

SMEs လုပ်ငန်းများအတွက် ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ ၅ မိနစ်စာ ကိုယ်တိုင်အကဲဖြတ်စစ်တမ်း

လုပ်ငန်းအမည်.....

ဖြေဆိုသူအမည်.....

စဉ်	မေးခွန်းများ	အဖြေ			
		ဆောင်ရွက်ပြီး	တစ်စိတ်တစ်ပိုင်းဆောင်ရွက်ပြီး	မဆောင်ရွက်ရသေးပါ	မသိပါ
အပိုင်း (၁) - အခြေခံလုံခြုံရေးဆိုင်ရာ အစီအမံများ					
၁	သင့်ကွန်ပျူတာများ၊ စမတ်ဖုန်းများနှင့် အခြားစက်ပစ္စည်းများ၏ စက်လည်ပတ်ရေးစနစ် (Operating Systems) နှင့် ဆော့ဖ်ဝဲများကို အမြဲမပြတ် (Up to Date) အဆင့်မြှင့်တင်ပေး ပါသလား။	၄	၂	၀	-၁
၂	သင့်ကွန်ပျူတာများ၊ စမတ်ဖုန်းများနှင့် အခြားစက်ပစ္စည်းများတွင် ဗိုင်းရပ်စ်ကာကွယ်ရေး ဆော့ဖ်ဝဲများတပ်ဆင်ထားပြီး၊ ဗိုင်းရပ်စ်နှင့်သက်ဆိုင်သော အချက်အလက်များအား အမြဲ မပြတ် (Up to Date) အဆင့်မြှင့်တင်ပေးပါသလား။	၄	၂	၀	-၁
၃	သင့်ရဲ့စကားဝှက်များကို လွယ်ကူစွာခန့်မှန်းမရအောင် ရှည်လျားပြီးရှုပ်ထွေးစွာ ဖန်တီးထား ပါသလား။	၄	၂	၀	-၁
၄	အရေးကြီးသော သတင်းအချက်အလက်များအတွက် သင့်လျော်သော အသုံးပြုခွင့်နှင့် ကန့်သတ်ချက်များ ချမှတ်ထားပါသလား။	၄	၂	၀	-၁
၅	သင့်ကုမ္ပဏီ/လုပ်ငန်းအတွင်း၌ ခြိမ်းခြောက်မှုအသစ်များနှင့် တိုက်ခိုက်မှုပုံစံအသစ်များ အကြောင်း သတင်းအချက်အလက်မျှဝေသည့် လုပ်ငန်းစဉ်ရှိပါသလား။	၄	၂	၀	-၁
အပိုင်း (၂) - ဝန်ထမ်းများနှင့်သက်ဆိုင်သော အစီအမံများ					
၆	ဝန်ထမ်းများသည် အီးမေးလ်များတွင် ပါလာသော ဖိုင်တွဲများ သို့မဟုတ် URL လင့်ခ်များမှ တစ်ဆင့် ဗိုင်းရပ်စ်ကူးစက်ခြင်းကိုကာကွယ်နိုင်ရန်အတွက် သတိထားပြီးဆောင်ရွက် ပါသလား။	၄	၂	၀	-၁

