**လိင်ပိုင်းဆိုင်ရာခေါင်းပုံဖြတ်မှုနှင့် မဖွယ်မရာပြုမှုတားဆီးကာကွယ်ရေး မြန်မာနိုင်ငံကွန်ယက်**

**နမူနာအချက်အလက်များကာကွယ်ရေးမူဝါဒ**

**နိဒါန်း**

လူတစ်ဦးချင်းစီအတွက် ၎င်းတို့၏ကိုယ်ရေးကိုယ်တာအချက်အလက်များနှင့် ဆက်သွယ်ပြောဆိုမှုများ အပေါ်တွင် သတ်မှတ်ထားသည့် သီးသန့်ကိုယ်ပိုင်အခွင့်အရေးများရှိပါသည်။ မြန်မာနိုင်ငံတွင် အချက် အလက်များအတွက် သီးခြားဥပဒေပြဌာန်းထားခြင်းမရှိသေးသော်လည်း “နိုင်ငံသားများ၏ ပုဂ္ဂိုလ်ရေး ဆိုင်ရာ လွတ်လပ်မှုနှင့်ပုဂ္ဂိုလ်ရေးဆိုင်င်ရာလုံခြုံမှုကိုကာကွယ်ပေးရေးဥပဒေ”[[1]](#footnote-1)သည်အီလက်ထရောနစ်ဆက်သွယ်ရေး သတင်းအချက်အလက်များ[[2]](#footnote-2) အပါအဝင် လူပုဂ္ဂိုလ်တစ်ဦးချင်းစီ၏ ကိုယ်ရေးကိုယ်တာအချက်အလက်များနှင့် ဆက်သွယ်ပြောဆိုမှုများကို ကာကွယ်ပေးရန် ပြဋ္ဌာန်းထားပါသည်။

မြန်မာနိုင်ငံရှိ ထိခိုက်နစ်နာသူများကို အကျိုးဆောင်ပေးရာတွင် [အဖွဲ့အစည်းအမည်] သည်တကယ်လိုအပ်နေသူများ၏ သတင်းအချက်အလက်များကို ကိုင်တွယ်ဆောင်ရွက်ပေးရန်လိုအပ်ပါသည်။ ပုဂ္ဂိုလ်ဆိုင်ရာအချက်အလက်များတွင် မည်သူမည်ဝါဖြစ်ကြောင်းခွဲခြားနိုင်သည့် အမည်၊ မွေးသက္ကရာဇ်၊ လိပ်စာ၊ ဖုန်းနံပါတ်၊ မှတ်ပုံတင်နံပါတ်၊ လက်ဗွေရာ၊ ဓါတ်ပုံ၊ ကျန်းမာရေးအခြေအနေ စသည့်အချက် အလက်များ ပါဝင်ပါသည်။

ဤအချက်အလက်များကာကွယ်ရေးမူဝါဒတွင် [အဖွဲ့အစည်းအမည်] သည် လိုအပ်နေသောလူများ၏ အခွင့် အရေးများကို ကာကွယ်ရာတွင် ဥပဒေနှင့်ကျင့်ဝတ်ဆိုင်ရာ တာဝန်ဝတ္တရားများနှင့်လျော်ညီစွာ သတင်း အချက်အလက်များကို မည်ကဲ့သို့ စုဆောင်း၊ ကိုင်တွယ်၊ သိမ်းဆည်း၊ ရှင်းထုတ်မည်ကို ဖော်ပြရပါမည်။ ဤမူဝါဒတွင် လိင်ပိုင်းဆိုင်ရာခေါင်းပုံဖြတ်မှုနှင့် မဖွယ်မရာပြုမှုစွပ်စွဲချက်များနှင့် စပ်လျဉ်းသည့် [အဖွဲ့အစည်း အမည်] က ကောက်ယူနိုင်သည့် သတင်းအချက်အလက်များ ပါဝင်ပါသည်။ ဤမူဝါဒတွင် အချက်အလက် ကာကွယ်ရေးနှင့်ပတ်သက်သည့် အဓိကအချက် (၁၀) ချက် ပါဝင်ပါသည်။

