်အလက်** မည်သည့် ဆက်သွယ်မှုမဆို သို့မဟုတ် ဖြစ်ရပ်များ၊ အချက်အလက်များ သို့မဟုတ် စာများ၊ ဂဏန်းများ၊ ဂရပ်များ၊ မြေပုံများ၊ ဇာတ်လမ်းများ သို့မဟုတ် ရုပ်သံ-

အသံဖိုင်များပါဝင်သည့် ပုံစံ သို့မဟုတ် ဆက်သွယ်ရေးနည်းလမ်းရှိ ထင်မြင်ယူဆချက်များ စသည်ကဲ့သို့သော အသိပညာအား ပြန်လည်တင်ပြခြင်းတစ်ခု

- လွတ်လပ်စွာလုပ်ဆောင်ခြင်း အသုံးပြုခြင်းနှင့် ပြန်လည်အသုံးပြုခြင်းအတွက် လွတ်လပ်စွာ ရယူနိုင်သော၊ မည်သည့်ရည်ရွယ်ချက်အတွက်မဆို ပြန်လည်ဖြန့်ဝေနိုင်သော (လွတ်လပ်စွာ လုပ်ဆောင်နိုင်ရန်အတွက် ကန့်သတ်မှုများမပါသော) ဆော့ဖ်ဝဲ၊ အချက်အလက်နှင့် တခြားဖော်ပြ အီလထရောနစ် အချက်အလက်များ

- လွတ်လပ်စွာအသုံးပြုနိုင်သော အချက်အလက်များ (Open data) ဆိုသည်မှာ မည်သူမဆို၊ မည်သည့်အချိန်၊ မည်သည့်နေရာတွင်မဆို လွတ်လပ်စွာ အသုံးပြုခြင်း၊ ပြန်လည်အသုံးပြုခြင်းနှင့် ပြန်လည်ရောင်းချခြင်းအတွက် လိုအပ်သော နည်းပညာနှင့် ဥပဒေဆိုင်ရာ လက္ခဏာများဖြင့် ဖွဲ့စည်းတည်ဆောက်ထားသော အချက်အလက်များပင်ဖြစ်သည်။ ယခု စာတမ်း၏ ရည်ရွယ်ချက်အရ မည်သူတစ်ဦးတစ်ယောက်၊ မည်သည့်အချိန်၊ မည်သည့်နေရာတွင်မဆို လွတ်လပ်စွာ အသုံးပြုနိုင်၊ ပြန်လည်အသုံးပြုနိုင်ခြင်းနှင့် ပြန်လည်ဖြန့်ဖြူးနိုင်စေရန်အတွက် နည်းပညာနှင့် ဥပဒေဆိုင်ရာ လက္ခဏာများဖြင့် ပြုလုပ်ဖန်တီးထားသော ဒစ်ဂျစ်တယ် အချက်အလက်။ ယေဘုယျအားဖြင့် အောက်ပါစည်းမျဉ်းများနှင့် ကိုက်ညီမှုရှိရမည်ဖြစ်သည်။

1. ဤပြည်သူလူထုဆိုင်ရာ ထုတ်ပြန်ချက်များ၏ ကိုယ်စားအနေဖြင့် လုပ်ငန်းများ သို့မဟုတ် အဖွဲ့အစည်းများမှ ကိုင်ဆောင်ထားသော အချက်အလက်များသည် ပြည်သူလုထုကိုယ်စား အစိုးရမှကိုင်ဆောင်ထားသည့် ပြည်သူပိုင် ပစ္စည်းများပင်ဖြစ်သည်။
2. အချက်အလက်များ၏ အသုံးချမှုအား တစ်ဦးတစ်ယောက်တည်းအတွက် မဖြစ်စေရဘဲ အချက်အလက်များအား ပြည်သူပိုင်ပစ္စည်းအနေဖြင့် တန်ဖိုးမြှင့်သထက်မြှင့်အောင်လုပ်ဆောင်ရမည်ဖြစ်သည်။
3. ပုဂ္ဂိုလ်ရေးဆိုင်ရာ၊ လျို့ဝှက်ထားခြင်းဆိုင်ရာနှင့် လုံခြုံမှုဆိုင်ရာ ကန့်သတ်ချက်များနှင့် ညီစွန်းမှုမရှိသရွေ့ ဥပဒေက ပြဋ္ဌာန်းထားသော အတိုင်းအတာအထိ လွတ်လပ်စွာရယူခွင့်အား လုပ်ဆောင်စေရန်အတွက် အစိုးရသည် မှန်ကန်သည်လုပ်ဆောင်ချက်များတွင် ရပ်တည်ပေးရမည်ဖြစ်သည်။

4. အထူး တောင်းဆိုခြင်းများအား စောင့်ဆိုင်းခြင်းမရှိဘဲ အချက်အလက်များအား အချိန်နှင့်အညီ ရယူနိုင်စေရန်အတွက် လုပ်ဆောင်ရမည်ဖြစ်သည်။ အချက်အလက်များအတွက် ထပ်တိုးတောင်းဆိုခြင်းများအား အစိုးရသည် ကောင်းမွန်စွာတုံ့ပြန်ရမည်ဖြစ်သည်။
5. ဖြန့်ဖြူးမှုအစွန်းထွက် စရိတ်နှင့် အင်တာနက်တွင် အဖိုးအခကုန်ကျမှုမရှိဘဲ အချက်အလက်များအား ရယူနိုင်ခြင်းရှိရမည်
6. ပြန်လည်ရယူနိုင်သော၊ ကူးယူနိုင်သော၊ အက္ခရာစီစဉ်ထားသော၊ ရှာဖွေနိုင်သော လွယ်ကူအဆင်ပြေသည့်၊ ပြန်လည်ပြင်ဆင်နိုင်သည့်၊ လွတ်လပ်စွာရယူနိုင်သည့် ပုံစံများအတိုင်း အချက်အလက်များသည် ရယူနိုင်ခြင်းရှိရမည်ဖြစ်သည်။ ပုံစံများသည် ကွန်ပြူတာများမှ နားလည်နိုင်သော အချက်အလက်များဖြစ်ရမည်။ လုပ်ဆောင်လျှင်လုပ်ဆောင်နိုင်သည့်လျှောက်ထိုပုံစံများသည် တစ်ဦးတစ်ယောက်၏ပိုင်ဆိုင်မှုနှင့် မသက်ဆိုင်သော၊ ပြည်သူလူထု ရရှိအသုံးပြုနိုင်သော၊ အသုံးပြုရာတွင် ကန့်သတ်ထားခြင်းမရှိသော ပုံစံများဖြစ်ရမည်။
7. အချက်အလက်များအား မည်သည့် ဥပဒေဆိုင်ရာ ရည်ရွယ်ချက်အတွက်မဆို၊ စီးပွားရေး သို့မဟုတ် စီးပွားရေးမဟုတ်သော ရည်ရွယ်ချက်အတွက်မဆို ပြန်လည်အသုံးပြုနိုင်သည်။
8. ကိုယ်ပိုင်အချက်အလက်များအား ထုတ်ပြန်ပေးခြင်းအပြင် မြန်မာနိုင်ငံတော်အစိုးရသည် တခြားပြည်နယ်နှင့် ဒေသတွင်းအစိုးရများ၊ တသီးပုဂ္ဂလကိုယ်စားလှယ်များနှင့် လူမှုအဖွဲ့အစည်းများ၏ အချက်အလက်ထုတ်ပြန်ခြင်းအား အားပေးအားမြှောက်ပြုခြင်းနှင့် လွယ်ကူစေရန်လုပ်ဆောင်ပေးခြင်းများ ပြုလုပ်မည်ဖြစ်သည်။
9. နိုင်ငံသူနိုင်ငံသားများနှင့် လူမှုဂန်းကျင်အား တတ်နိုင်သလောက် အကျိုးပြုစေရန်အတွက် အစိုးရသည် ၄င်းတို့၏ လွတ်လပ်စွာအသုံးပြုနိုင်သော အချက်အလက်များအား အသုံးပြုစေရန် တိုက်တွန်းသွားမည်ဖြစ်သည်။
10. အသုံးပြုသော အချက်အလက်များအား အထောက်အကူပြုစေရန်အတွက် ဆက်သွယ်မေးမြန်းမည့်နေရာအား တည်ထောင်သွားမည်ဖြစ်သလို ဤလွတ်လပ်စွာအသုံးပြုနိုင်သော အချက်အလက်များ၏ လိုအပ်ချက်များအား အထောက်အပံ့ဖြစ်စေရန်အတွက် တိုင်ကြားပြောဆိုမှုများနှင့် ပြန်လည်ပြောကြားချက်များကိုလည်း ပြန်လည်ဖြေကြားသွားမည်ဖြစ်သည်။

လွတ်လပ်စွာအသုံးပြုနိုင်သော အလက်များ၏ လမ်းညွှန်

လွတ်လပ်စွာအသုံးပြုနိုင်သောအလက်များ၏ လမ်းညွှန်ကို ITCSD မှ တည်ထောင်သွားမည်ဖြစ်သည်။ ဤလမ်းညွှန်သည် အစိုးရအတွက် တစ်ခုတည်းသော အာဏာပိုင် ပလပ်ဖောင်းတစ်ခု ဖြစ်မည်ဖြစ်ပြီး Myanmar National Portal နှင့် ချိတ်ဆက်ထားမည်ဖြစ်သည်။ လိုအပ်နေသော သတင်းအချက်အလက်များကို ရှာဖွေသူတို့အတွက် လျှင်မြန်သော ထိရောက်သော ပလပ်ဖောင်းတစ်ခုဖြစ်စေရန် အစိုးရ၏ အချက်အလက်အားလုံးအတွက် တစ်ခုတည်းသော ပလပ်ဖောင်းအားလုပ်ဆောင်မည်ဖြစ်သည်။

အဖွဲ့အစည်းတစ်ခုချင်းစီသည် ၎င်းတို့ကိုယ်ပိုင် လွတ်လပ်စွာအသုံးပြုနိုင်သော အချက်အလက်လမ်းညွှန်အား တိုးတက်လုပ်ဆောင်ရန်မလိုအပ်သလို လုပ်ဆောင်ရန်လည်း မသင့်ပေ။ သူတို့၏ အချက်အလက်များအား အချိန်အခါနှင့် လျော်ညီစွာ ထုတ်ပြန်ရန်၊ ထိုအချက်အလက်များနှင့် တခြားဖော်ပြချက်ပါဂင်သည့် သတင်းအချက်အလက်များအား လွတ်လပ်စွာအသုံးပြုနိုင်သော ပုံစံဖြင့် လုပ်ဆောင်ရန်နှင့် ထိုအချက်အလက်များ၏ အသုံးပြုသူများနှင့် တွဲဖက်လုပ်ကိုင်ခြင်းသာ အလေးထားလုပ်ဆောင်ရမည်ဖြစ်သည်။

သတင်းအချက်အလက် အရင်းအမြစ်များအား စီမံခန့်ခွဲခြင်းရှိ အဖွဲ့အစည်းများ၏ သတ်မှတ်ချက်များ အသေးစိတ်ကို နောင်အပိုင်းတွင် ဖော်ပြထားပါသည်။

မူဝါဒဆိုင်ရာ သတ်မှတ်ချက်

ယခုအပိုင်း အပိုင်း (၁) နှင့် အပိုင်း (၂) ရှိ သတ်မှတ်ချက်များကို အချက်အလက်အသစ်များ စုဆောင်းခြင်း၊ ဖန်တီးခြင်းနှင့် စနစ်တိုးတက်အောင် လုပ်ဆောင်ခြင်းများသာမက လက်ရှိတည်ရှိနေသော သတင်းအချက်အလက်စနစ်များအား ပိုမိုတိုးတက်အောင်လုပ်ဆောင်မည့် စီမံကိန်းများအတွက် အသုံးပြုရမည်ဖြစ်သည်။ အပိုင်း (၃) ရှိ သတ်မှတ်ချက်များအား အဖွဲ့အစည်း၏ သတင်းအချက်အလက်စနစ်များအတွင်း အသုံးပြုထားသည့် အချက်အလက်မှတ်တမ်းအားလုံးကို စီမံခန့်ခွဲခြင်းအတွက် အသုံးပြုရမည်ဖြစ်သည်။ အဖွဲ့အစည်းအားလုံးသည် တန်ဖိုးမြင့်မားသော အချက်အလက်မှတ်တမ်းအား ဦးစားပေးလုပ်ဆောင်ကာ ယခု မူဝါဒတွင် ဖော်ပြထားသော လွတ်လပ်စွာ

လုပ်ဆောင်နိုင်ခြင်း နည်းလမ်းများကို အသုံးပြုကာ လက်ရှိတည်ရှိနေသော အချက်အလက်မှတ်တမ်းများအား ရယူနိုင်ခြင်းနှင့် အသုံးပြုနိုင်ခြင်းအား တိုးတက်လာစေရန်အတွက် အားပေးအားမြှောက်လုပ်ဆောင်ရမည်ဖြစ်သည်။

အစိုးရ အဖွဲ့အစည်းအားလုံးသည် အစိုးရ၏ လွတ်လပ်စွာ အချက်အလက်များအသုံးပြုနိုင်ရေးအတွက် လုပ်ဆောင်မှုများအား ခိုင်မာစေရန်နှင့် အချက်အလက်အရင်းအမြစ်များ၏ စီမံခန့်ခွဲမှုအား တိုးတက်စေရန်အတွက် အောက်ပါလုပ်ဆောင်မှုများအား ဆောင်ရွက်ရမည်ဖြစ်သည်။

၁။ အချက်အလက်များ၏ လုပ်ဆောင်မှုနှင့် မျှဝေသုံးစွဲမှုအား အထောက်အပံ့ဖြစ်စေသော နည်းလမ်းဖြင့် စုဆောင်ခြင်း သို့မဟုတ် ဖန်တီးခြင်း

အထူးသဖြင့် အဖွဲ့အစည်းများသည် အောက်ပါတို့ကို လုပ်ဆောင်ရမည်ဖြစ်သည်။

a. ကွန်ပြူတာမှနားလည်သော အချက်အလက်များနှင့် လွတ်လပ်စွာ ကူးယူနိုင်သော ပုံစံများအား အသုံးပြုခြင်း အချက်အလက်များအား အလိုအလျောက်ပင် အီလထရောနစ်နည်းအရ စုဆောင်းမှုပြုနေစဉ်အတွင်း အီလထရောနစ်ကိရိယာများနှင့် တယ်လီဖုန်း သို့မဟုတ် စာရွက်အခြေပြု သတင်းအချက်အလက်များ စုဆောင်းခြင်းများနှင့် ဆက်သွယ်လုပ်ဆောင်ရာတွင် ကွန်ပြူတာမှနားလည်သောအချက်အလက်များ၊ လွတ်လပ်စွာ ကူးယူနိုင်သော ပုံစံများအား အသုံးပြုရမည်ဖြစ်သည်။ ဥပဒေ၏ ခွင့်ပြုထားမှုများအရ လွတ်လပ်စွာကူးယူနိုင်သော ပုံစံများသည် တစ်ဦးတစ်ယောက်၏ ပိုင်ဆိုင်မှုနှင့် သက်ဆိုင်ခြင်းမရှိရဘဲ ပြည်သူလူထု ရယူအသုံးပြုနိုင်ရမည်ဖြစ်သည်။
b. အချက်အလက်စံနှုန်းများအား အသုံးပြုခြင်း အချက်အလက်များအတွက် ကိုက်ညီမှုရှိသော စံနှုန်းများနှင့် လမ်းညွှန်ချက်များအား ဖော်ပြလုပ်ဆောင်သွားမည်ဖြစ်သည်။ အချက်အလက်များ စုဆောင်းခြင်း သို့မဟုတ် ဖန်တီးပြီးသည်နှင့် တစ်ပြိုင်နက် ထိုစံနှုန်းများ၊ လမ်းညွှန်များအား အသုံးပြုနိုင်မည်ဖြစ်ပြီး အချက်အလက်များ၏ ပေါင်းစည်းလုပ်ဆောင်ခြင်းနှင့် လွတ်လပ်စွာအသုံးပြုနိုင်ခြင်းအား တိုးမြှင့်စေရန်အတွက် ထိုစံနှုန်းများ၊လမ်းညွှန်ချက်များအား အဖွဲ့အစည်းများသည် အသုံးပြုရမည်ဖြစ်သည်။ ကိုက်ညီမှုမရှိသော အချက်အလက်မှတ်တမ်းပုံစံများအား အစောပိုင်း ရရှိအသုံးပြုနိုင်ခြင်းသည် မည်သို့ပင်ဖြစ်စေကာမူ