စဉ်	မေးခွန်းများ	အဖြေ			
		ဆောင်ရွက်ပြီး	တစ်စိတ်တစ်ပိုင်းဆောင်ရွက်ပြီး	မဆောင်ရွက်ရသေးပါ	မသိပါ
၇	အီးမေးလ်နှင့်ဖက်စ်ပို့သည့် နေရာလိပ်စာမှားယွင်းမှုများ မဖြစ်စေရန် အစီအမံများ ချမှတ် ထားပါသလား။	၄	၂	၀	-၁
၈	အရေးကြီးသောအချက်အလက်များကို အီးမေးလ်စာသားထဲတွင် ရေးသားဖော်ပြခြင်းမပြုပဲ ဖိုင်တွဲများအဖြစ် ပေးပို့ခြင်းနှင့် အဆိုပါဖိုင်တွဲများအား စကားဂျက် (သို့မဟုတ်) အခြားနည်းလမ်းများဖြင့် ကာကွယ်ထားပါသလား။	၄	၂	၀	-၁
၉	ကြိုးမဲ့အင်တာနက် (Wi-Fi) လုံခြုံရေးအတွက် သင့်လျော်သော (Encryption) နည်းလမ်းများ သတ်မှတ်ခြင်းကဲ့သို့သော အစီအမံများ ပြုလုပ်ထားပါသလား။	၄	၂	၀	-၁
၁၀	အင်တာနက်မှတစ်ဆင့် ဗိုင်းရပ်စ်ကူးစက်ခြင်း သို့မဟုတ် လူမှုမီဒီယာပေါ်တွင် မသင့်လျော်သော ပို့စ်များတင်ခြင်းကဲ့သို့သော ပြဿနာများအတွက် အစီအမံများ ရှိပါသလား။	၄	၂	၀	-၁
၁၁	ကွန်ပျူတာ/ဆာဗာများ ဗိုင်းရပ်စ်ကူးစက်ခြင်း၊ အလုပ်မလုပ်ခြင်း သို့မဟုတ် လုပ်ဆောင်ချက် အမှားများကြောင့် အရေးကြီးအချက်အလက်များ ဆုံးရှုံးမှုမရှိစေရန် အရန်သိမ်းဆည်း ထားပါသလား။	၄	၂	၀	-၁
၁၂	အရေးကြီးသော အချက်အလက်ပါသည့် စာရွက်စာတမ်းများနှင့် အီလက်ထရောနစ်မီဒီယာ များကို စားပွဲပေါ်ကဲ့သို့သော အလွယ်တကူရယူနိုင်သော နေရာများတွင် မထားဘဲ ဖိုင်သိမ်းသည့် ဘီရိုကဲ့သို့သော လုံခြုံသောနေရာတွင် သိမ်းဆည်းထားပါသလား။	၄	၂	၀	-၁
၁၃	လုပ်ငန်းခွင်မှ အပြင်သို့ အရေးကြီးအချက်အလက်ပါသည့် စာရွက်စာတမ်း (သို့မဟုတ်) အီလက်ထရောနစ် မီဒီယာများ ယူဆောင်သွားရသည့်အခါ ခိုးယူခံရခြင်း (သို့မဟုတ်) ပျောက်ဆုံးခြင်းမှ ကာကွယ်ရန် အစီအမံများ ထားရှိပါသလား။	၄	၂	၀	-၁