**အချက်အလက်ကာကွယ်ရေး အခြေခံမူများ**

၁။ **တရားဝင် ရည်ရွယ်ချက်။** [အဖွဲ့အစည်းအမည်] သည် သတ်သတ်မှတ်မှတ်ဖြစ်သော၊ တရားဝင်ဖြစ်သော၊ ဥပဒေနှင့်ညီညွတ်သောရည်ရွယ်ချက်(ဥပမာ- အထောက်အပံ့အတွက် လူများကိုစာရင်းသွင်းခြင်း) နှင့် ဘောင်ဝင်သည့် အချက်အလက်များကိုသာ စုဆောင်းမည်ဖြစ်ပြီး ထိုရည်ရွယ်ချက်နှင့်ကိုက်ညီမှုရှိသည့် နည်းလမ်းများဖြင့်သာ အဆိုပါအချက်အလက်များကို အသုံးပြုပါမည်။ မူလရည်ရွယ်ချက် (စောင့်ကြပ် ကြည့်ရှုခြင်း) နှင့် ကျိုးကြောင်းဆီလျော်စွာ တိုက်ရိုက်ဆက်နွယ်မှုရှိပါက ကိုယ်ရေးကိုယ်တာအချက် အလက်များကို ဆင့်ပွားရည်ရွယ်ချက်များအတွက် အသုံးပြုနိုင်သည်။

၂။ **အန္တရာယ်ကို သိရှိနားလည်ခြင်း။** [အဖွဲ့အစည်းအမည်] သည်တစ်ခုချင်းစီအတွက် သတ်သတ်မှတ်မှတ်ရှိရမည့်အကြောင်းအရာများ - ၁။ရွေးချယ်မှုနှင့်သက်ဆိုင်သော အန္တရာယ်များ (ဥပမာ- တစ်ဦးချင်းစီက ၎င်းတို့၏ အချက်အလက်များကိုပေးရန် လွတ်လပ်စွာရွေးချယ်ခွင့်ပြုလျှင်)၊ ၂။လျှို့ဝှက်ထိန်းသိမ်းခြင်း(အချက်အလက်များကို မဆီလျော်စွာထုတ်ပေးခံရခြင်း (သို့မဟုတ်) ဖောက်ထွင်းခံရခြင်း) နှင့် ၃။ကာကွယ်စောင့်ရှောက်ခြင်းဆိုင်ရာ အန္တရာယ်များ (ကိုယ်ရေးကိုယ်တာအချက်အလက်များကိုပေးခြင်း (သို့မဟုတ်) ၎င်းအချက်အလက်များ ကို အသုံးပြုရာတွင် လူတစ်ဦး၏အခွင့်အရေး (လုံခြုံမှုနှင့် ဂုဏ်သိက္ခာအပါအ၀င်) စသည့်အချက်များကို ကိုယ်ရေးကိုယ်တာအချက်အလက်များနှင့် privacyကို ကာကွယ်ရန်အတွက် ၎င်းတို့ နှင့်သက်ဆိုင်သော အန္တရာယ်ရှိမှုများကို အကဲဖြတ်ရမည်။ [အဖွဲ့အစည်းအမည်] သည် ကိုယ်ရေးကိုယ်တာအချက်အလက်များကို မည်ကဲ့သို့ကောက်ယူစုစည်းမည်၊ မည်ကဲ့သို့ လုပ်ဆောင်မည်ကို အန္တရာယ်ရှိနိုင်မှုများပေါ်မူတည်၍ ပြုပြင်ကိုက်ညှိရမည်။ လုပ်ငန်းအကောင်အထည်ဖော် နေစဉ်ကာလအတွင်း အန္တရာယ်လျော့ပါးရေးအစီအမံများကိုဆောင်ရွက်၍ ၎င်းတို့ထိရောက်မှု ရှိ/မရှိကို စောင့်ကြည့်ရပါမည်။