ထိုအချက်အလက်အသုံးပြုသူများအတွက် တန်ဖိုးတစ်စုံတစ်ရာ ဖြစ်ထွန်းနိုင်သဖြင့် လိုအပ်သော စံနှုန်းများနှင့် အပြည့်အဝ မကိုက်ညီသော တစ်ဦးတစ်ယောက်၏ အချက်အလက်မှတ်တမ်းများ ထုတ်ပေးခြင်းကိုလည်း ခွင့်ပြုပေးရမည်ဖြစ်သည်။ သို့သော် စံနှုန်းများမှ သွေဖည်နေသည့် အချက်များအား ရှင်းပြရမည်ဖြစ်ပြီး စံနှုန်းများနှင့်ကိုက်ညီအောင် လုပ်ဆောင်မည်ဟူသော သဘောတူညီမှုအား ဖော်ပြထားရမည်ဖြစ်သည်။

c. လွတ်လပ်စွာအသုံးပြုခွင့်ရသော လိုင်စင်များ အသုံးပြုခြင်း
စုဆောင်းထားသောသတင်းအချက်အလက်များ သို့မဟုတ် ဖန်တီးထားသော သတင်းအချက်အလက်များအတွက် လွတ်လပ်စွာအသုံးပြုခွင့်ရသော လိုင်စင်များ အသုံးပြုရမည်ဖြစ်သည်။ ထိုမှသာ ပြည်သူလူထုအတွက် ဖော်ဆောင်သော အချက်အလက်များသည် မိတ်တူကူးရာတွင်၊ ထုတ်ပေးရာတွင်၊ ဖြန့်ပေးရာတွင် သို့မဟုတ် တခြား စီးပွားရေးအဖြစ် သို့မဟုတ် စီးပွားရေးမဟုတ်သော လုပ်ဆောင်မှုများအတွက် အသုံးပြုရာတွင် မည်သည့် အကန့်အသတ်မှ ရှိနေမည်မဟုတ်ပေ။

d. ဖော်ပြချက်ပါဝင်သည့် အချက်အလက်များအား ထုတ်ပေးခြင်း အချက်အလက်စာရင်း တစ်ခုချင်းစီနှင့် ဆက်စပ်နေသော ဖော်ပြချက်ပါဝင်သည့် အချက်အလက်များအား ထုတ်ပေးရမည်ဖြစ်သည်။ ထိုအချက်အလက်များတွင် မူလအချက်အလက်များ၊ ချိတ်ဆက်ထားသည့် အချက်အလက်များ၊ ပထဝီမြေပြင်အခြေအနေပြ နေရာများ၊ အချက်အလက်၏ အရည်အသွေးများနှင့် အချက်အလက်မူရင်း၏ ခိုင်မာမှုအား ပြည်သူလူထုကဆုံးဖြတ်နိုင်ရန်အတွက် အချက်အလက်စာရင်းများကြား ဆက်သွယ်မှုများကို ဖော်ပြပေးနိုင်သည့် တခြားသက်ဆိုင်ရာ ဖော်ပြချက်များ ပါဝင်ရမည်ဖြစ်သည်။ ယေျဘူယျ ဖော်ပြချက်ပါဝင်သည့် အချက်အလက်များအား စံနှုန်းများ၊ သီးခြားသတ်မှတ်ချက်များ သို့မဟုတ် မတူညီသော နယ်ပယ်များရှိ တိုးတက်ပြောင်းလဲမှု ပုံစံများ (ငွေကြေး၊ ကျန်းမာရေး၊ ဥပဒေစိုးမိုးရေး) အပေါ် တွင်မူတည်ကာ ချဲ့ထွင်လုပ်ဆောင်နိုင်ပေသည်။

၂။ ပေါင်းစည်းလုပ်ဆောင်ခြင်းနှင့် သတင်းအချက်အလက် ရယူနိုင်ခြင်းအား အထောက်အကူဖြစ်စေသည့် သတင်းအချက်အလက်စနစ်အား တည်ဆောက်ခြင်း သို့မဟုတ် ခေတ်မှီအောင်လုပ်ဆောင်ခြင်း ပြုလုပ်ရမည်ဖြစ်သည်။ စနစ်၏ ဒီဇိုင်းသည်စကေးအရ ပြောင်းလဲနိုင်မှု၊ ပြောင်းလဲလုပ်ဆောင်နိုင်မှု၊

မူလဒီဇိုင်းအပြင် ဖြစ်နိုင်သော အသုံးပြုမှုများအပါအဝင် အတွင်းပိုင်းနှင့်
အပြင်ပိုင်းလိုအပ်ချက်များပြောင်းလဲခြင်းကဲ့သို့သော အမျိုးမျိုးအသုံးပြုမှုများအတွက်သာမက
ပုံစံအမျိုးမျိုးဖြင့် အချက်အလက်များထုတ်ယူခြင်းတွင်လည်း လွယ်ကူမှုရရှိရမည်ဖြစ်သည်။

၃။ အချက်အလက်များ စီမံခန့်ခွဲခြင်းနှင့် ထုတ်ပြန်ခြင်း လုပ်ဆောင်မှုများအား ခိုင်မာစေခြင်း ယခု မူဝါဒ ထုန်ပြန်သည့်ရက်စွဲမှနေ၍ ၆ လအတွင်းတွင် အဖွဲ့အစည်းများသည် ၄င်းတို့၏ အချက်အလက်စီမံခန့်ခွဲခြင်းနှင့် ထုတ်ပြန်ခြင်းလုပ်ဆောင်မှုများအား ခိုင်မာစေရန်အတွက် တည်ရှိပြီးသား မူဝါဒများနှင့် လုပ်ထုံးလုပ်နည်းများအား မည်သည့် သင့်လျော်ရာ ပြန်လည်တည်းဖြတ်မှုများလုပ်ဆောင်ခြင်း ပြန်လည်ဆန်းစစ်ခြင်းများလုပ်ဆောင်ခြင်းအား ပြုလုပ်ရမည်ဖြစ်သည်။ ယခု မူဝါဒရှိ သတ်မှတ်ချက်များနှင့် ကိုက်ညီအောင်လုပ်ဆောင်ရမည့်အပြင် အောက်ပါလုပ်ဆောင်မှုများကိုလည်း ဆောင်ရွက်ရမည်ဖြစ်သည်။

a. လုပ်ငန်းဆိုင်ရာ အချက်အလက် စာရင်းတစ်ခုအား ဖန်တီးခြင်းနှင့် ထိန်းသိမ်းခြင်း အစိုးရ အဖွဲ့အစည်းအားလုံးသည် အဖွဲ့အစည်း၏ သတင်းအချက်အလက်စနစ်တွင် အသုံးပြုသော အချက်အလက်မှတ်တမ်းတွင် ထည့်သွင်းလုပ်ဆောင်ရန်အတွက် လုပ်ငန်းဆိုင်ရာ အချက်အလက်စာရင်းတစ်ခုအား တည်ဆောက်ရမည်ဖြစ်သည်။ ထိုစာရင်းသည် မည်သည့်အချက်များသည် ပြည်သူလူထုထံသို့ရောက်ရှိသည်နှင့် မည်သည့်အချက်အလက်များ ပြသည်သူလူထုအသုံးပြုရန်အတွက် အဆင်သင့်ရှိသည် စသော အချက်အလက်မှတ်တမ်းများအားလုံးကို ဖော်ပြမည်ဖြစ်သည်။
b. ပြည်သူလူထုဆိုင်ရာ အချက်အလက် စာရင်းအား ဖန်တီးခြင်းနှင့် ထိန်းသိမ်းခြင်း လုပ်ငန်းဆိုင်ရာအချက်အလက်စာရင်းရှိ ပြည်သူလူထုအသုံးပြုနိုင်သော အချက်အလက်မှတ်တမ်းအားလုံးအား အဖွဲ့အစည်း၏ တရားဝင်ဂျက်ဆိုဒ်တွင် ကွန်ပြူတာမှနားလည်သော ပုံစံဖြင့် စာရင်းဖော်ပြထားရမည်ဖြစ်သည်။ ထိုမှသာ National portal ၏ အလိုအလျောက် စုဆောင်းခြင်းကို လုပ်ဆောင်နိုင်မည်ဖြစ်သည်။ အချိန်တစ်ခုပြီးသည့်နောက်တွင် အဖွဲ့အစည်းအားလုံး၏ ပြည်သူလူထုအသုံးပြုနိုင်စေရန် လုပ်ဆောင်ထားသော အချက်အလက်မှတ်တမ်းအားလုံးသည် ပါဝင်လာမည်ဖြစ်သည်။
c. အချက်အလက်များထုတ်ပြန်ရာတွင် အဆင်ပြေချောမွေ့စေရန်အတွက် အသုံးပြုသူများနှင့် ဆက်သွယ်ပြောဆိုခြင်း အချက်အလက်မှတ်တမ်းများ ထုတ်ပြန်ရာတွင် အရေးကြီးမှုအလိုက်

စီစဉ်လုပ်ဆောင်ရန်နှင့် ထုတ်ပြန်ခြင်းအတွက် အသင့်လျော်ဆုံး ပုံသံအား ဆုံးဖြတ်ရန်အတွက် အသုံးပြုသူများနှင့် ဆက်သွယ်ပြောဆိုခြင်းများ လိုအပ်ပါသည်။ ဥပမာအနေဖြင့် ဆော့ဖ်ဝဲကျွမ်းကျင်သူများ စိတ်ဝင်စားနိုင်သော ပမာဏများပြားသည့် အချက်အလက်မှတ်တမ်းအား များပြားသော ဒေါင်းလုဒ်များနှင့် Application Programming Interfaces (APIs) အသုံးပြုကာ ထုတ်ပြန်ရမည်ဖြစ်သည်။

d. ထိရောက်သော အချက်အလက် ထုတ်ပြန်ခြင်းဆိုင်ရာ နည်းလမ်းများအတွက် ကဏ္ဍများနှင့် တာဝန်များအား ရှင်းလင်းဖော်ပြခြင်း ထိရောက်သော အချက်အလက်ထုတ်ပြန်ခြင်းဆိုင်ရာ နည်းလမ်းများအတွက် အစိုးရအဖွဲ့အစည်းများအားလုံးကို ကဏ္ဍများနှင့် တာဝန်များအား ရှင်းလင်းစွာခန့်အပ်ထားရမည်။ ၎င်းတွင်

   i. ဌာနတွင်း တာဝန်ရှိသူများ နှင့် ပြည်သူလူထုထံသို့ လွတ်လပ်စွာအသုံးပြုနိုင်သော အချက်အလက်များ၏ အရေးကြီးသော တန်ဖိုးအား ဆက်သွယ်ပြောကြားခြင်း
   ii. ပြန်လည်မေးမြန်းခြင်းများ သို့မဟုတ် အကြံပြုချက်များအား ပြန်လည်ဖြေဆိုရန်အတွက် ဆက်သွယ်ရန်နေရာတစ်ခုနှင့်အတူ ထုတ်ပြန်ထားသော အချက်အလက်များသည် လွတ်လပ်စွာအသုံးပြုနိုင်ခြင်း။
   iii. အသုံးချဆော့ဖ်ဝဲများနှင့် ဝန်ဆောင်မှုများ ဖန်တီးလုပ်ဆောင်ရာတွင် အချက်အလက်များကို အသုံးပြုရန်အတွက် စီးပွားရေးနှင့် လူမှုအဖွဲ့အစည်းများအား အားပေးအားမြှောက်ပြုခြင်း။
   iv. ပိုမိုကောင်းမွန်သော လွတ်လပ်စွာအသုံးပြုနိုင်သော အချက်အလက် လုပ်ဆောင်မှုများရှိသည့် အစိုးရဌာန သို့မဟုတ် ရုံးခန်းများမှနေ၍ အကောင်းဆုံး လုပ်ဆောင်မှုများအား ရယူခြင်း။
   v. ပုဂ္ဂိုလ်ဆိုင်ရာအချက်အလက်များနှင့် လုံခြုံစိတ်ချခြင်းများ မထိခိုက်စေရန်အတွက် တခြားတာဝန်ရှိသူများနှင့် တွဲဖက်လုပ်ကိုင်ခြင်း။
   vi. ဌာနရှိ ထိခိုက်လွယ်သော အချက်အလက်များနှင့် လုံခြုံရေးလုပ်ဆောင်မှုများ ထုတ်ပြန်ခြင်း အန္တရာယ်များအား စစ်ဆေးရန်အတွက် လုံခြုံရေးအဖွဲ့များနှင့် တွဲဖက်လုပ်ကိုင်ခြင်း။

၄။ အချက်အလက်အားလုံးရှိ ပုဂ္ဂိုလ်ရေးဆိုင်ရာအချက်အလက်များ၊ လျှို့ဝှက်ထားသည့်အချက်အလက်များနှင့် လုံခြုံရေးအား အာမခံနိုင်သော လုပ်ဆောင်မှုများအား

အားဖြင့်ညှိဆောင်ရွက်ခြင်း။ ပြည်သူလူထုအား ပြသနိုင်ခြင်းရှိမရှိ၊ လွတ်လပ်စွာ လုပ်ဆောင်နိုင်ခြင်းနှင့် ကိုက်ညီမှုရှိမရှိနှင့် ဥပဒေကခွင့်ပြုထားခြင်းရှိမရှိ၊ ပုဂ္ဂိုလ်ရေးဆိုင်ရာအချက်အလက်များနှင့် လုံခြုံရေးကန့်သတ်ချက်များနှင့် ညှိစွန်းခြင်းရှိမရှိအား စစ်ဆေးရန်အတွက် စုဆောင်းထားသော အချက်အလကအားလုံး သို့မဟုတ် ဖန်တီးထားသော အချက်အလက်အားလုံးအား ခွဲခြမ်းစိတ်ဖြာခြင်းလုပ်ဆောင်ရမည်ဖြစ်သည်။ အကယ်၍ ပြည်သူလူထုအတွင် အသုံးပြုနိုင်ခြင်းမရှိပါက အဖွဲ့အစည်းသည် ထိုအကြောင်းပြချက်များအား ဖော်ပြရမည်ဖြစ်သည်။

၅။ အချက်အလက်စီမံခန့်ခွဲမှု လုပ်ဆောင်မှုအားလုံးတွင် လိုအပ်သော ပေါင်းစည်းလုပ်ဆောင်ခြင်းနှင့် လွတ်လပ်စွာရယူနိုင်ခြင်းများအတွက် ပေါင်းစည်းဆောင်ရွက်ခြင်း အဖွဲ့အစည်းအားလုံးသည် သူတို့၏ အချက်အလက်စီမံခန့်ခွဲမှုလုပ်ဆောင်ချက်များအား အဖွဲ့အစည်း၏ စီမံဆောင်ရွက်မှု၊ ငွေကြေးလည်ပတ်မှု၊ ထိန်းသိမ်းစောင့်ရှောက်မှုနှင့် ငွေကြေးစီမံခန့်ခွဲမှု စသည်တို့၏ အဓိက လုပ်ဆောင်မှုများအတွင်းသို့ ပေါင်းထည့်ရမည်ဖြစ်သည်။ သူတို့၏ အားလုံးသောလုပ်ဆောင်မှုအတွင်း ယခု မူဝါဒတွင် ပြဋ္ဌာန်းထားသည့် ပေါင်းစည်းလုပ်ဆောင်မှုနှင့် လွတ်လပ်စွာအချက်အလက်များအသုံးပြုနိုင်မှု၏ လိုအပ်ချက်များကိုလည်း အဖွဲ့အစည်းအတွင်း အဓိကတာဝန်အနေဖြင့် ထားရှိရမည်ဖြစ်သည်။

လက်တွေ့လုပ်ဆောင်ခြင်း

ယခုအပိုင်းတွင် မူဝါဒ၏ ယေဘူယျက်တွေ့လုပ်ဆောင်မှုများသာမက အဖွဲ့အစည်းများ၏ အဓိက အစိတ်အပိုင်းများ၏ အရေးကြီးသော လက္ခဏာများအား ဖော်ပြထားပါသည်။

1. တာဝန်နှင့် ဝတ္တရားများ

ဗဟိုအဖွဲ့ ကောင်းမွန်စွာလုပ်ဆောင်နိုင်သော လွတ်လပ်စွာအသုံးပြုနိုင်သည့် အချက်အလက်ဆိုင်ရာ လမ်းညွှန်တစ်ခုရှိ လိုအပ်သော တည်ဆောက်ပုံများရရှိစေရန်အတွက် ပင်မ အဖွဲ့အစည်းများပါဝင်သော ဗဟိုအဖွဲ့တစ်ခုအား ဖွဲ့စည်းရမည်ဖြစ်သည်။ ထိုဗဟိုအဖွဲ့တွင် ITCSD သည် ဥက္ကဋ္ဌနေရာတွင်ရှိမည်ဖြစ်ပြီး အဖွဲ့၏ လုပ်ဆောင်မှုအားလုံးနှင့် ပူးပေါင်းလုပ်ဆောင်သွားမည်ဖြစ်သည်။ အောက်တွင်ဖော်ပြထားသော အဖွဲ့များရှိ ကိုယ်စားလှယ်များနှင့်လည်း ဖွဲ့စည်းသွားမည်ဖြစ်သည်။

a. ဗဟို ကိန်းဂဏန်းအချက်အလက်ဆိုင်ရာ အဖွဲ့အစည်း၊ စီမံကိန်းနှင့် ဘဏ္ဍာရေးဂန်ကြီးဌာန
b. ပြန်ကြားရေး ဂန်ကြီးဌာန
c. တန်ဖိုးမြင့်မားသော အချက်အလက်မှတ်တမ်းများရှိသည့် တခြားရွေးချယ်ထားသည့် အဖွဲ့အစည်းများ

ဗဟိုအဖွဲ့သည် အောက်ပါလုပ်ငန်းများအတွက် တာဂန်ရှိမည်ဖြစ်သည်။

a. လွတ်လပ်စွာအသုံးပြုနိုင်သော အချက်အလက်များဆိုင်ရာ မူဂါဒ ခြုံငုံသုံးသပ်ခြင်း
b. လွတ်လပ်စွာအသုံးပြုနိုင်သော အချက်အလက်များ အကောင်အထည်ဖော်သည့် အဖွဲ့အစည်းအားလုံးနှင့် ဌာနအားလုံးအား အသေးစိတ်လမ်းညွှန်ချက်များ ထုတ်ပေးခြင်း
c. လွတ်လပ်စွာအသုံးပြုနိုင်သော အချက်အလက်များအတွက် စီးပွားရေးနှင့် နည်းပညာဆိုင်ရာ စံနှုန်းများသတ်မှတ်ပေးခြင်း
d. ့ပရိုဂရမ်များ သတ်မှတ်ဖော်ပြခြင်းနှင့် ပရိုဂရမ် စီမံခန့်ခွဲမှု၏ ခြုံငြုံသုံးသပ်မှုများ
e. မဟာဗျူဟာချမှတ်ခြင်းနှင့် အရေးပါမှုအလိုက် အစီအစဉ်ချမှတ်ခြင်း
f. အစိုးရ၏ အတွင်းပိုင်းနှင့် အပြင်ပိုင်းအတွင်း အရည်အသွေးတိုးတက်စေနိုင်သော အစီအစဉ်များ ဖန်တီးလုပ်ဆောင်ခြင်း
g. သက်ဆိုင်ရာ အဖွဲ့အစည်းများမှနေ၍ ထည့်သွင်းစဉ်းစားထားသော အချက်အလက်များအား တောင်းခံခြင်းများနှင့် ထိုအချက်အလက်များအား ပြည့်မှီအောင်လုပ်ဆောင်နိုင်ရန်အတွက် အတူတကွ ပူးပေါင်းလုပ်ဆောင်ခြင်း
h. လွတ်လပ်စွာအသုံးပြုနိုင်သော အချက်အလက်ဆိုင်ရာလမ်းညွှန်၏ တိုးတက်မှုနှင့် လည်ပတ်ဆောင်ရွက်မှု
i. လွတ်လပ်စွာအသုံးပြုနိုင်သော အချက်အလက်ဆိုင်ရာ လမ်းညွှန်ရှိ အချက်အလက်မှတ်တမ်းများနှင့် ဆက်စပ်နေသော ဖော်ပြထားသည့်အချက်အလက်များအတွက် စံနှုန်းများအား ဖန်တီးလုပ်ဆောင်ခြင်းနှင့် ခိုင်မာစေခြင်း

j. ပုဂ္ဂိုလ်ရေးဆိုင်ရာအချက်အလက်များ၊ လုံခြုံရေးစစ်ဆေးခြင်းများ၊ အမည်မဖော်ပြဘဲ လျှို့ဝှက်ထားခြင်းများနှင့် တခြားလိုအပ်သော လုပ်ဆောင်မှုများပါဝင်သည့် အချက်အလက်ထုတ်ပြန်မှု ဆုံးဖြတ်ချက်များနှင့် ပြင်ဆင်မှုများအား ကူညီပေးခြင်း

ယခုမူဝါဒအား လက်တွေ့အကောက်အထည်ဖော်ဆောင်နိုင်စေရန်အတွက် အဖွဲ့အစည်းအားလုံးသည် နည်းစနစ်တကျ လုပ်ဆောင်ရမည်ဖြစ်ပြီး အစောဆုံးကာလ သို့မဟုတ် အရေးကြီးသော ရည်ရွယ်ချက်များအား ထောက်ကူပေးနိုင်သည့် ထိုအခြေခံလုပ်ဆောင်မှုများအား ပထမဦးစွာ လက်တွေ့အကောင်အထည်ဖော်ရမည်ဖြစ်သည်။ ၎င်းတို့၏ အဓိက၊ အမြဲမပြတ်လုပ်ဆောင်ရမည့် တာဝန်များမှာ -

a. သက်ဆိုင်ရာ အဖွဲ့အစည်းခေါင်းဆောင် သို့မဟုတ် တာဝန်လွှဲပြောင်းပေးအပ်ထားသောသူမှနေ၍ တရားဝင်ခွင့်ပြုထားသည့်အတိုင်း အချက်အလက်များကို ထုတ်ပြန်ခြင်း
b. ဗဟိုအဖွဲ့နှင့်ဆက်သွယ်မည့် အဖွဲ့အစည်းအတွင်းရှိ ဆက်သွယ်ရေး လူအားခန့်အပ်ခြင်းနှင့် လိုအပ်သော အချက်အလက်ထုတ်ပြန်ခြင်းများ ပြုလုပ်ခြင်း
c. သဘောတူညီထားသော အချက်အလက်အားလုံးအား ထုတ်ပြန်ခြင်းနှင့် ပြဿနာတစ်စုံတစ်ခု သို့မဟုတ် အခက်အခဲတစ်ခုရှိပါက ဗဟိုအဖွဲ့အား အကြောင်းကြားခြင်း
d. လုပ်ငန်းဆိုင်ရာ အချက်အလက် စာရင်းအား ဖြန့်ဝေခြင်းနှင့် တင်ပြပေးခြင်း

2. အရင်းအမြစ်များ

အဖွဲ့အစည်း၏ လက်ရှိတည်ရှိနေသော အချက်အလက်များအား စီမံဆောင်ရွက်ခြင်း ဖြစ်စဉ်အပေါ် မူတည်ကာ မူဝါဒအား အကောင်အထည်ဖော်ခြင်းသည် ရင်းနှီးမြှုပ်နှံမှုများ လိုအပ်မည်ဖြစ်သည်။ ၎င်းတို့အား လက်ရှိ ဖြစ်စဉ်ကို စစ်ဆေးလေ့လာရန် အားပေးအားမြှောက်ပြုရမည်ဖြစ်ပြီး ပြည်သူလူထု၏ ဘဏ္ဍာငွေအား အထိရောက်ဆုံးအသုံးပြုနိုင်သည့် အခွင့်အရေးများ ဖော်ဆောင်နိုင်သည့် အခြေအနေအား ဖော်ပြပေးရမည်ဖြစ်သည်။ ဤမူဝါဒရှိ လိုအပ်ချက်များအား ပြည့်မှီသည့် ဖြစ်လာနိုင်သော ရင်းနှီးမြှုပ်နှံမှုများ၊ ကိရိယာများနှင့် လိုအပ်သော

အရင်းအမြစ်များအား ၎င်းတို့၏ ငွေကြေးအစီအစဉ်နှင့် လျာထားငွေ လုပ်ဆောင်မှုများမှတစ်ဆင့် အကူအညီ တောင်းခံရမည်ဖြစ်သည်။

3. တိုင်းတာဆောင်ရွက်မှုနှင့် ပြန်လည်ဆန်းစစ်မှု

ဤမူဝါဒတွင် ဖော်ပြထားသော သတ်မှတ်ချက်များအလိုက် တိုးတက်မှုအား တိုင်းတာရန်အတွက် ပဟိုအဖွဲ့သည် တိုင်းတာဆောင်ရွက်မှုနှင့် အစီရင်ခံခြင်း မူဘောင်အား တိုးတက်အောင်လုပ်ဆောင်ရမည်ဖြစ်သည်။ လွတ်လပ်စွာ အသုံးပြုနိုင်သော အချက်အလက်ဆိုင်ရာ လမ်းညွှန်အား ပုံမှန်တိုင်းတာခြင်းများဖြစ်သည့် ခရီးသည် အရေအတွက်၊ အချက်အလက်မှတ်တမ်းအရေအတွက်၊ အချက်အလက်မှတ်တမ်းများအား ဒေါင်းလုပ်ဆွဲခြင်း အရေအတွက်နှင့် အမျိုးအစားများ၊ လမ်းညွှန်အား အချက်အလက်များပံ့ပိုးပေးသော အဖွဲ့အစည်းအရေအတွက်၊ API အသုံးပြုမှု၊ စွန့်ဦးတီထွင်သူ အရေအတွက်၊ စာရင်းသွင်းထားသော စီးပွားရေးလုပ်ငန်းများ သို့မဟုတ် ဆော့ဖ်ဝဲကျွမ်းကျင်သူများ၊ ရရှိသောအချက်အလက်များအတွက် တောင်းခံမှုအရေအတွက်၊ ပြန်လည်အကြံပြုခြင်းများနှင့် တခြား လူမှုရေးဆိုင်ရာလုပ်ဆောင်မှုများ စသည်တို့နှင့် တိုင်းတာဆောင်ရွက်နိုင်သည်။

ဤမူဝါဒအား အဖွဲ့အစည်းများနှင့် အချက်အလက်အသုံးပြုသူများထံမှရရှိသော အတွေ့အကြုံများ မှတ်ချက်များအလိုပ် ပုံမှန် ဆန်းစစ်ရမည်ဖြစ်သည်။

အပိုင်း (၂) အီလက်ထရောနစ်ကုန်သွယ်မှုနှင့် ဆက်စပ်နေသော မူဝါဒများ

နောက်ခံအကြောင်းအရာ

ယခုဖော်ပြထားသည်မှာ အမျိုးသားဆိုင်ရာ အီလက်ထရောနစ် ကုန်သွယ်မှု မူဝါဒဖြစ်ပြီး အီလက်ထရောနစ်ကုန်သွယ်ရေးလုပ်ငန်းစဉ် ချမှတ်လမ်းညွှန်မှုဆိုင်ရာ ကော်မတီ (E- Commerce Steering Committee) နှင့်အတူ ပေါ်ထွက်လာခြင်းဖြစ်သည်။ (မြန်မာ Cyber ဥပဒေ၊ အပိုင်း (၄) တွင်ကြည့်ရှုပါ) မြန်မာနိုင်ငံအတွင်း အီလထရောနစ်ကုန်သွယ်မှုများ လွယ်ကူချောမွေ့စေရန်အတွက် ဤကော်မတီသည် ပြည်သူလူထုအတွက် ဦးဆောင်အဖွဲ့အစည်းအနေဖြင့် လုပ်ဆောင်နေခြင်းဖြစ်သည်။ ထိုကဲ့သို့ အသင်းအဖွဲ့ရှိခြင်းဖြင့် အီလက်ထရောနစ်ကုန်သွယ်မှု တိုးတက်စေရန်နှင့် အသုံးပြုစေရန်အတွက် အားပေးအားမြှောက်ပြုသော အခြေအနေများအား ဥပဒေ၊လုပ်ထုံးလုပ်နည်းများနှင့် မူဝါများဖန်တီးကာ လုပ်ဆောင်ရမည်ဖြစ်သည်။ မြန်မာနိုင်ငံ၏ စီးပွားရေးတိုးတက်မှုများနှင့် လူမှုအသိုက်အဝန်းတိုးတက်မှုများအား မောင်းနှင်ပေးနိုင်သော သတင်းအချက်အလက်နှင့် နည်းပညာများ တိုးတက်လာစေရန်အတွက် ထိုလုပ်ဆောင်မှုများက လုပ်ဆောင်ပေးနိုင်မည်ဖြစ်သည်။