၃။ **အချက်အလက်ကောက်ယူမှုကိုနည်းနိုင်သမျှနည်းစေမှု။ ။** [အဖွဲ့အစည်းအမည်] သည်တရားဝင်ဖြစ်သောအကြောင်းအရာများကိုရရှိရန်အတွက် လိုအပ်သည့် ကိုယ်ရေးကိုယ်တာအချက်အလက်များ ကိုသာ ကောက်ယူရပါမည်။လူမျိုး၊ ကိုးကွယ်သည့်ဘာသာကဲ့သို့သော သတင်းအချက်အလက်များကို ကောက်ယူရန်မလိုအပ်ပါ။ အခြားအချက်အလက်များ (ဥပမာ- ပညာရေးအဆင့်အတန်း၊ မသန်စွမ်းဖြစ်မှု၊ ကျန်းမာရေးအခြေအနနှင့် ပြည်တွင်းရွေ့ပြောင်းဒုက္ခသည်/ ဒုက္ခသည်အဆင့်အတန်း) ကို အစီအစဉ်အခြေအနေအပေါ်မူတည်၍ ဆောင်ရွက်ရမည်။ [အဖွဲ့အစည်းအမည်] သည် ကောက်ယူ ထားသည့် မည်သည့်သတင်းအချက်အလက်များကိုမဆို အစီအစဉ်များ ရေးဆွဲ/ပြင်ဆင်ရန်နှင့် မူဝါဒများ ကို အကောင်အထည်ဖော်ရာတွင်အသုံးပြုနိုင်ရန် (အထူးသဖြင့် လွယ်လင့်တကူဖြစ်အောင်ပြုလုပ်နိုင်ရန်နှင့် မိမိရည်မှန်းသတ်မှတ်ချက်ကို ပြည့်မှီစေရန်) တက်ကြွစွာ ကြိုးပမ်းရမည်။

၄။ **အချက်အလက်လုံလောက်မှု။** [အဖွဲ့အစည်းအမည်] သည် ကောက်ယူသည့် ကိုယ်ရေးကိုယ်တာအချက် အလက်များသည် ဆီလျော်မှုရှိရန်နှင့် လုံလောက်မှုရှိရန် ဆောင်ရွက်ရမည်။ ၎င်းအချက်အလက်များ သည် မှန်ကန်ပြီးအချိန်နှင့်တပြေးညီကိုက်ညီမှုရှိစေရန် သင့်တင့်သောလုပ်ငန်းစဉ်များကိုလုပ်ဆောင်ရမည်။အချက်အလက်များတိကျမှန်ကန်မှုကိုမှတ်တမ်းမှတ်ရာIDကဲ့သို့သောခိုင်မာသည့်အထောက်အထားများမှမှတစ်ဆင့်ရရှိရန်ကြိုးပမ်းသင့်သည်။ ကိုယ်ရေးကိုယ်တာအချက်အလက်များကို ဗဟိုအချက်အလက်သိမ်းဆည်းမှုစနစ် (Central Database) တွင် သိမ်းဆည်းထားခြင်းဖြင့် အချက် အလက်များစုစည်းထားသည့်နေရာမျိုးစုံဖြစ်နေခြင်းကို လျှော့ချနိုင်ပါမည်။

၅။ **အနည်းဆုံး လက်လှမ်းမီမှု။** [အဖွဲ့အစည်းအမည်] သည် ကိုယ်ရေးကိုယ်တာအချက်အလက်များ ကိုအလွယ်တကူရရှိနိူင်သူအရေအတွက်အဆိုပါအချက်အလက်များကို အလွယ်တကူရရှိနိုင်သူပမာဏကို အနည်းဆုံး ဖြစ်စေရန်ဆောင်ရွက်ရမည်။ ဆောင်ရွက်ရာတွင် အဖွဲ့အစည်းအတွင်းပေးအပ်ထားသည့်မိမိတို့၏သက်ဆိုင်ရာ တာဝန်နှင့်အညီ ခွဲခြားသတ်မှတ်ပေးရမည်။ ကိုယ်ရေးကိုယ်တာအချက်အလက်များပါဝင်သည့် ဒေတာဘေ့စ်၏အချက်အလက်အားလုံးကိုအသုံးပြုသည့်ဝန်ထမ်းများအားလုံးမြင်သာအောင် မဟုတ်ဘဲ သက်ဆိုင်ရာအဆင့်အလိုက် လက်လှမ်းမီအောင်အသုံးပြုနိုင်ရန်သာ သတ်မှတ်ပေးရမည်။ အဖွဲ့အစည်းသည် ထိခိုက်လွယ်သည့် ကိုယ်ရေး ကိုယ်တာအချက်အလက်များ (လိင်ပိုင်းဆိုင်ရာခေါင်းပုံဖြတ်မှုနှင့် မဖွယ်မရာပြုမှုကဲ့သို့သောအချက် အလက်များ) ကိုရွေးထုတ်ပြီး သေချာစွာလျှို့ဝှက်ထိန်းသိမ်းထားရမည်။ အဖွဲ့အစည်း၏ လုပ်ထုံး လုပ်နည်းများအတိုင်း တိကျစွာလိုက်နာ၍ အစီရင်ခံရမည်။ လိင်ပိုင်းဆိုင်ရာခေါင်းပုံဖြတ်မှုနှင့် မဖွယ်မရာ ပြုမှုကဲ့သို့သော ကိုယ်ရေးကိုယ်တာအချက်အလက်များကို သီးသန့်ဒေတာဘေ့စ်တွင် သိမ်းဆည်းရမည်။

၆။ **အသိပေးသဘောတူညီမှု။** [အဖွဲ့အစည်းအမည်] သည် ကိုယ်ရေးကိုယ်တာအချက်အလက်များကို ရယူရာတွင် ကာယကံရှင်(သို့မဟုတ် ကာယကံရှင်များ၏တရားဝင်အုပ်ထိန်းသူ) က သေချာစွာသိရှိနားလည်ပြီး ဆန္ဒအလျောက် လွတ်လပ်စွာပေးသည့် အချက်အလက်များကိုသာ ကောက်ယူရမည်။ ထိုအသိပေး သဘောတူညီမှုတွင် အချက်အလက်များကိုမည်သို့ကောက်ယူရမည်၊ မည်သည့်အချိန်တွင် မည်ကဲ့သို့ အသုံးပြုမည်၊ သိမ်းဆည်းမည်၊ မျှဝေမည်၊ ၊စွန့်ပစ်မည်အစရှိသောအချက်များအပါအဝင်၊င့် ၎င်းတို့၏ကိုယ်ရေးကိုယ်တာအချက် အလက်များကို အဖွဲ့အစည်းသို့ပေးအပ်ခြင်းကြော င့်ဖြစ်ပေါ်လာနိုင်မည့် ားမလိုလားအပ်သောအရာများကို သေချာစွာ နားလည်နိုင်စေမည့်အချက်များ ပါဝင်ပါသည်။ သဘောတူညီမှုသည် ပြည့်စုံရှင်းလင်းစွာ (နှုတ်ဖြင့်လည်း ကောင်း၊ စာရွက်စာတမ်းများတွင်လက်မှတ်ထိုးခြင်း (သို့မဟုတ်) လက်ဗွေနှိပ်၍လည်းကောင်း) (သို့မဟုတ်) သွယ်ဝိုက်ပြီး (ထိုသူအားသတင်းအချက်အလက်ပေးခဲ့ပြီး ၎င်းတို့၏ ဆန္ဒလျောက်ရွေးချယ်ပိုင်ခွင့်ကို ကျင့်သုံးခြင်းနှင့် ဖော်ပြခြင်းတို့တွင် တားဆီးခွင့်မရှိကြောင်းနှင့် ထိုသို့ပြုလုပ်လာပါက ကန့်ကွက်ခွင့် မရှိကြောင်းတို့ကို) ဖော်ပြရန်လိုအပ်ပါမည်။ အချို့သောကိစ္စရပ်များတွင် သဘောတူခွင့်ပြုချက်ကို ကိုယ်စားပေးခြင်းသည် လုံလောက်ပါသည်။ (ဥပမာ- ကလေး (သို့မဟုတ်) ပုဂ္ဂိုလ်တစ်ဦးသည် စိတ်ပိုင်း ဆိုင်ရာချို့တဲ့သူ (သို့မဟုတ်) ဥာဏ်ရည်မမှီသူဖြစ်၍ အသိပေးသဘောတူညီမှုကို ကိုယ်တိုင်မပေးစွမ်းနိုင် ပါက ၎င်း၏အကျိုးစီးပွားအလို့ငှာ ၎င်း၏မိဘ (သို့မဟုတ်) အုပ်ထိန်းသူထံမှ ရယူနိုင်ပါသည်)။