အီလက်ထရောနစ် ကုန်သွယ်မှု ကိစ္စရပ်များရှိ မတူညီသော အခြေအနေများကြောင့် Cyber လုံခြုံရေးအမျိုးအစားရှိ အစိတ်အပိုင်း (၂) ခုဖြစ်သော C3 E- Authentication နှင့် C4 E-Signatures အား ယခု မူဝါဒတွင် ထည့်သွင်းလုပ်ဆောင်ထားပါသည်။ တူညီသောအကြောင်းအရင်းများအတိုင်းပင် အီလက်ထရောနစ် ကုန်သွယ်ရေး လုပ်ငန်းစဉ်ဆိုင်ရာ ချမှတ်ရေးအဖွဲ့သည် အောက်ပါ အဖွဲ့များနှင့်အတူ ပူးပေါင်းလုပ်ဆောင်သွားမည်ဖြစ်သည်။

1. e-Government ဦးစီးကော်မတီ(e-Government Steering Committee)
2. အီလထရောနစ် အမှတ်သင်္ကေတ လုပ်ဆောင်ရေး ကော်မတီ (e-ID Working Commiittee)
3. စားသုံးသူကာကွယ်ရေးဆိုင်ရာ ဗဟိုကော်မတီ (CPCC)
4. ဒစ်ဂျစ်တယ်စီးပွားရေးဖွံ့ဖြိုးတိုးတက်မှု ကော်မတီ (DEDC)
5. Ministry of Labour, Immigration and Population
6. ကုန်သွယ်ရေး ဝန်ကြီးဌာနရှိ စားသုံးသူကာကွယ်ရေးဌာန
7. အကောက်ခွန် ဌာန

8. မြန်မာနိုင်ငံတော် ဗဟိုဘဏ်

အီလက်ထရောနစ် အခြေအနေဖြင့် နယ်စပ်ဖြတ်ကျော်ကာ သတင်းအချက်အလက်များလွှဲပြောင်းခြင်း (B 1)

1. ဤကော်မတီသည် အီလက်ထရောနစ်ကုန်သွယ်မှုနှင့် အွန်လိုင်းကုန်သွယ်မှု၏ အပိုင်းကဏ္ဍတွင်ရှိသော နယ်စပ်ဖြတ်ကျော် အချက်အလက်များ စီးဆင်းမှု၏ လုံခြုံရေးနှင့် စိတ်ချရေးတို့အတွက် ဖော်ဆောင်သွားမည်ဖြစ်သည်။
2. Cloud တွက်ချက်မှုအား သက်ဝင်စေခြင်း - ဤကော်မတီသည် ပြည်သူလူထုဆိုင်ရာ အပိုင်းကဏ္ဍများတွင် Cloud ၏ တွက်ချက်ခြင်းများကို အသုံးပြုခြင်းအား ဖော်ဆောင်သွားမည်ဖြစ်သည်။ (Cloud ၏ ပထမဦးဆုံး မူဝါဒတွင်ကြည့်ရှုပါ)
3. နိုင်ငံတကာနှင့် ကိုက်ညီမှုများ
    a. ဤကော်မတီသည် နယ်စပ်ဖြတ်ကျော် အချက်အလက်များစီးဆင်းမှုအား Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTTP) ကဲ့သို့သော ကမ္ဘာလုံးဆိုင်ရာစံသတ်မှတ်ချက်များနှင့် အညီ လုပ်ဆောင်သွားမည်ဖြစ်သည်။
    b. ဤကော်မတီသည် အချက်အလက်များ နယ်စပ်ဖြတ်ကျော်စီးဆင်းရာတွင် လိုအပ်သော အသုံးပြုသူများ၏ အချက်အလက်များအား ကာကွယ်မှုများအား ထိန်းညှိပေးနိုင်သည့် ခိုင်မာသော အချက်အလက်ကာကွယ်ရေး ဥပဒေအား ပြဋ္ဌာန်းသွားမည်ဖြစ်သည်။
    c. ဤကော်မတီသည် ခိုင်မာသော အချက်အလက်ကာကွယ်ရေး ဥပဒေတစ်ခု တိုးမြှင့်လုပ်ဆောင်နိုင်ရေးအတွက် ကုန်သွယ်ရေးပန်ကြီးဌာနလက်အောက်ရှိ စားသုံးသူကာကွယ်ရေးဆိုင်ရာ ဌာန၊ စားသုံးသူကာကွယ်ရေးဆိုင်ရာ ကော်မတီနှင့် ပုဂ္ဂိုလ်ရေးဆိုင်ရာ အချက်အလက်လုံခြုံရေး ကော်မရှင်တို့နှင့် ပူးပေါင်းလုပ်ဆောင်သွားမည်ဖြစ်သည်။
4. အချက်အလက်များ နယ်စပ်ဖြတ်ကျော် စီးဆင်းခြင်း
    a. ဤကော်မတီသည် အချက်အလက်များ ထားရှိရာနေရာအား ကန့်သတ်မှုမရှိစေရန် လုပ်ဆောင်မည်ဖြစ်သည်။

b. အချက်အလက်များ လိုက်လျောညီထွေဖြစ်စဉ်အား ပိုမိုလွယ်ကူစေရန်အတွက် ဤကော်မတီသည် အချက်အလက်များခွဲခြားရာတွင် မူဝါဒတစ်ခုအား လက်တွေ့အကောင်အထည်ဖော်ဆောင်သွားမည်ဖြစ်သည်။ (အထက်တွင်ကြည့်ပါ)

c. ဤကော်မတီသည် ဒေသခံလူများနှင့် နိုင်ငံခြားသားများကြား Cloud နှင့် အချက်အလက်ဆိုင်ရာ ပန်ဆောင်မှုရယူရာတွင် မည်သည့်ခွဲခြားမှုများမရှိစေရန်လုပ်ဆောင်သွားမည်ဖြစ်သည်။

5. ပုံမှန် တည်ငြိမ်မှုနှင့် လိုက်နာစေရန်လုပ်ဆောင်မှု

a. ဤကော်မတီသည် အွန်လိုင်းစီးပွားရေးလုပ်ငန်းများအား အနည်းဆုံးလိုအပ်ချက်များ၊ လိုင်စင်လုပ်ဆောင်ရမှု အနည်းဆုံးဖြင့် စီးပွားရေးစတင်နိုင်စေရန် လုပ်ဆောင်သွားမည်ဖြစ်သည်။

b. ဤကော်မတီသည် အောက်ပါတို့ကဲ့သို့သော နိုင်ငံတကာနှင့် ဒေသတွင်း မူဘောင်များနှင့် မြန်မာနိုင်ငံ၏ နယ်စပ်ဖြတ်ကျော် ဒေတာအချက်အလက်စီးဆင်းမှု မူဝါဒများ ကိုက်ညီမှုရှိစေရန် ဆောင်ရွက်သွားမည်ဖြစ်သည်:

i. ASEAN Framework on Digital Data Governane[30] နှင့် ASEAN Cross Broder Data Flow Mechanism ရှိ ဦးစားပေးမဟာဗျူဟာ (၂) ကဲ့သို့သော နိုင်ငံတကာနှင့် ဒေသတွင်း ကန့်သတ်မှုများအရ

ii. APEC Cross Border Privacy Rules (CBPR) system.[31]

အီလက်ထရောနစ်စနစ်ဖြင့် ငွေပေးချေမှု (B2)

1. ဘဏ်ပန်ဆောင်မှုများပိုမိုရရှိရန်နှင့် ပူးပေါင်းလည်ပတ်နိုင်ရန် ဤကော်မတီအနေဖြင့် ဘဏ္ဍာရေးပန်ဆောင်မှုလုပ်ငန်းကဏ္ဍ၊ မြန်မာနိုင်ငံတော် ဗဟိုဘဏ်တို့နှင့်အတူ (မိုဘိုင်းပိုက်ဆံငွေစုစာရင်း အပါအဝင်) ဘဏ်စုငွေစာရင်း ရှိသူ အသက် ၁၅ နှစ်အထက် ပုဂ္ဂိုလ်တစ်ဦးချင်းစီအရေအတွက် တိုးလာစေရန် လုပ်ဆောင်သင့်သည်။

[30] https://asean.org/storage/2012/05/6B-ASEAN-Framework-on-Digital-Data-Governance_Endorsed.pdf
[31] http://cbprs.org

2. ဤကော်မတီအနေဖြင့် ဘဏ်များအချင်းချင်း ငွေပေးချေမှုစနစ်များကို လက်ခံခြင်းနှင့် စတင်မိတ်ဆက်ခြင်းတို့ကို အရှိန်အဟုန်ဖြင့် ဆောင်ရွက်ရန်အတွက် ဘဏ္ဍာရေးဂန်ဆောင်မှုလုပ်ငန်း ကဏ္ဍ၊ မြန်မာနိုင်ငံတော် ဗဟိုဘဏ်တို့နှင့်အတူ လုပ်ဆောင်သင့်သည်။
3. ဤကော်မတီအနေဖြင့် ဘဏ်များအချင်းချင်း ငွေပေးချေမှု၊ ငွေလွှဲပြောင်းမှုများနှင့်ပတ်သက်ပြီး မည်သည့် ကန့်သတ်ချက်များကိုမဆို ဖယ်ရှားရန်အတွက် ဘဏ္ဍာရေးဂန်ဆောင်မှု လုပ်ငန်းကဏ္ဍ၊ မြန်မာနိုင်ငံတော် ဗဟိုဘဏ်တို့နှင့်အတူ လုပ်ဆောင်သင့်သည်။
4. ဘဏ်လုပ်ငန်းဆိုင်ရာ စည်းမျဉ်းဥပဒေများကို ပြန်လည်ဆန်းစစ် မွမ်းမံရမည်။ - ဤကော်မတီသည် ဘဏ္ဍာရေးဂန်ဆောင်မှု လုပ်ငန်းများရှိ အစုရှယ်ယာရှင်များနှင့် ပူးပေါင်းပြီး ပြည့်စုံသော အီလက်ထရောနစ် ကူးသန်းရောင်းဂယ်ရေးစည်းမျဉ်းဥပဒေတစ်ခု ပေါ်ပေါက်လာစေရန် လုပ်ဆောင်မှုစီမံကိန်းတစ်ခုတည်ဆောက်သင့်သည်။

စက္ကူလွတ် ကုန်သွယ်ရေး (B 3)

1. စက္ကူလွတ် သတိပေးချက်များနှင့် အီလက်ထရောနစ်ငွေပေးချေမှုများကို အစိုးရမှ သဘောတူ လက်ခံခြင်း။
    a. ဤကော်မတီအနေဖြင့် အခြားအစိုးရအဖွဲ့အစည်းများ (ဥပမာအားဖြင့် အစိုးရ အဖွဲ့အစည်းများ အကြား ငွေပေးချေမှုများ)၊ ပုဂ္ဂလိက လုပ်ငန်းများ (ဥပမာအားဖြင့် လိုင်စင်ငွေပေးချေမှုများနှင့် ခွင့်ပြုချက်များ) နှင့် နိုင်ငံသားများ (ဥပမာအားဖြင့် လိုင်စင်များ၊ အခွန်၊ လမ်းတံတားဖြတ်သန်းခများ စုဆောင်းခြင်း၊ လူမှုလုံခြုံရေး ငွေထုတ်ပေးမှုများ) စသည်တို့ကဲ့သို့သော ငွေလွှဲပြောင်းမှု ကိစ္စရပ်အားလုံးတွင် အီလက်ထရောနစ်စနစ် ငွေပေးချေမှုများကို အစိုးရအဖွဲ့အစည်းများအားလုံးမှ လက်ခံအသုံးပြုနိုင်ရန် သေချာစေသင့်သည်။
    b. ဤကော်မတီ အနေဖြင့် စက္ကူလွတ် စနစ်နှင့် ဒီဂျစ်တယ်စနစ် သတိပေးချက်များ ဥပမာအားဖြင့် အီးလ်မေးမှ တဆင့် သတိပေးချက်၊ မိုဘိုင်းကိရိယာမှ သတိပေးချက် စသည်တို့ကို အစိုးရအဖွဲ့အစည်းအားလုံးမှ လက်ခံသဘောတူသည်မှာ သေချာစေသင့်သည်။

c. အထူးသဖြင့် အစိုးရမှ နည်းပညာနှင့် အချင်းချင်းအပြန်အလှန်ချိတ်ဆက်မှု ပထမဆုံးမူဝါဒတစ်ခု အသုံးပြုရယူနိုင်ရန် အိုင်စီတီချဉ်းကပ်မှုနည်းလမ်းများကို စံကိုက်ပြုလုပ်ခြင်းနှင့် ပတ်သက်၍ အမျိုးသားအိုင်စီတီမဟာဗျူဟာနှင့် ကြိုးစားအားထုတ်မှုများ ကိုက်ညီစေရန် ဤကော်မတီအနေဖြင့် e-Government ဦးစီးကော်မတီနှင့် အတူလုပ်ဆောင်သင့်သည်။ အီလက်ထရောနစ် ကူးသန်းရောင်းဝယ်ရေးနှင့် စပ်လျဉ်းသော ကိစ္စရပ်များတွင် ငွေတောင်းခံလွှာများ ထုတ်ပေးခြင်း၊ ငွေပေးချေမှုများ လက်ခံပေးခြင်း၊ အပြန်အလှန်ချိတ်ဆက်မှု ဖွဲ့စည်းတည်ဆောက်ပုံ ရွေးချယ်ခြင်း၊ ဆော့ဖ်ဝဲလ်၊ ထိန်းသိမ်းမှုနှင့် အခြား e-Government စံနှုန်းများအတွက် အတူတကွ လုပ်ဆောင်နိုင်စေသည့် စံနှုန်းများကို ရရှိစေခြင်း စသည်တို့ပါဝင်မည်ဖြစ်သည်။

d. ဤကော်မတီသည် စက္ကူလွတ်ကုန်သွယ်ရေးမူဝါဒများကို အီလက်ထရောနစ် ကူးသန်းရောင်းဝယ်ရေးဆိုင်ရာ အာဆီယံ သဘောတူညီချက် ကဲ့သို့သော နိုင်ငံတကာနှင့် ဒေသဆိုင်ရာ မူဘောင်များနှင့် ချိန်ညှိသင့်သည်။

2. ဤကော်မတီသည် အောက်ပါနယ်ပယ်များ ဖွံ့ဖြိုးစေရန်၊ ဖြစ်ပေါ်လာနိုင်စေရန် နှင့် အရှိန်အဟုန်မြှင့် တိုးတက်စေရန် လုပ်ဆောင်သင့်သည်။

a. အလိုအလျောက်လုပ်ဆောင်သည့် အီလက်ထရောနစ် အခွန်ကောက်ခံမှုစနစ် (မြန်မာနိုင်ငံ ကုန်ပစ္စည်း အလိုအလျောက် ရှင်းလင်းရေးစနစ် (MACCA))ကို အကောက်ခွန်ဦးစီးဌာနနှင့် ပူးပေါင်းပြီး အပြည့်အဝ အကောင်အထည်ဖော် ဆောင်ရွက်ရန်။

b. နယ်စပ်ဒေသများရှိ အကောက်ခွန်နှင့် အခြားကုန်သွယ်မှုထိန်းချုပ်ရေး အေဂျင်စီများတွင် အင်တာနက်ဆက်သွယ်မှုရရှိရေးကို သေချာစေရန်။

c. ASEAN Single Window (ASW) စနစ်သို့ ဝင်ရောက်ရန်အတွက် မြန်မာနိုင်ငံ၏ National Single Window (NSW) ကို ဖွံ့ဖြိုးစေရန်။

d. အကောက်ခွန်ကြေငြာလွှာများအား အီလက်ထရောနစ်စနစ်ဖြင့် တင်သွင်းခြင်းကို ခွင့်ပြုရန်။

e. အီလက်ထရောနစ်လျှောက်လွှာများနှင့် မူလဦးစားပေးလက်မှတ်များနှင့် ကျန်းမာသန့်ရှင်းမှုနှင့် တင်သွင်းမှုလိုအပ်ချက်များ ကိုက်ညီကြောင်းလက်မှတ်များထုတ်ပေးခြင်းနှင့်