၇။ **အချက်အလက်လုံခြုံမှု။** [အဖွဲ့အစည်းအမည်] တွင် ကိုယ်ရေးကိုယ်တာအချက်အလက်များကို လုံခြုံစွာ သိမ်းဆည်းထားပြီး အချက်အလက်ပျောက်ဆုံးမှု (သို့မဟုတ်) ခွင့်ပြုချက်မရှိဘဲဝင်ရောက်ကြည့်ရှုခြင်းမှ ကာကွယ်သည့် စနစ်များရှိရပါမည်။ စာရွက်စာတမ်းမိတ္တူများအတွက် သော့ခတ်ထားသည့်အံဆွဲ (သို့မဟုတ်) ဗီရိုများတွင် သိမ်းဆည်းခြင်းနှင့် စက္ကူဖျက်ဆီးသည့်စက်ဖြင့် ဖျက်စီးခြင်းကဲ့သို့သော လုံခြုံသောနည်းလမ်းဖြင့် စွန့်ပစ်ခြင်းများပြုလုပ်ရမည်။ အီလက်ထရောနစ်စနစ်ဖြင့် သိမ်းဆည်းထား သည့် ကိုယ်ရေးတာအချက်အလက်များအတွက် ခိုင်မာသောစကားဝှက်များအသုံးပြုခြင်း၊ ဖိုင်စာဝှက် စနစ်၊ ဗိုင်းရပ်စ်နှိမ်နှင်းရေးပရိုဂရမ်များနှင့် ကွန်ယက်လုံခြုံရေးစနစ်Firewall အသုံးပြုခြင်း၊ ယုံကြည်စိတ်ချရသည့် ဆာဗာများ ထားရှိခြင်း၊ အင်တာနက်မှတဆင့် သက်ဆိုင်ရာဆာဗာCloud ပေါ်တွင် အချက်အလက်များသိမ်းဆည်းခြင်းနှင့် အရန် သိမ်းဆည်းထားသည့် အချက်အလက်များကို ပုံမှန်စစ်ဆေးခြင်းစသည့် အိုင်တီစနစ်များကို အသုံးပြုရမည်။ USB နှင့် CD တို့ကဲ့သို့သော အလွယ်တကူရွှေ့ပြောင်းနိုင်သည့် အီလက်ထရောနစ်ပစ္စည်းများကို မသုံးမပြုသည့်အချိန် တွင် လုံခြုံစွာသော့ခတ်သိမ်းဆည်းထားရမည်။ အချက်အလက်ပေါက်ကြားမှုဖြစ်ပွားလာပါက အဖွဲ့အစည်းအနေဖြင့် ချက်ချင်းအရေးယူဆောင်ရွက်ရမည်။

**ကျပန်းစကားဝှက်ရယူမှုကို ဤနေရာတွင် ဝင်ရောက်ရယူနိုင်ပါသည်။** [**here**](https://www.avast.com/random-password-generator)

Windows 10 ထည့်သွင်းထားသည့် လက်ပ်တော့များအတွက် အချက်အလက်များ ပယ်ဖျက်ခြင်း/ ဖယ်ရှားခြင်းဆိုင်ရာ ညွှန်ကြားချက်များကို ဤနေရာတွင် ကြည့်ရှုနိုင်ပါသည်။ [here](https://www.thewindowsclub.com/remote-wipe-windows-10/)

၈။ **အချိန်အကန့်အသတ်။** [အဖွဲ့အစည်းအမည်] သည် တရားဝင်ရည်ရွယ်ချက်ကိုဆောင်ရွက်ရန် လိုအပ်သည့်အချိန်ထက်ပို၍ ကိုယ်ရေးကိုယ်တာအချက်အလက်များကို ထိန်းသိမ်းထားမည်မဟုတ်ပါ။ အဖွဲ့အစည်းထံသို့ ၎င်းတို့၏ ကိုယ်ရေးကိုယ်တာအချက်အလက်များကို အသုံးပြုရန် ခွင့်ပြုပေးသူများ သည် အဆိုပါအချက်အလက်များကို ရယူပိုင်ခွင့်၊ ပြန်လည်ပြင်ဆင်ခွင့် (သို့မဟုတ်) ဖျက်ပစ်ခွင့် နှင့် “မေ့ပစ်ပိုင်ခွင့်” ရှိပါသည်။ ပရောဂျက်သက်တမ်းကုန်ဆုံးပြီးသည့်နောက် သိမ်းဆည်းထားသည့်ကိုယ်ရေးကိုယ်တာအချက် အလက်များကို လိုအပ်သည့်စာရင်းစစ်လုပ်ငန်းများပြုလုပ်ရန် ခေတ္တခဏသိမ်းဆည်းထားပြီးနောက် စွန့်ပစ်ရပါါမည်။ သို့သော် အဆိုပါကိုယ်ရေးကိုယ်တာအချက်အလက်များကို သိမ်းဆည်းထားမှုသည် (ဥပမာ- သဘာဝဘေးအန္တရာယ်များဖြစ်ပေါ်လာ၍ အရေးပေါ်အကူအညီအတွက် အသုံးပြုရန်လိုအပ် လာခဲ့လျှင်) တရားဝင်ဖြစ်နိုင်ပါသည် ။