ဤလက်မှတ်များကို အခြားနိုင်ငံများနှင့် အီလက်ထရောနစ်စနစ် အသုံးပြုကာ ဖလှယ်နိုင်စေရန်။

f. အကောက်ခွန်ပြန်လည်အမ်းငွေများအတွက် အီလက်ထရောနစ်စနစ်ဖြင့် လျှောက်ထားခြင်းကို ခွင့်ပြုရန်။

g. အီလက်ထရောနစ်စနစ်ဖြင့်လုပ်ငန်းစဉ်များကို လုပ်ဆောင်ရန်အတွက် ကုန်သည်များထံသို့ ဒီဂျစ်တယ်လက်မှတ်များ ထုတ်ပေးပေးနိုင်ရန် အသိအမှတ်ပြု လက်မှတ် ထုတ်ပေးရေးအခွင့်အာဏာကို တည်ဆောက်ရန်။

h. အကောက်ခွန်ဦးစီးဌာနမှ ကုန်စည်တင်ပို့မှု အီလက်ထရောနစ်စနစ် ခြေရာခံခြင်းအတွက် ခွင့်ပြုခြင်း ကဲ့သို့သော ကုန်သွယ်ရေးနှင့်စပ်လျဉ်းသော အီလက်ထရောနစ်အချက်အလက် ဖလှယ်မှုတွင် အခြားနိုင်ငံများနှင့် ပါဂင်ဆောင်ရွက်ရန်။

i. ဘဏ်များနှင့်အာမခံလုပ်ငန်းများကို စက္ကူအသုံးပြုစာရွက်စာတမ်းများဖြင့် မလုပ်ဆောင်ဘဲ ငွေလွှဲစာတမ်းပြန်လည်ရယူမှု ခွင့်ပြုရန်။

အကောက်ခွန်များ (B4)

1. ဤကော်မတီသည် အီလက်ထရောနစ်စနစ်ဖြင့် အကောက်ခွန်ပေးဆောင်ခြင်းနှင့် အခြားဆက်စပ်နေသော အီလက်ထရောနစ်ကူးသန်းရောင်းဝယ်ရေးအခွန်များ ဖွံ့ဖြိုးတိုးတက်ရန် အတွက် စီမံကိန်းနှင့် ဘဏ္ဍာရေးဂန်ကြီးဌာနနှင့် အတူလုပ်ဆောင်သင့်သည်။ ဤအချက်ကို အီလက်ထရောနစ် အခွန်ဥပဒေတစ်ခုတွင် အစီအစဉ်ဆွဲထားသည်။
2. ဤကော်မတီသည် အခွန်ကင်းလွတ်ခွင့်များအပါအဂင် အွန်လိုင်းစီးပွားရေးလုပ်ငန်းများအတွက် အခွန်ကောက်ခံမှု အစီအစဉ်တစ်ခုကို စီမံကိန်းနှင့် ဘဏ္ဍာရေးဂန်ကြီးဌာနနှင့် အတူ လုပ်ဆောင်သင့်သည်။
3. ဤကော်မတီသည် အကောက်ခွန်ပေးချေမှုနှင့် ပြန်လည်အမ်းငွေများအတွက် အီလက်ထရောနစ် စနစ်တစ်ခုကို စတင်မိတ်ဆက်ရန် လုပ်ဆောင်သင့်သည်။ (B3 စက္ကူလွတ် ကုန်သွယ်ရေး ကဏ္ဍကို ကြည့်ပါ)

အွန်လိုင်း ကုန်သွယ်ရေး (B5)

1. ဤကော်မတီသည် အပြည်ပြည်ဆိုင်ရာဖန်ဆောင်မှုတာဖန် ရန်ပုံငွေအဖွဲ့နှင့်အတူ နိုင်ငံတွင်း အင်တာနက်အသုံးပြုနှုန်းတိုးပွားလာစေရန် တွန်းအားပေးလုပ်ဆောင်သင့်သည်။ (သတင်းအချက်အလက် အခြေခံအဆောက်အအုံ တည်ဆောက်မှုတွင် e-Government ကဏ္ဍကို ကြည့်ပါ။
2. ဤကော်မတီသည် နိုင်ငံတွင်း စီးပွားရေးလုပ်ငန်းမှ စားသုံးသူသို့ကွန်ယက်ရှိမှုတိုးတက်စေရန် အောက်ပါအတိုင်းလုပ်ဆောင်သင့်သည်။ - နိုင်ငံတွင်း၌ လူဦးရေ တစ်သန်းလျှင် လုံခြုံစိတ်ချရသော အင်တာနက်ဆာဗာ အရေအတွက် တိုးလာခြင်း

3. အငြင်းပွားမှု ဖြေရှင်းခြင်း နည်းလမ်း - ကော်မတီသည် စားသုံးသူကာကွယ်ရေးဗဟိုကော်မတီနှင့် အတူတကွ ပူးပေါင်းဆောင်ရွက်၍ အီလက်ထရောနစ်ကူးသန်းရောင်းဝယ်ရေးရှိ အရောင်းအဝယ်ကိစ္စများအတွက် ပြဋ္ဌာန်းထားသော စားသုံးသူကာကွယ်ရေးဥပဒေ (စားသုံးသူအငြင်းပွားမှုဖြေရှင်းရေးဌာနများ) အတွက် ပြဋ္ဌာန်းထားသော အငြင်းပွားမှုဖြေရှင်းရေးယန္တရား ချောမွေ့စွာနှင့် ထိရောက်စွာ လုပ်နိုင်ရန်ဆောင်ရွက်ပေးရမည်။

အီလက်ထရောနစ်စနစ်ဖြင့် အထောက်အထားပြသခြင်း (C3)

1. ဤကော်မတီသည် ဒီဂျစ်တယ်အထောက်အထားများ၊ စစ်မှန်ကြောင်း အထောက်အထားပြခြင်း နည်းလမ်းများ နှင့် ဒီဂျစ်တယ်လက်မှတ်များ စသည်တို့နှင့်စပ်လျဉ်းသည့် ဥပဒေပြဋ္ဌာန်းမှုများနှင့် စည်းမျဉ်း များကို အဆင့်မြင့်မွမ်းမံရန် e-Government ဦးစီးကော်မတီ၊ ပြည်ထောင်စုစာရင်းစစ်ချုပ်ရုံး၊ အလုပ်သမားဖန်ကြီးဌာန၊ လူဖင်မှုကြီးကြပ်ရေးနှင့် ပြည်သူ့အင်အားဖန်ကြီးဌာန၊ e-Governme ဦးစီးကော်မတီ နှင့် အီလက်ထရောနစ် သက်သေခံကဒ်ပြား လုပ်ဆောင်မှုကော်မတီတို့နှင့်အတူ ဆောင်ရွက်သင့်သည်။
2. အီလက်ထရောနစ်စနစ်ဖြင့် အထောက်အထားပြသခြင်း
    a. လုံခြုံရေးစံနှုန်းများ ဤကော်မတီသည် အစိုးရနှင့် ပုဂ္ဂလိက ကဏ္ဍများ နှစ်မျိုးစလုံးအတွက် ခိုင်မာသော အီလက်ထရောနစ်အထောက်အထားပြသခြင်းနှင့် အီလက်ထရောနစ် ငွေပေးချေမှု စံနှုန်းများနှင့် လမ်းညွှန်ချက်များ တည်ထောင်ရန်အတွက် e-Government

ဦးစီးကော်မတီ၊ ဗဟိုဘဏ်နှင့် ပြည်ထောင်စုစာရင်းစစ်ချုပ်ရုံး တို့နှင့်အတူ အောက်ပါအတိုင်းလုပ်ဆောင်သင့်သည်။

i. HTTPS မှတဆင့် လုံခြုံစိတ်ချရသော ဆက်သွယ်ရေးများရရှိစေခြင်း

ii. နောက်ထပ်လုံခြုံရေးအတွက် EMV (ယူရိုပေး၊ မာစတာကဒ်၊ ဗီဇာ) နှင့် ငွေပေးချေမှုကဒ် လုပ်ငန်း အချက်အလက် လုံခြုံရေး စံနှုန်း (PCI DSS) စသည်တို့ကဲ့သို့သော နိုင်ငံတကာစံချိန်စံညွှန်းများကို ပံ့ပိုးပေးခြင်း

iii. ဒီဂျစ်တယ်စနစ်ဖြင့် လုပ်ပိုင်ခွင့်ပေးခြင်းများကို အုပ်ချုပ်စီမံရန်နှင့် လုံခြုံစိတ်ချရသော မိုဘိုင်းငွေပေးချေမှုများ ဖော်ဆောင်နိုင်စေရန် အမျိုးသားဆိုက်ဘာလုံခြုံရေးစင်တာ၏ လက်အောက်တွင် နိုင်ငံသား လက်မှတ်ထုတ်ပေးရေးအာဏာပိုင် (နိုင်ငံသား CA) တစ်ခုတည်ထောင်ခြင်း

3. အီလက်ထရောနစ်အထောက်အထား

a. ဤကော်မတီသည် သက်သေခံကဒ်ပြားများထုတ်ဝေရေး အရှိန်အဟုန်မြှင့်စေရန်နှင့် မြန်မာနိုင်ငံသားများနှင့် နေထိုင်သူများအားလုံးကို သက်သေခံနံပါတ်မတူညီစွာ ထုတ်ပေးနိုင်ရန် အလုပ်သမားဝန်ကြီးဌာန၊ လူဝင်မှုကြီးကြပ်ရေးနှင့် ပြည်သူ့အင်အား ဝန်ကြီးဌာန၊ အီလက်ထရောနစ် အထောက်အထားဆိုင်ရာ လုပ်ငန်း ကော်မတီ၊ တို့နှင့်အတူ လုပ်ဆောင်သင့်သည်။

b. ဤကော်မတီသည် မြန်မာနိုင်ငံသားအထောက်အထားကဒ်များကို မှန်ကန်ကြောင်း အတည်ပြုစစ်ဆေးရန်အတွက် အစိုးရစံနှုန်းတစ်ခုအဖြစ် ဤတစ်ခုနှင့်တစ်ခုမတူညီသော နံပါတ်များ အသုံးပြုခြင်းကို အတည်ပြုသည့် အစိုးရမူဂါဒတစ်ခုကိုလည်း တည်ထောင်သင့်သည်။

c. ဤကော်မတီသည် ပုဂ္ဂိုလ်ရေးဆိုင်ရာအချက်အလက်များကို လုံလောက်စွာ ကာကွယ်ပေးထားပြီး သက်သေခံကဒ်၏ မည်သည့် လွဲမှားအသုံးပြုနိုင်ခြေမဆို မပေါ် ပေါက်လာစေရေးသေချာစေရန် ပုဂ္ဂိုလ်ရေးဆိုင်ရာ အချက်အလက် ကာကွယ်မှု ကော်မရှင်နှင့် စီးပွားရေးနှင့် ကူးသန်းရောင်းဝယ်ရေး ဝန်ကြီးဌာန၏ စားသုံးသူ ကာကွယ်ရေး ဌာနတို့နှင့် အတူ လုပ်ဆောင်သင့်သည်။

အီလက်ထရောနစ်- လက်မှတ်များ (C4)

1. ဤကော်မတီသည် အီလက်ထရောနစ်ဆက်သွယ်ဆောင်ရွက်ရေးဥပဒေကို အီလက်ထရောနစ်နှင့် ဒီဂျစ်တယ်လက်မှတ်များ၏ တရားဝင်မှုကို အသိအမှတ်ပြုသည့် အီလက်ထရောနစ် ကူးသန်းရောင်းဝယ်ရေး နိုင်ငံတကာ ကွန်သွယ်ရေးဥပဒေဆိုင်ရာ ကုလသမဂ္ဂအဖွဲ့အစည်း၏ အနုပညာစီရင်ထုံး ဥပဒေ အပိုဒ်ခွဲ ၉၊ ၁၂(၂)၊ ၁၂ (၃) တို့နှင့် ကိုက်ညီစေရန် ချိန်ညှိပြီး မွမ်းမံပြင်ဆင်ရမည်။ (မြန်မာဆိုက်ဘာဥပဒေ အပိုင်း ၄ ကိုကြည့်ပါ။)
2. ဤကော်မတီသည် အီလက်ထရောနစ်နှင့် ဒီဂျစ်တယ်လက်မှတ်များ၏ တရားဝင်မှုကို အသိအမှတ်ပြုသည့် အီလက်ထရောနစ် ကူးသန်းရောင်းဝယ်ရေး နိုင်ငံတကာ ကွန်သွယ်ရေးဥပဒေဆိုင်ရာ ကုလသမဂ္ဂအဖွဲ့အစည်း၏ အနုပညာစီရင်ထုံး ဥပဒေ ၏ အပိုင်း ၆(၃) ကို ဥပဒေပြုထည့်သွင်းရန် သက်သေခံဥပဒေကို ပြင်ဆင်မည်ဖြစ်သည်။ (မြန်မာဆိုက်ဘာဥပဒေ အပိုင်း ၄ ကိုကြည့်ပါ။)

အပိုင်း(၃) ဆိုက်ဘာလုံခြုံရေးနှင့် သက်ဆိုင်သော မူဝါဒများ

နိဒါန်း

မြန်မာဆိုက်ဘာဥပဒေသည် အခန်း (၅) တွင် ဆိုက်ဘာလုံခြုံရေးကို ရည်ညွှန်းပြောဆိုသည်။ အခန်း (၆) တွင် ပုဂ္ဂိုလ်ရေးဆိုင်ရာအချက်အလက်ကာကွယ်မှု ကော်မရှင် (PDPC) တစ်ခုကို တည်ထောင်ပြီး အခန်း (၇) တွင် ကွန်ပျူတာများယွင်းအသုံးပြုမှုနှင့် ဆိုက်ဘာပြစ်မှုများအတွက် ဥပဒေပြုရေး အခြေခံအုတ်မြစ် အကြောင်းကို တင်ပြထားသည်။ မြန်မာနိုင်ငံတွင် လိုအပ်နေသော ဆိုက်ဘာလုံခြုံရေးအတွက် (ဥပဒေမူကြမ်း၏ အခန်း (၅) ကိုကြည့်ပါ။) မူဝါဒနှစ်ခုကို[32] အကြံပြုဆွေးနွေးထားသည် -

1. C1 ကိုယ်ရေးကိုယ်တာနှင့် အချက်အလက်ကာကွယ်စောင့်ရှောက်ရေးကို လုပ်ဆောင်ရန် ပုဂ္ဂိုလ်ရေးဆိုင်ရာ အချက်အလက် ကာကွယ်စောင့်ရှောက်မှု ကော်မရှင်တစ်ခုကို တည်ထောင်ခြင်းနှင့်
2. C2 ဆိုက်ဘာခြိမ်းခြောက်မှုများနှင့် ဆိုက်ဘာပြစ်မှုများကို ထိတွေ့မှု လျော့ချနိုင်ရေး ဆောင်ရွက်ရန် အမျိုးသား ဆိုက်ဘာလုံခြုံရေး မဟာဗျူဟာတစ်ခုကို တည်ထောင်ခြင်း စသည်တို့ဖြစ်သည်။

ပုဂ္ဂိုလ်ရေးဆိုင်ရာအချက်အလက် ကာကွယ်စောင့်ရှောက်မှု ကော်မရှင်မှတဆင့် ကိုယ်ရေးကိုယ်တာနှင့် အချက်အလက် ကာကွယ်စောင့်ရှောက်ခြင်း(C1)

1. ပုဂ္ဂိုလ်ရေးဆိုင်ရာအချက်အလက် ကာကွယ်စောင့်ရှောက်မှုကော်မရှင် တည်ထောင်ခြင်း
    a. မြန်မာဆိုက်ဘာဥပဒေသည် ပုဂ္ဂိုလ်ရေးဆိုင်ရာအချက်အလက် ကာကွယ်စောင့်ရှောက်မှု ကော်မရှင်(PDPC) ကို တည်ထောင်မည်ဖြစ်သည်။ PDPC ကိုထူထောင်သည့်အတွက် အပြည်ပြည်ဆိုင်ရာအကောင်းဆုံး လုပ်ဆောင်မှုများဖြစ်ပေါ် စေရန် အာက်ပါလုပ်ဆောင်မှုများကို ဆောင်ရွက်သင့်သည်။ (မူဝါဒအခြေခံစံနှုန်း အစီရင်ခံစာ ကိုကြည့်ပါ)
    b. ပုဂ္ဂိုလ်ရေးဆိုင်ရာဥပဒေများပြဋ္ဌာန်းခြင်းကို လုပ်ဆောင်ရန် တာဂန်ရှိသည့် ထိရောက်သော အေဂျင်စီတစ်ခု သို့မဟုတ် ထိန်းသိမ်းသည့်အဖွဲ့အစည်းတစ်ခုအဖြစ် မြန်မာ PDPC ကို တည်ထောင်သင့်သည်။

[32] C3 (အီလက်ထရောနစ်စနစ်ဖြင့် စစ်မှန်ကြောင်းအထောက်အထားပြသခြင်း) နှင့် C4 (အီလက်ထရောနစ်စနစ်ဖြင့် ရေးထိုးထားသော လက်မှတ်များ) ကို အီလက်ထရောနစ်ကူးသန်းရောင်းဝယ်ရေးမူဝါဒတွင် ထည့်သွင်းထားသည်။

2. အွန်လိုင်းအချက်အလက်များထည့်သွင်းရန်နှင့် ပုဂ္ဂိုလ်ရေးဆိုင်ရာ အချက်အလက်များကို ကိုင်တွယ်ခြင်း သို့မဟုတ် အသုံးပြုခြင်း၊ စုဆောင်းခြင်းတို့ကို အုပ်ချုပ်စီမံမည့် စည်းမျဉ်းများ တည်ဆောက်ရန် မြန်မာနိုင်ငံအနေဖြင့် နိုင်ငံသားများ၏ ကိုယ်ရေးကိုယ်တာနှင့် လုံခြုံမှုကို ကာကွယ်ပေးသည့် လက်ရှိ ၂၀၁၇ ဥပဒေ ကို ပြင်ဆင်မွမ်းမံသင့်သည်။ သို့မဟုတ် ပုဂ္ဂိုလ်ရေးဆိုင်ရာ အချက်အလက်များ ကာကွယ်ရေးကော်မရှင် အား အမိန့်ကြေညာစာထုတ်ပြန်၍ အချက်အလက် ကာကွယ်ရေး စည်းမျဉ်းဥပဒေများ ထုတ်ပြန်ရန် တာဝန်ပေးသင့်သည်။
3. ဤပြင်ဆင်မွန်းမံမှုသည် အဓိက ကိုယ်ရေးကိုယ်တာနှင့် အချက်အလက်အယူအဆများကို အဓိပ္ပါယ်ဖွင့်ဆိုသင့်သည် -
    a. ပုဂ္ဂိုလ်ရေးဆိုင်ရာအချက်အလက် - ပုဂ္ဂိုလ်ရေးဆိုင်ရာအချက်အလက်သည် ပုံမှန်ပုဂ္ဂိုလ်တစ်ဦးအဖြစ် သတ်မှတ်ထားသော သို့မဟုတ် သတ်မှတ်နိုင်သော ပုဂ္ဂိုလ်တစ်ဦးနှင့် စပ်လျဉ်းသည့် မည်သည့်သတင်းအချက်အလက်ကိုမဆို ရည်ညွှန်းသည်။ ပြန်လည်သတ်မှတ်ထားသော၊ ကုဒ်အဖြစ်ပြောင်းလဲထားသော သို့မဟုတ် အခြားစကားလုံးများ အဖြစ်ပြန်လည်ပြောင်းလဲထားသော်လည်း လူပုဂ္ဂိုလ်တစ်ဦးကို ပြန်လည်ဖော်ထုတ်ရန် အသုံးပြုနိုင်သည့် ပုဂ္ဂိုလ်ရေးဆိုင်ရာအချက်အလက်သည် ပုဂ္ဂိုလ်ရေးဆိုင်ရာအချက်အလက်အဖြစ်ကျန်ရှိပြီး ဥပဒေနယ်ပယ်အတွင်း အကျုံးဝင်သည်။
    b. ပုဂ္ဂိုလ်ရေးအရ သတ်မှတ်နိုင်သော သတင်းအချက်အလက်များ (PII) – PII သည် ပုဂ္ဂိုလ်တစ်ဦးကို အခြားတစ်ဦးနှင့် ခွဲခြားရန်၊ ပုဂ္ဂိုလ်တစ်ဦးကို မည်သူမည်ဂါဖြစ်ကြောင်း သတ်မှတ်ဖော်ထုတ်ရန်၊ ဆက်သွယ်ရန် သို့မဟုတ် ရှာဖွေရန် သို့မဟုတ် ပတ်ဝန်းကျင်အခြေအနေတစ်ခုတွင် ပုဂ္ဂိုလ်တစ်ဦးကိုသတ်မှတ်ရန် ထိုအချက်အလက် တစ်မျိုးတည်း သို့မဟုတ် အခြားသတင်းအချက်အလက်နှင့် အသုံးပြုနိုင်သည့် မည်သည့်အချက်အလက်ကို မဆိုရည်ညွှန်းသည်။ ဤအထဲတွင် မှတ်ပုံတင်နံပါတ်များ(ဥပမာအားဖြင့် လူမှုလုံခြုံရေးနံပါတ်များ) သို့မဟုတ် ရုပ်ပိုင်းဆိုင်ရာ၊ ဇီဝကမ္မဗေဒဆိုင်ရာ၊ စိတ်ပိုင်းဆိုင်ရာ၊ စီးပွားရေးဆိုင်ရာ၊ ယဉ်ကျေးမှုဆိုင်ရာ သို့မဟုတ် လူမှုရေးဆိုင်ရာ မည်သူမည်ဂါ ဖြစ်ကြောင်း သတ်မှတ်ဖော်ထုတ်ချက် (ဥပမာအားဖြင့် အမည်နှင့် အမည်၏ ပထမစာလုံး၊ မွေးနေ့၊ ခန္ဓာကိုယ်ကိုအသေးစိတ်ဖော်ပြချက်၊ လက်ဗွေများ၊ ဒီအင်နေအေ၊ စသည်ဖြင့်) တစ်ချက် သို့မဟုတ် ပိုမိုများပြားသောအချက်များ စသည်တို့ပါဂင်သည်။

c. အချက်အလက်ပိုင်ဆိုင်သူများ - အချက်အလက်ပိုင်ဆိုင်သူတစ်ဦးသည် အချက်အလက်ပိုင်ဆိုင်မှုတစ်ခုအတွက် တာဝန်ရှိသူတစ်ဦးဖြစ်သည်။ အဖွဲ့အစည်းများအတွင်း၌ အချက်အလက်ပိုင်ဆိုင်မှုသည် ပုံမှန်အားဖြင့် အချို့သော အချက်အလက်များကို လုပ်ပိုင်ခွင့်ရှိနိုင်သည် သို့မဟုတ် ရရှိရန်ငြင်းပယ်နိုင်သည့် ဌာနတစ်ခု၊ အသင်းအဖွဲ့၊ သို့မဟုတ် စီးပွားရေးလုပ်ငန်းတစ်ခုမှ တာဝန်ယူပြီး ထိုအချက်အလက်၏ တိကျမှု၊ ပြည့်စုံမှုနှင့် မှန်ကန်သည့်အချိန်တွင် ရရှိနိုင်မှု တို့အတွက် ၎င်းတွင်တာဝန်ရှိသည်။

d. အချက်အလက်ထိန်းချုပ်သူများ - အချက်အလက်ထိန်းချုပ်သူတစ်ဦးသည် ကိုယ်ရေးကိုယ်တာအချက်အလက်များကို လုပ်ဆောင် ကိုင်တွယ်သည့်မည်သည့် အပြုအမူနှင့် ရည်ရွယ်များကိုမဆို (တစ်ဦးတည်းသော်လည်းကောင်း သို့မဟုတ် ပူးတွဲ၍ သော်လည်းကောင်း သို့မဟုတ် အခြား ပုဂ္ဂိုလ်များနှင့် မျဟေ၍သော်လည်းကောင်း) ဆုံးဖြတ်ချက်ချသည့် ပုဂ္ဂိုလ်တစ်ဦးဖြစ်သည်။

e. အချက်အလက်လုပ်ငန်းစဉ်ကို ဆောင်ရွက်သူများ - အချက်အလက်လုပ်ငန်းစဉ်ကို ဆောင်ရွက်သူတစ်ဦးသည် (အချက်အလက်ထိန်းချုပ်သူ၏ ဂန်ထမ်းတစ်ဦးမှတပါး) အချက်အလက်ထိန်းချုပ်သူကိုယ်စား အချက်အလက်လုပ်ငန်းစဉ်ကို ဆောင်ရွက်ရသည့် ပုဂ္ဂိုလ်တစ်ဦးဖြစ်သည်။

f. အချက်အလက်ဆိုင်ရာ လုပ်ငန်းစဉ်- အချက်အလက်ဆိုင်ရာ လုပ်ငန်းစဉ် ဆိုသည်မှာ အချက်အလက်ရယူခြင်း၊ မှတ်တမ်းတင်ခြင်း သို့မဟုတ် ထိန်းသိမ်းခြင်းနှင့် သတင်းအချက်အလက်ပေါ်တွင် မည်သည့် လုပ်ဆောင်ချက် သို့မဟုတ် လုပ်ဆောင်မှု အစီအစဉ်ကိုမဆို ဆောင်ရွက်ခြင်းကို ဆိုလိုသည်။ ၎င်းလုပ်ငန်းစဉ်တွင် -

   i. သတင်း သို့မဟုတ် အချက်အလက်ကို ဖွဲ့စည်းခြင်း၊ ရယူခြင်း သို့မဟုတ် ပြောင်းလဲခြင်း။

   ii. သတင်း သို့မဟုတ် အချက်အလက်ကို ပြန်လည်ရယူခြင်း၊ တိုင်ပင်ခြင်း၊ သို့မဟုတ် အသုံးပြုခြင်း။

   iii. သတင်းအချက်အလက် သို့မဟုတ် အချက်အလက်ကို ဆက်သွယ်ဖြန့်ကျက်ခြင်း၊ ဖြန့်ဝေခြင်း၊ သို့မဟုတ် အခြားနည်းလမ်းအားဖြင့် ရရှိစေရန်ပြုလုပ်ခြင်းဖြင့် ထုတ်ဖော်ကြေငြာခြင်း။

iv. သတင်းအချက်အလက် သို့မဟုတ် အချက်အလက်ကို စီစဉ်ချိန်ညှိခြင်း၊ ပေါင်းစပ်ခြင်း၊ ပိတ်ပင်ခြင်း၊ ဖယ်ရှားခြင်း သို့မဟုတ် ဖျက်ဆီးခြင်း

g. မြင်သာသော အချက်အလက်နှင့် အများပြည်သူဆိုင်ရာ အချက်အလက်ကဲ့သို့သော အချက်အလက်အမျိုးအစားများ (အမျိုးသား အိုင်စီတီ မဟာဗျူဟာအစီအစဉ်တွင် ပါဝင်သော အချက်အလက်အမျိုးအစား ခွဲခြားခြင်းမူဘောင်နှင့် မြင်သာသောအချက်အလက် မူဘောင်ကိုလေ့လာကြည့်ပါ။)

4. ဤပြင်ဆင်မွမ်းမံမှုသည် APEC သီးသန့်လုံခြုံရေးမူဘောင်နှင့် ဥရောပသမဂ္ဂ၏ အထွေထွေအချက်အလက်ကာကွယ်စောင့်ရှောက်မှုစည်းမျဉ်း (GDPR) ကို ထည့်သွင်းခြင်းအတွက် လိုအပ်ချက်များကို လိုက်နာဆောင်ရွက်ရန် မြန်မာနိုင်ငံကို ခွင့်ပြုသင့်သည်။

5. ဤပြင်ဆင်မွမ်းမံမှုသည် အချက်အလက်ထိန်းချုပ်သူများအနီးရှိ မှတ်ပုံတင်ခြင်း လမ်းညွှန်ချက်များကို ရှင်းလင်းပြတ်သားစေသင့်သည်။ - အဖွဲ့အစည်းများသည် ပုဂ္ဂိုလ်ရေးရာနှင့် အဖွဲ့အစည်းဆိုင်ရာ အချက်အလက် ကာကွယ်ရေးတာဝန်များကို ကြီးကြပ်ကွပ်ကဲရန်အတွက် အချက်အလက် ထိန်းသိမ်းသူတစ်ဦး အနည်းဆုံးခန့်အပ်ရန် မူဝါဒများနှင့် လုပ်ဆောင်မှုများကို ဖော်ဆောင်နိုင်မည် ဖြစ်သည်။ လိုက်နာမှုတိုးမြှင့်ရန် အဖွဲ့အစည်းများအနေဖြင့် အချက်အလက်ထိန်းသိမ်းသူများသည် အချက်အလက် လျှို့ဝှက်ထိန်းသိမ်းမှုတာဝန်ခံ အစိုးရအဖွဲ့အစည်းများနှင့် မှတ်ပုံတင်ထားသည်မှာ သေချာနိုင်ရမည်။ စင်ကာပူနိုင်ငံ၏ ပုဂ္ဂိုလ်ရေးဆိုင်ရာအချက်အလက်ကာကွယ်စောင့်ရှောက်မှု ကော်မရှင်အပေါ် အခြေခံပြီး ဤမှတ်ပုံတင်မှုလုပ်ငန်းစဉ်ကို ဖန်တီးနိုင်မည်ဖြစ်သည်။