1. **အချက်အလက်များမျှဝေခြင်း။** အချက်အလက်များကိုကာယကံရှင်နှင့်တိုက်ရိုက်သက်ဆိုင်မှုမရှိသောနောက်ထပ်အဖွဲ့အစည်းများ ားထံသို့ မျှဝေခြင်းမပြုမီ tအမည်နာမကိုယ်ရေးကိုယ်တာ အချက်အလက်များကိုဖယ်ရှားသင့်သည်။ သို့မှသာ အချက်အလက်နှင့် ဆက်နွယ်ပတ်သက် နေသူများသည် မည်သူမည်ဝါဖြစ်ကြောင်း သိရှိနိုင်မည်မဟုတ်ပါ။ အကယ်၍ ကိုယ်ရေးကိုယ်တာအချက် အလက်များကို နိုင်ငံတော်၊ စစ်တပ် (သို့မဟုတ်) အခြားဆောင်ရွက်နေသူများမှ တောင်းခံခြင်း (သို့မဟုတ်) အတင်းအကျပ်စေခိုင်းလျှင် (သို့မဟုတ်) အာဏာပိုင်များမှသိမ်းယူခြင်းများ ပြုလုပ်ခံရပါက ဝန်ထမ်းသည် အဆိုပါအချက်အလက်များကို အချက်အလက်များကာကွယ်စောင့်ရှောက်မှုတာဝန်ခံသို့ လွှဲပြောင်းပေးရမည်။ အကယ်၍ ကိုယ်ရေးကိုယ်တာအချက်အလက်များကို တရားဝင်မျှဝေမှုများ ပြုလုပ်ရန်လိုအပ်ပါက မည်သည့်အချက်အလက်များကိုမျှဝေမည်၊ မည်သို့အသုံးပြုမည်၊ မည်ကဲ့သို့ ကာကွယ်မည်ကိုဖော်ပြထားသည့် သဘောတူညီမှုစာတမ်းကို ထားရှိရပါမည်။ အဖွဲ့အစည်းသည် ကိုယ်ရေးကိုယ်တာအချက်အလက်များကို ကာယကံရှင်နှင့်တိုက်ရိုက်သက်ဆိုင်မှုမရှိသောနောက်ထပ်အဖွဲ့အစည်းများ ထံသို့ မျှဝေသည့်အခါတွင်လည်း သက်ဆိုင်သူ များ၏သဘောတူညီမှုရှိမှသာပြုလုပ်ရမည်။ အဖွဲ့အစည်းသည် ကိုယ်ရေးကိုယ်တာအချက်အလက်များကို တိုက်ရိုက်သက်ဆိုင်မှုမရှိသောနောက်ထပ်အဖွဲ့အစည်းများ ထံမှ ရရှိသည့်အခါတွင်လည်း အချက်အလက်မျှဝေသူကာယကံတို့မှ သိရှိသဘောတူညီကြောင်း သေချာရန် သင့်လျော်သည့် စုံစမ်းမေးမြန်းမှုများကို ပြုလုပ်ရမည်။

၁၀။ **တာဝန်ခံမှု။** အဖွဲ့အစည်းသည် ထိခိုက်နစ်နာသူများ၏ ကိုယ်ရေးကိုယ်တာအချက်အလက်များနှင့် ပတ်သက်၍ တာဝန်ခံရပါမည်။ အဖွဲ့အစည်းသည် ထိခိုက်နစ်နာသူများကို ၎င်းတို့၏ ကိုယ်ရေးကိုယ်တာ အချက်အလက်များရယူမှုနှင့်စပ်လျဉ်း၍ တိုင်ပင်ဆွေးနွေးရမည်ဖြစ်ပြီး အသက်၊ ကျား/မ၊ ဘာသာစကား၊ စာတတ်မြောက်မှု၊ မသန်စွမ်းမှုနှင့် အခြားမတူကွဲပြားသည့် သတင်းအချက်အလက်များကို ကာကွယ် ထားမည့်အကြောင်း ၎င်းတို့အား ပြောကြားထားရမည်။ ၎င်းတို့၏အချက်အလက်များကို အသုံးပြုနေ သည့်နည်းလမ်းများနှင့်ပတ်သက်၍ ပြုပြင်ပြောင်းလဲမှုများကိုတောင်းဆိုရန်နှင့် တိုင်ကြားမှုများပြုလုပ် နိုင်ရန် အဖွဲ့အစည်းသည် တိုင်ကြားမှုနှင့်တုံပြန့်ချက်စနစ် (Complaints and Feedback Mechanism) ကို နည်းလမ်းတစ်ခုအဖြစ် အသုံး ပြုရမည်။ CFM အသုံးပြုသူများ၏ ကိုယ်ရေးကိုယ်တာအချက်အလက်များကို လိင်ပိုင်းဆိုင်ရာ ခေါင်းပုံဖြတ်မှုနှင့် မဖွယ်မရာပြုမူတားဆီးကာကွယ်ရေးမူဝါဒနှင့်အညီ တိကျစွာကိုင်တွယ်ရပါမည်။

**တာဝန်များ**

* အဖွဲ့အစည်းအတွက် (သို့မဟုတ်) အဖွဲ့အစည်းနှင့်တွဲဖက်၍ အလုပ်လုပ်နေသူများသည် အချက် အလက်များကို ကာကွယ်ရန်တာဝန်ရှိပြီး မည်သည့်အချက်အလက်ကိုမဆို ဤမူဝါဒနှင့်အညီ သေချာစွာ ကိုင်တွယ်ရမည်။
* အဖွဲ့အစည်းသည် ကိုယ်ရေးကိုယ်တာအချက်အလက်များကို ကောက်ယူခြင်း၊ လက်ခံခြင်း (သို့မဟုတ်) မျှဝေခြင်းများပြုလုပ်ရာတွင် တိုင်ပင်ဆွေးနွေးရန်အတွက် အချက်အလက်များ ကာကွယ်စောင့်ရှောက်မှုတာဝန်ခံကို ခန့်အပ်ထားပြီးဖြစ်သည်။ အချက်အလက်များကာကွယ်စောင့်ရှောက်မှုတာဝန်ခံသည် ဝန်ထမ်းအသစ် များအား အချက်အလက်များကာကွယ်ပေးမှုနှင့်ပတ်သက်သည်များကို (ဤမူဝါဒကိုအသုံးပြုခြင်းအပါ အဝင်) အသိပေးထားရမည်ဖြစ်ပြီး အလုပ်တွင်မည်သို့အသုံးချရမည်ကို လေ့ကျင့်ပေးရန် တာဝန်ရှိသည်။
* IT တာဝန်ခံသည် အချက်အလက်များသိမ်းဆည်းရာတွင် အသုံးပြုသည့်စနစ်များ၊ ဝန်ဆောင်မှုများနှင့် ပစ္စည်းကိရိယာများအားလုံးတို့သည် လက်ခံနိုင်သည့်လုံခြုံရေးစံနှုန်းများနှင့် ကိုက်ညီမှုရှိစေရန် သေချာ အောင်ပြုလုပ်ရမည်ဖြစ်ပြီး ၎င်းအရာများကို ပုံမှန်စစ်ဆေးကြည့်ရှုရန် တာဝန်ရှိသည်။
* အဖွဲ့အစည်းမှ အလုပ်ထွက်မည့်ဝန်ထမ်းများသည် အကူအညီလက်ခံရရှိသူ၏ မည်သည့်ကိုယ်ရေး ကိုယ်တာအချက်အလက်များကိုမဆို (အီးမေးလ်များ၊ လက်ပ်တော့များ၊ စမတ်ဖုန်းများ၊ USB (သို့မဟုတ်) စာရွက်စာတမ်းမိတ္တူများအပေါ်တွင်ရှိနေသည့် အချက်အလက်များအပါအဝင်) ယူဆောင် မထားရန် တာဝန်ရှိသည်။

1. ပြည်ထောင်စုလွှတ်တော်ဥပဒေ အမှတ် ၅ ၊ ၂၀၁၇ ခုနှစ် မတ်လ (၈) ရက် [↑](#footnote-ref-1)
2. အပိုဒ် ၈ [↑](#footnote-ref-2)