6. ဤပြင်ဆင်မွမ်းမံမှုသည် ချိုးဖောက်မှုအကြောင်းကြားစာလိုအပ်ချက်တစ်ခုလည်း ပါဝင်သင့်သည်။ ပုဂ္ဂိုလ်ရေးရာ အချက်အလက်နှင့်/သို့မဟုတ် အဖွဲ့အစည်းတစ်ခုက လုပ်ဆောင်ထားသော PII ကို ပျောက်ဆုံးသည့်အခါ သို့မဟုတ် ခွင့်ပြုချက်မရှိဘဲရယူခြင်း သို့မဟုတ် ဖွင့်ဟခြင်းစသည်တို့ ဖြစ်ပွားသည့်အခါ အချက်အလက်ပေါက်ကြားမှုဖြစ်ပေါ် သည်ကို တွေ့ရှိရသည်။ ဥပမာအားဖြင့် ဥရောပသမဂ္ဂ အထွေထွေအချက်အလက် ကာကွယ်စောင့်ရှောက်မှု စည်းမျဉ်း (GDPR) သည် အချက်အလက်ပေါက်ကြားခြင်း သတိပေးချက်အားလုံးကို တွေ့လျှင်တွေ့ချင်း ၇၂ နာရီ အတွင်း တင်သွင်းရမည်ဟု ပြဋ္ဌာန်းထားသည်။ အချက်အလက် ပေါက်ကြားမှုတစ်ခုသည် ကိုယ်ရေးကိုယ်တာ သတင်းအချက်အလက် ပေါက်ကြားခံရသည့် ပုဂ္ဂိုလ်တစ်ဦးအပေါ်

ပြင်းထန်သည့် အန္တရာယ်ဖြစ်စေနိုင်မည်ဆိုလျှင် အဖွဲ့အစည်းများသည် သက်ရောက်ခံရသော ပုဂ္ဂိုလ်တစ်ဦးချင်းစီနှင့် သက်ဆိုင်ရာအစိုးရ အာဏာပိုင်များထံ သတိပေးအကြောင်းကြားရန် လိုအပ်မည်ဖြစ်သည်။ ဥပမာအားဖြင့် ဥရောပသမဂ္ဂ အထွေထွေအချက်အလက် ကာကွယ်စောင့်ရှောက်မှုစည်းမျဉ်း (GDPR) သည် ပုဂ္ဂိုလ်တစ်ဦး၏ အခွင့်အရေးများနှင့် လွတ်လပ်ပိုင်ခွင့်အပေါ် အန္တရာယ်ရှိနိုင်မည်ဆိုလျှင် အချက်အလက်ပေါက်ကြားမှုကို ပထမဆုံးစတင်သတိပြုမိသည်မှ ၇၂ နာရီ အတွင်း သတင်းပို့သင့်သည်ဟု ပြဋ္ဌာန်းထားသည်။[33] သက်ရောက်သော ပုဂ္ဂိုလ်တစ်ဦးချင်းအား သတိပေးအကြောင်းကြားစာများတွင် ပေါက်ကြားမှုကို တုံ့ပြန်ရာတွင် လုပ်ဆောင်သင့်သည့်အဆင့်များအကြောင်းကို အကြံပြုချက်များပါဝင်ရမည်။ နောက်ထပ် ပေါက်ကြားမှုသတိပေးချက်ဆိုင်ရာ ပြဋ္ဌာန်းချက်များကို ဩစတြေးလျ သတင်းအချက်အလက်ကော်မရှင် (OAIC) မှ ၂၀၁၈ ဖေဖော်ဝါရီတွင် သီးသန့်လုံခြုံရေးအက်ဥပဒေ ၁၉၈၈ ၏ အောက်တွင် မိတ်ဆက်ခဲ့သည့် ဩစတြေးလျနိုင်ငံ၏ သတိပြုမိနိုင်သော အချက်အလက် ပေါက်ကြားမှု (NDB) အစီအစဉ် အပေါ်တွင် ပုံစံယူရေးသားသင့်သည်။[34]

7. ဤပြင်ဆင်မွမ်းမံမှုသည် နယ်စပ်ဖြတ်ကျော် အချက်အလက်လွှဲပြောင်းမှုကို မြှင့်တင်သင့်သည်။ အဖွဲ့အစည်းများသည် အချက်အလက်များကို လိုအပ်သလို ရုပ်ပိုင်းဆိုင်ရာ သို့မဟုတ် အမှန်တကယ်တည်နေရာသို့ လွတ်လပ်စွာ ရွှေ့ပြောင်းနိုင်ရန် နယ်စပ်ပြဋ္ဌာန်းချက်များကို ထည့်သွင်းနိုင်သည်။ ပုဂ္ဂိုလ်ရေးအချက်အလက်များကို မြန်မာနိုင်ငံပြင်ပရှိ လက်ခံသူများထံ အပြောင်းအရွှေ့ လုပ်ဆောင်ခြင်းကို အောက်ပါကိစ္စရပ်များတွင် ခွင့်ပြုနိုင်သည်။
    a. လက်ခံသူ ရှိနေသည့်နေရာရှိ တရားစီရင်ပိုင်ခွင့်သည် အချက်အလက် ကာကွယ်မှုကို လုံလောက်သော အဆင့်တစ်ခုလုပ်ဆောင်နိုင်သည်ဟု ယူဆရလျှင်
    b. အချက်အလက်ပို့ဆောင်သူသည် အချက်အလက်ကို သင့်လျော်သည့် အကာအကွယ်များတွင် ထည့်သွင်းပို့ဆောင်ခြင်း သို့မဟုတ်
    c. အထူးကင်းလွတ်ခွင့်တစ်ခု တောင်းဆိုလျှောက်ထားခြင်း

[33] https://eugdpr.org/the-regulation/
[34] https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme

ဆိုက်ဘာခြိမ်းခြောက်မှုနှင့် ဆိုက်ဘာပြစ်မှု (C2) တို့ကို ဆိုက်ဘာလုံခြုံရေးအတွက် အမျိုးသားမဟာဗျူဟာတစ်ခုနှင့် ထိတွေ့ခြင်း

ဆိုက်ဘာခြိမ်းခြောက်မှုများ ဖြစ်ပွားမှုလျော့ပါးသက်သာစေရန်နှင့် မြန်မာနိုင်ငံသားများ ဆိုက်ဘာပြစ်မှုနှင့် ထိတွေ့မှုများ လျော့နည်းစေရန် ဆိုက်ဘာလုံခြုံရေးအတွက် အမျိုးသားမဟာဗျူဟာတစ်ခုကို ထူထောင်ရန် အရေးကြီးသည်။

အခန်းကဏ္ဍနှင့် တာဝန်ဝတ္တရားများ

1. ဆိုက်ဘာလုံခြုံရေးအတွက် အမျိုးသားမဟာဗျူဟာကို မြန်မာဆိုက်ဘာဥပဒေတွင် ဖော်ပြပါရှိသည့်အတိုင်း ITCSD မှ ဦးဆောင်မည်ဖြစ်သည်။
    a. ဆိုက်ဘာလုံခြုံရေးတွင် ပါဝင်သော ဆက်စပ်နေသည့် ကိစ္စရပ်များကြောင့် ITCSD သည် အောက်ပါအဖွဲ့များနှင့်အတူ ပူးပေါင်းလုပ်ဆောင်သင့်သည်။
        i. သမ္မတရုံးဝန်ကြီးဌာန
        ii. Ministry of Home Affairs (မြန်မာနိုင်ငံရဲတပ်ဖွဲ့)
        iii. ကာကွယ်ရေးဝန်ကြီးဌာန
        iv. ပြည်ထောင်စုရှေ့နေချုပ်ရုံး
        v. အခြား လိုအပ်သည့် ပုဂ္ဂလိက ကဏ္ဍအဖွဲ့အစည်းများ
    b. ဆိုက်ဘာလုံခြုံရေးအတွက် အမျိုးသားမဟာဗျူဟာကို အများပြည်သူနှင့် တိုင်ပင်ဆွေးနွေးပြီး အခါအားလျော်စွာ ပြန်လည်ဆန်းစစ်ရန် အကြံပြုထားသည်။
    c. ဆိုက်ဘာလုံခြုံရေးအတွက် အမျိုးသားမဟာဗျူဟာကို (ITU ၏ တစ်ကမ္ဘာလုံးဆိုင်ရာ ဆိုက်ဘာလုံခြုံရေး အညွှန်းကိန်း ကဲ့သို့သော) နိုင်ငံတကာစံချိန်စံညွှန်းများနှင့် ကိုက်ညီနိုင်စေရန် အပြည်ပြည်ဆိုင်ရာတိုင်းတာမှု နည်းလမ်းများအရ အကဲဖြတ်ရန် အကြံပြုထားသည်။
    d. ဆိုက်ဘာလုံခြုံရေး ခြိမ်းခြောက်မှုများနှင့် ဆိုက်ဘာပြစ်မှုများကို တုံ့ပြန်ရာ၌ အစိုးရအေဂျင်စီတွင် အဓိက တာဝန်နှင့် အခွင့်အရေးရှိသည်ဆိုသည့်အချက်မှာ ရှင်းလင်းမှုအနည်းငယ်သာရှိသည် ဆိုသည့်အချက် အပေါ် လေ့လာမှုကို တုံ့ပြန်ရာတွင် အစိုးရရှိ အခန်းကဏ္ဍများနှင့် တာဝန်များကို ရှင်းလင်းပြတ်သားစွာတည်ဆောက်ရန် နှင့်

ထိုအရာများကို ပြည်သူလူထုထံဆက်သွယ်နိုင်ရန် ITCSD အနေဖြင့် သက်ဆိုင်သူများအားလုံးနှင့်အတူ လုပ်ဆောင်သင့်သည်ဟု အကြံပြုထားသည်။ ဤသို့လုပ်ဆောင်ခြင်းဖြင့် အစိုးရအနေဖြင့် ဆိုက်ဘာခြိမ်းခြောက်မှုများနှင့် ဆိုက်ဘာပြစ်မှုများကို တုံ့ပြန်သည့်အကြိမ်အရေအတွက် တိုးလာစေမည်ဖြစ်သည်။

အရေးကြီးသောအချက်အလက် အခြေခံအဆောက်အအုံများကို ကာကွယ်ခြင်း (CII)

1. CII ၏ အဓိပ္ပါယ်ဖွင့်ဆိုချက် အောက်ပါကိစ္စရပ်များဖြစ်ခဲ့လျှင် ကွန်ပျူတာတစ်လုံး သို့မဟုတ် ကွန်ပျူတာစနစ်တစ်ခုကို CII ဟုအဓိပ္ပါယ်ဖွင့်ဆိုနိုင်သည်။
    a. ကွန်ပျူတာစနစ်သည် မရှိမဖြစ်ဂန်ဆောင်မှုတစ်ခုကို အဆက်မပြတ် လုပ်ဆောင်ပေးရန် အတွက် မရှိမဖြစ်အရေးပါမည်ဆိုလျှင်နှင့် အဆိုပါကွန်ပျူတာ သို့မဟုတ် ကွန်ပျူတာစနစ်၏ အားနည်းချက် သို့မဟုတ် ပျောက်ဆုံးမှုများသည် ပြည်ထောင်စုသမ္မတမြန်မာနိုင်ငံ၏ မရှိမဖြစ်ဂန်ဆောင်မှုရရှိနိုင်မှုအပေါ် အားလျော့စေသည့်သက်ရောက်မှုတစ်ခုကို ဖြစ်စေနိုင်ခဲ့လျှင်-
    b. အဆိုပါ ကွန်ပျူတာ သို့မဟုတ် ကွန်ပျူတာစနစ်သည် ပြည်ထောင်စု သမ္မတ မြန်မာနိုင်ငံတွင် တစ်စိတ်တစ်ဒေသ သို့မဟုတ် အပြည့်အဂ တည်ရှိနေလျှင်-
2. CII ကို ဆုံးဖြတ်ချက်ချခြင်း - သီးခြားစနစ်တစ်ခုကို အရေးကြီးသော သတင်းအချက်အလက် အခြေခံ အဆောက်အဦးတစ်ခုအဖြစ် သတ်မှတ်ရန် ယုံကြည်ရမည့် အကြောင်းပြချက်တစ်ခု ရှိသည့် ကိစ္စရပ်တွင် ဤစနစ်များသည် CII စံနှုန်းကို ပြည့်မီရဲ့လား ဆိုသည်ကို သိရှိနိုင်ရန် ITCSD တွင် ကွန်ပျူတာစနစ်များ၏ ပိုင်ရှင်များထံမှ သတင်း အချက်အလက်များ ပါဂင်သင့်သည်။ ITCSD ကိုလည်း စနစ်တစ်ခုသည် အရေးကြီးသတင်းအချက်အလက် အခြေခံအဆောက်အအုံ၏ စံနှုန်းကို မပြည့်မီတော့သည့်အချိန်ကို ဆုံးဖြတ်ပိုင်ခွင့်ပေးထားပြီး CII တစ်ခုအဖြစ် သတ်မှတ်ထားခြင်းမှ ရုပ်သိမ်းနိုင်သည်။
3. CII အတွက် ထိန်းချုပ်ခြင်း၊ အုပ်ချုပ်ခြင်းနှင့် လိုက်နာခြင်းစနစ်များ - ITCSD သည် -
    a. ဒီဇိုင်း၊ စီစဉ်မှုနှင့် လုံခြုံရေးဆိုင်ရာ အရေးကြီးသတင်းအချက်အလက် အခြေခံ အဆောက်အအုံတစ်ခု၏ ပိုင်ရှင်ထံမှ နောက်ထပ်သတင်းအချက်အလက်ကို တောင်းဆိုနိုင်သည်။

b. ဤစနစ်များ၏ ဆိုက်ဘာလုံခြုံရေးကို စိတ်ချရစေရန် အရေးကြီးသော သတင်းအချက်အလက် အခြေခံအဆောက်အအုံပိုင်ရှင်များ၏ စည်းမျဉ်းဥပဒေအတွက် စွမ်းဆောင်ရည်စံနှုန်းများနှင့် လုပ်ဆောင်မှုအစီအစဉ်များကို ရေးသား ထုတ်ပေးနိုင်သည်။

c. အရေးကြီးသတင်းအချက်အလက် အခြေခံအဆောက်အအုံနှင့် အပြန်အလှန် ဆက်နွယ်နေသော သို့မဟုတ် ဆက်သွယ်ထားသော ကွန်ပျူတာစနစ်များအပါအဝင် ပိုင်ရှင်၏ ထိန်းချုပ်မှုလက်အောက်ရှိ ကွန်ပျူတာစနစ်တစ်ခုပေါ်ရှိ မည်သည့်ဆိုက်ဘာ ဆက်နွယ်ဖြစ်ရပ်များကိုမဆို အစီရင်ခံရန် CII ၏ပိုင်ရှင်များအတွက် လိုအပ်ချက်များကို မိတ်ဆက်နိုင်သည်။

d. ပုံမှန်ဆိုက်ဘာလုံခြုံရေးစစ်ဆေးခြင်းများနှင့် အရေးကြီးအချက်အလက် အခြေခံအဆောက်အအုံ အန္တရာယ်ရှိနိုင်ခြေ အကဲဖြတ်မှုများလုပ်ဆောင်သွားရန် CII ပိုင်ရှင်ကို ညွှန်ကြားနိုင်သည်။

ဆိုက်ဘာလုံခြုံရေး အန္တရာယ်ရှိနိုင်ခြေ အကဲဖြတ်မှုများ၊ ထိန်းချုပ်မှုများနှင့် စစ်ဆေးမှုများ

1. မြန်မာနိုင်ငံ ဆိုက်ဘာဥပဒေသည် ဆိုက်ဘာလုံခြုံရေး အန္တရာယ်ရှိနိုင်ခြေအကဲဖြတ်မှုများ၊ စောင့်ကြည့်စစ်ဆေးမှုနှင့် ထိန်းချုပ်မှုစနစ်များအပါအဝင် mmCERT ၏ လုပ်ဆောင်မှုများနှင့် တာဝန်များကို သတ်မှတ်ထားသည်။
2. mmCERT နှင့် ITCSD သည် ဆိုက်ဘာတိုက်ခိုက်မှုများကို အစီရင်ခံတင်ပြသည့် ခိုင်မာသော အဖြစ်အပျက် အစီရင်ခံတင်ပြမှု ထုံးစံတစ်ခုကို သေချာစေရန် လုပ်ဆောင်သင့်သည်။ သို့မှသာ ဒီဂျစ်တယ်စနစ်ဖြင့် မှုခင်းခွဲခြမ်းစိတ်ဖြာမှုကို ဆောင်ရွက်နိုင်မည်ဖြစ်ပြီး ဆိုက်ဘာတိုက်ခိုက်မှု လမ်းကြောင်းများကို ဖော်ထုတ်သတ်မှတ်နိုင်မည်ဖြစ်သည်။ ဥပမာအားဖြင့် နယ်သာလန်နိုင်ငံသည် ဖွင့်ဟအသိပေးသော အစီရင်ခံစာများ၊ လုံခြုံရေးအကြံပေးချက်များနှင့် မှတ်ပုံတင်စနစ်တစ်ခုကို အသုံးပြုသော ဖြစ်ရပ်များကို နှစ်စဉ်တင်ပြလေ့ရှိသည်။
   ပေါ်ပေါက်လာသောခြိမ်းခြောက်မှုများအပေါ် အရေးယူဆောင်ရွက်ရန် ဆိုက်ဘာလုံခြုံရေးကျွမ်းကျင်သူများကို သတိပေးသည့် ၄င်းတို့၏

ဆိုက်ဘာလုံခြုံရေးအကဲဖြတ်မှုနယ်သာလန်အစီရင်ခံစာ[35]တွင် ထိုအချက်ကို တင်ပြအစီရင်ခံထားသည်။

3. ဆိုက်ဘာလုံခြုံရေးအကဲဖြတ်မှုများ၊ ထိန်းချုပ်မှုများနှင့် စစ်ဆေးမှုများသည် နိုင်ငံတကာစံချိန်စံညွှန်းအတိုင်း လိုက်နာသင့်သည်။ (အမျိုးသား ICT မဟာဗျူဟာ ၏ စံချိန်စံညွှန်းကဏ္ဍတွင်ကြည့်ပါ။) ဤထိန်းချုပ်မှု နည်းလမ်းများအသုံးပြု၍ အမှီအခိုကင်းသော စစ်ဆေးမှုများကို လုပ်ဆောင်နိုင်သည်။

ဆိုက်ဘာပြစ်မှု

1. အခန်း (၇) ကွန်ပျူတာလွဲမှားအသုံးပြုမှုနှင့် ဆိုက်ဘာပြစ်မှုဆိုင်ရာ ဆိုက်ဘာဥပဒေမူကြမ်းသည် အချက်အလက်နှင့် ကွန်ပျူတာစနစ်များပြည့်စုံမှုကို အကာအကွယ်ပေးရန်အတွက် ဆိုက်ဘာပြစ်မှုများကို သတိပြုမိရန်နှင့် ဥပဒေပြုရေးနှင့် အခြားလုပ်ဆောင်မှု အစီအစဉ်များ ဖွံ့ဖြိုးတိုးတက်ရန် ခေါင်းဆောင်အဖွဲ့အစည်း တစ်ခုအနေနှင့် ဆောင်ရွက်မည့် ဆိုက်ဘာပြစ်မှုဆိုင်ရာ ကိစ္စရပ်များကို အရေးယူဆောင်ရွက်သောအဖွဲ့တစ်ခုကို တည်ထောင်ခဲ့သည်။
2. ဆိုက်ဘာပြစ်မှုဆိုင်ရာ ကိစ္စရပ်များကို အရေးယူဆောင်ရွက်သောအဖွဲ့သည် အောက်ပါကဏ္ဍနှင့် တာဝန်များကို အဓိကထားလုပ်ဆောင်သင့်သည်။
    a. ဆိုက်ဘာလုံခြုံရေး အန္တရာယ်များကို သတိပြုမိစေရန် အမျိုးသားဆိုက်ဘာ လုံခြုံရေး စင်တာနှင့် mmCERT တို့နှင့်အတူလုပ်ဆောင်ရန်။
    b. ဆိုက်ဘာခြိမ်းခြောက်မှုများကို လုံလောက်စွာတုံ့ပြန်ရန် ဆိုက်ဘာလုံခြုံရေး ကျွမ်းကျင်သူများ အထူးသဖြင့် mmCERT အဖွဲ့သားများအတွက် ဇ လေ့ကျင့်ရေးအစီအစဉ်များ ပေါ်ပေါက်လာစေရန် e-Government ဦးစီးကော်မတီနှင့်အတူ လုပ်ဆောင်ရန်။ မြန်မာနိုင်ငံသည် ဆိုက်ဘာခြိမ်းခြောက်မှုများအတွက် လုံလောက်စွာပြင်ဆင်ထားရန် အခြားနိုင်ငံများမှလုပ်ဆောင်ခဲ့သည့် ကြိုးစားအားထုတ်မှုများအား လေ့လာနိုင်သည်။ ဥပမာအားဖြင့် မလေးရှားနိုင်ငံ ဆိုက်ဘာလုံခြုံရေး နိုင်ငံတွင်း သတင်းအချက်အလက် လုံခြုံရေးအတွက် တာဝန်ရှိသော

[35] https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-R1-PDF-E.pdf

အစိုးရအဖွဲ့သည် မလေးရှားနိုင်ငံတွင် အဆင့်မြင့် ပညာရေးအဖွဲ့အစည်းများမှ တဆင့် ကျွမ်းကျင်မှုသင်တန်းများပေးသည်။

c. အွန်လိုင်းရာဇဝတ်မှုများနှင့် မြန်မာနိုင်ငံ ဆိုက်ဘာ ဥပဒေတွင် အဆိုပြုထားသည့် အခြားဆိုက်ဘာပြစ်မှု အမျိုးအစားများကို ပါဝင်စေရန်အတွက် ပြစ်မှုဆိုင်ရာ ဥပဒေအရပ်ရပ်အား ပြန်လည်သုံးသပ်ပြီး မွမ်းမံပြင်ဆင်ချက်များအား အဆိုပြုခြင်း။

d. ဆိုက်ဘာခြိမ်းခြောက်မှုများကို ကိုင်တွယ်ဖြေရှင်းရန် အများပြည်သူနှင့် ပုဂ္ဂလိက ကဏ္ဍများနှင့်အတူ လုပ်ဆောင်ရန်။

   i. ဆိုက်ဘာခြိမ်းခြောက်မှုများကို လုံလောက်စွာတုံ့ပြန်ရန် ဆိုက်ဘာပြစ်မှုဆိုင်ရာ ကိစ္စရပ်များကို အရေးယူဆောင်ရွက်သောအဖွဲ့သည် အများပြည်သူနှင့် ပုဂ္ဂလိက ကဏ္ဍများအကြား ပူးပေါင်းဆောင်ရွက်မှုမြှင့်တင်ခြင်းတွင် ပိုမိုအားစိုက်သင့်သည်။

   ii. မြန်မာနိုင်ငံသည် အပြန်အလှန်သဘောတူညီမှု ဥပဒေရေးရာကူညီမှုစာချုပ်များ (MLATs) နှင့် ASEAN, APEC ဥရောပကောင်စီ စသည်တို့မှ တဆင့် အခြားပူးပေါင်းဆောင်ရွက်မှုများ ပါဂင်နိုင်သည့် ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ ပူးပေါင်းဆောင်ရွက်မှုအတွက် နှစ်ဦးနှစ်ဖက် သို့မဟုတ် ဘက်ပေါင်းစုံပါဂင်သော သဘောတူညီမှုများတွင် ပါဂင်နိုင်မှုကိုလည်း ထည့်သွင်းစဉ်းစားနိုင်သည်။

   iii. မြန်မာနိုင်ငံသည် နှစ်ဦးနှစ်ဖက် သို့မဟုတ် ဘက်ပေါင်းစုံပါဂင်သော သဘောတူညီမှုများတွင် ဒေသဆိုင်ရာနှင့် နိုင်ငံတကာ CERTS နှင့်အတူ တက်ကြွစွာပါဂင်ဆောင်ရွက်နိုင်သည်။ မြန်မာနိုင်ငံသည် CERTs ကို FinCERT၊ ISP/တယ်လီကွန် CERT၊ CII လုပ်ဆောင်လည်ပတ်သူ CERT နှင့် ပညာရေးဆိုင်ရာ CERT စသည်ဖြင့ ကဏ္ဍအလိုက် တည်ထောင်ရန် လေ့လာနိုင်ပြီး အမျိုးသား CERT (mmCERT) နှင့် ကဏ္ဍအလိုက် CERTs များအကြားရှိ ပူးပေါင်းဆောင်ရွက်မှုကို အဆင်ပြေချောမွေ့စေနိုင်သည်။

တရားဥပဒေနှင့်အညီ ကြားဂင်တားဆီးခြင်း

1. ဆိုက်ဘာပြစ်မှုဆိုင်ရာ ကိစ္စရပ်များကို အရေးယူဆောင်ရွက်သော အဖွဲ့သည် တောင်းဆိုထားသောအချက်အလက်အရ ဆောင်ရွက်ရန် သို့မဟုတ် လက်ခံခြင်းကိုငြင်းဆန်ရန် သက်ဆိုင်ရာ အုပ်စုများအတွက် စွမ်းရည် နှင့် ကျိုးကြောင်းဆီလျော်သော တောင်းဆိုမှု

အကြိမ်အရေအတွက်၊ သင့်လျော်သော ကြိုစားခြင်းအပေါ် အခြေခံသော တရားရုံးအမိန့်စာတစ်ခု သို့မဟုတ် အလားတူလုပ်ငန်းစဉ်တစ်ခုမှတဆင့် အချက်အလက်များရရှိရန်အတွက် ပွင့်လင်းမြင်သာသော စနစ်တစ်ခုအကောင်အထည်ဖော်ရန် အီလက်ထရောနစ် ကူးသန်းရောင်းဝယ်ရေး လုပ်ငန်းကြီးကြပ်မှုကော်မတီ၊ မြန်မာနိုင်ငံရဲတပ်ဖွဲ့၏ ဒီဂျစ်တယ်ပြစ်မှုဌာန နှင့် စာတိုက်နှင့် ဆက်သွယ်ရေးဦးစီးဌာန (PTD) တို့နှင့်အတူ လုပ်ဆောင်သင့်သည်။ (အီလက်ထရောနစ် - ကူးသန်းရောင်းဝယ်ရေး မူဝါဒရှိ အချက်အလက်လုံခြုံရေးကဏ္ဍကိုကြည့်ပါ။)

2. ဤကိစ္စရပ်သည် ချိတ်ဆက်နေသော အမှီအခိုကင်းသော တယ်လီဆက်သွယ်ရေး ထိန်းသိမ်းမှု အဖွဲ့အစည်း၏ ကဏ္ဍနှင့် များစွာတူညီနေသည့် ကိစ္စရပ်တစ်ခုဖြစ်သည့်အတွက် ဆိုက်ဘာပြစ်မှုဆိုင်ရာ ကိစ္စရပ်များကို အရေးယူဆောင်ရွက်သော အဖွဲ့သည် အီလက်ထရောနစ် ကူးသန်းရောင်းဝယ်ရေး ကော်မတီ၊ မြန်မာ ရဲတပ်ဖွဲ့၊ PTD အစရှိသည်တို့နှင့် ကနဦးဆွေးနွေးရာတွင် အခန်းကဏ္ဍများနှင့် တာဝန်များ ခွဲဝေဆွေးနွေးရန် ဆန္ဒရှိနိုင်သည်။
3. အဆိုပြုထားသော မည်သည့်တရားဝင်ကြားဝင် ဆောင်ရွက်မှုစနစ်အပေါ်တွင်မဆို အများပြည်သူဆွေးနွေးအကြံပေးပွဲတစ်ခုကို လုပ်ဆောင်ရန် အကြံပြုထားသည်။

အီးမေးလ်ထဲသို့ မလိုလားပဲအဆက်မပြတ်ပေးပို့လာသော (ကြော်ငြာ၊ မသက်ဆိုင်သည့်စာ စသည်ဖြင့်) အီးမေးလ်စာစောင်များ

1. ဆိုက်ဘာပြစ်မှုဆိုင်ရာ ကိစ္စရပ်များကို အရေးယူဆောင်ရွက်သော အဆိုပါအဖွဲ့သည် အွန်လိုင်း spam များကို ထိန်းချုပ်ရေး သို့မဟုတ် တားဆီးရေးနှင့် ဆက်စပ်နေသော အမျိုးသားမူဝါဒများကို ရေးဆွဲသင့်ပြီး အွန်လိုင်းပြစ်မှုများ ပိုမိုရှုပ်ထွေးလာခြင်းကို ထိန်းသိမ်းကိုင်တွယ်နိုင်ရန်အတွက် ကွန်ပျူတာဗိုင်းရပ်စ်များမှ ကာကွယ်ပေးသောစနစ်များ၊ လုံခြုံရေးလိုင်စင်များနှင့် လက်မှတ်သက်တမ်းတိုးခြင်းများမှတဆင့် မြန်မာနိုင်ငံ၏ ဆိုက်ဘာခြိမ်းခြောက်မှု ကာကွယ်ရေးအဆင့်ကို မြှင့်တင်ရန်အတွက် လမ်းညွှန်ချက်စာရွက်စာတမ်းများ အကြံပြုချက်များပံ့ပိုးရန် ဆက်လက်လုပ်ဆောင်သင့်သည်။
2. ဆိုက်ဘာပြစ်မှုဆိုင်ရာ ကိစ္စရပ်များကို အရေးယူဆောင်ရွက်သော အဆိုပါအဖွဲ့သည် ရဲတပ်ဖွဲ့နှင့် မဆိုင်သော ကိစ္စရပ်များအတွက် မှုခင်းဆေးပညာကို ဒီဂျစ်တယ်နည်းပညာဖြင့်ဆောင်ရွက်ရန်

အစိုးရအသိအမှတ်ပြုအခြားပံ့ပိုးသူအဖွဲ့အစည်းများကို ခေါ်ဆောင်လာခြင်းအားဖြင့် မြန်မာနိုင်ငံရဲတပ်ဖွဲ့ (MPF) ၏ ဆိုက်ဘာရာဇဝတ်မှုဌာနခွဲ (CID)မှ ဆောင်ရွက်နေသော မှုခင်းဆေးပညာကို ဒီဂျစ်တယ်စနစ်ဖြင့်ဆောင်ရွက်နိုင်မည့် မြန်မာနိုင်ငံ၏ စွမ်းရည် ချဲ့ထွင်ခြင်းကို ထည့်သွင်းစဉ်းစားနိုင်သည်။