စဉ်	မေးခွန်းများ	အဖြေ			
		ဆောင်ရွက်ပြီး	တစ်စိတ်တစ်ပိုင်းဆောင်ရွက်ပြီး	မဆောင်ရွက်ရသေးပါ	မသိပါ
၁၄	လုပ်ငန်းခွင်မှ ခဏထွက်ခွာသည့်အခါ ကွန်ပျူတာဖန်သားပြင်ကို ခွင့်ပြုချက်မရှိသူများ ကြည့်ရှုခြင်း (သို့မဟုတ်) အသုံးပြုခြင်းမှ ကာကွယ်ရန် သတိထားဆောင်ရွက်ပါသလား။	၄	၂	၀	-၁
၁၅	လုပ်ငန်းခွင်သို့ တာဝန်ရှိသူများ/ခွင့်ပြုထားသူများကိုသာ ဝင်ရောက်ခွင့်ပြုခြင်းမျိုး ကန့်သတ်ထားပါသလား။	၄	၂	၀	-၁
၁၆	ရုံးမှထွက်ခွာသည့်အခါ ကွန်ပျူတာနှင့် အခြားပစ္စည်းများကို Shutdown ချခြင်းနှင့် သော့ခတ်ခြင်းကဲ့သို့သော အစီအမံများ ထားရှိပါသလား။	၄	၂	၀	-၁
၁၇	ရုံးခန်း၌ လူမရှိသည့်အချိန်မျိုးတွင် သော့ပိတ်ရန်မေ့သွားခြင်း ကဲ့သို့သောဖြစ်စဉ်များ မရှိစေရန် အစီအမံများ ထားရှိပါသလား။	၄	၂	၀	-၁
၁၈	အရေးကြီးအချက်အလက်ပါသော စာရွက်စာတမ်းများ (သို့မဟုတ်) မီဒီယာများအား ဖျက်စီးစွန့်ပစ်သည့်အခါ ၎င်းတို့အား ပြန်လည်ရယူ၍ မရစေရန် အစီအမံများ ထားရှိပါသလား။	၄	၂	၀	-၁
အပိုင်း (၃) - လုပ်ငန်း/ကုမ္ပဏီ/အဖွဲ့အစည်းဆိုင်ရာ အစီအမံများ					
၁၉	သင့်လုပ်ငန်း/ကုမ္ပဏီ/အဖွဲ့အစည်းသည် ဝန်ထမ်းများအား လိုက်နာရမည့် “လျှို့ဝှက်ချက်များ ထိန်းသိမ်းခြင်းနှင့် လုပ်ငန်းခွင်ဆိုင်ရာအချက်အလက်များ အပြင်ဘက်သို့ ထုတ်ဖော်ပြောကြားမှု မပြုစေခြင်း” နှင့်သက်ဆိုင်သော စည်းမျဉ်းများအား နားလည်အောင် ဆောင်ရွက်ပေးပါသလား။	၄	၂	၀	-၁
၂၀	ဝန်ထမ်းများအား ဆိုက်ဘာလုံခြုံရေးသင်တန်းများ (သို့မဟုတ်) ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ အသိပညာပေး အစီအစဉ်များ စီစဉ်ပေးပါသလား။	၄	၂	၀	-၁

စဉ်	မေးခွန်းများ	အဖြေ			
		ဆောင်ရွက်ပြီး	တစ်စိတ်တစ်ပိုင်းဆောင်ရွက်ပြီး	မဆောင်ရွက်ရသေးပါ	မသိပါ
၂၁	ကိုယ်ပိုင်စက်ပစ္စည်းများအား လုပ်ငန်းဆိုင်ရာအသုံးပြုခြင်းတို့အတွက် ဆိုက်ဘာလုံခြုံရေး အစီအမံများ သတ်မှတ်ထားရှိပါသလား။	၄	၂	၀	-၁
၂၂	အရေးကြီးအချက်အလက်ဖလှယ်သည့် လုပ်ငန်းမိတ်ဖက်များနှင့် ချုပ်ဆိုထားသော စာချုပ်များတွင် လုပ်ငန်းနှင့်သက်ဆိုင်သည့်လျှို့ဝှက်ချက်ဆိုင်ရာ သတ်မှတ်ချက်များ ထည့်သွင်းပါရှိ ပါသလား။	၄	၂	၀	-၁
၂၃	Cloud ဝန်ဆောင်မှုနှင့် ဝက်ဘ်ဆိုဒ်ရေးဆွဲခြင်းလုပ်ငန်းကဲ့သို့သော ပြင်ပဝန်ဆောင်မှုများအား ရယူရာတွင် ၎င်းတို့၏ လုံခြုံရေးနှင့်ယုံကြည်စိတ်ချရမှုအပေါ် အခြေခံ၍ ရွေးချယ်ပါသလား။	၄	၂	၀	-၁
၂၄	သင်၏လုပ်ငန်း/ ကုမ္ပဏီ/ အဖွဲ့အစည်းသည် ဆိုက်ဘာလုံခြုံရေး ကျိုးပေါက်မှု အခြေအနေများ အတွက် ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ တုံ့ပြန်ရေးလုပ်ငန်းစဉ်များနှင့် အရေးပေါ်အစီအစဉ်များ ချမှတ်ခြင်းကဲ့သို့သော အစီအမံများ အသင့်ပြင်ဆင်ထားရှိပါသလား။	၄	၂	၀	-၁
၂၅	သင်၏လုပ်ငန်း/ကုမ္ပဏီ/အဖွဲ့အစည်းအနေဖြင့် အထက်တွင် ဖော်ပြထားသော အမှတ်စဉ် ၁ မှ ၂၄ ကဲ့သို့သော အချက်အလက်လုံခြုံရေးဆိုင်ရာ စည်းမျဉ်းများ သတ်မှတ်ထားရှိပြီး ဝန်ထမ်းများအား ရှင်းလင်းစွာ အသိပေးထားရှိပါသလား။	၄	၂	၀	-၁

“ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ ၅ မိနစ်စာ ကိုယ်တိုင်အကဲဖြတ်စစ်တမ်း” အတွက်
အကဲဖြတ်ရမှတ်နှင့် ရှင်းလင်းချက်

ရမှတ် ၁၀၀	အခြေခံဆိုက်ဘာလုံခြုံရေး အစီအမံများ အောင်မြင်စွာ အကောင်အထည် ဖော်ပြီးဖြစ်ပါသည်။ သင့်လုပ်ငန်းတွင် သတင်းအချက်အလက်ကာကွယ်ရေးစနစ်ကို ပိုမိုအားကောင်းစေရန်အတွက် နောက်ထပ်အဆင့်များကို စဉ်းစား ဆောင်ရွက်ရန် လိုအပ်ပါသည်။
ရမှတ် ၇၀-၉၀	အခြေခံဆိုက်ဘာလုံခြုံရေးအစီအမံများတွင် အားနည်းနေသေးသည့် အချက်များရှိနေပါသည်။
ရမှတ် ၅၀-၆၉	အခြေခံဆိုက်ဘာလုံခြုံရေး အစီအမံများတွင် ထိရောက်စွာ အကောင်အထည် မဖော်ရသေးသည့် အားနည်းချက်များ သိသာထင်ရှားစွာ ရှိနေပါသည်။
ရမှတ် ၄၉ မှတ်နှင့် အောက်	သတင်းအချက်အလက်နှင့် ဆိုက်ဘာလုံခြုံရေးကျိုးပေါက်မှုများ အချိန်မရွေး ဖြစ်ပွားနိုင်ပါသည်။

SMEs လုပ်ငန်းရှင်များအနေဖြင့် ဆိုက်ဘာလုံခြုံရေးအတွက် လုပ်ဆောင်သင့်သည့်အချက်များ

အပိုင်း(၁) အခြေခံဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ အစီအမံများ

- (၁) Operating Systemနှင့် ဆော့ဖ်ဝဲများကို အမြဲမပြတ်အဆင့်မြှင့်တင်ခြင်း(Update) ပြုလုပ်ထားပါ။
- (၂) ဗိုင်းရပ်စ်ကာကွယ်ရေးဆော့ဖ်ဝဲများကိုအသုံးပြုပါ။ ထို့အပြင် ဗိုင်းရပ်စ်ကာကွယ်ရေး ဆော့ဖ်ဝဲများအား ပုံမှန် Update ပြုလုပ်ပေးပါ။
- (၃) အားကောင်းခိုင်မာသော စကားဝှက်များကို အသုံးပြုပါ။
- (၄) ဒေတာ/ဖိုင်မျှဝေခြင်းနှင့် ပတ်သက်သည့် Setting များအား ပြန်လည်သုံးသပ်ပါ။
- (၅) ဆိုက်ဘာလုံခြုံရေးခြိမ်းခြောက်မှုများ၊ တိုက်ခိုက်မှုနည်းလမ်းများနှင့် သတင်းများကို စဉ်ဆက်မပြတ် သတိပြုလေ့လာပြီး ဤအသိပညာကို အသုံးပြု၍ ကာကွယ်ရေးနည်းလမ်းများကို ဖော်ထုတ်ပါ။

အပိုင်း (၂) ဝန်ထမ်းများနှင့်သက်ဆိုင်သော အစီအမံများ

- (၆) မသိသောသူများထံမှ ပေးပို့လာသည့်အီးမေးလ်များကို အမြဲသတိထားပါ။
- (၇) အီးမေးလ်များအား လိပ်စာမှားယွင်းပေးပို့ခြင်းမှ သတိထားကာကွယ်ပါ။
- (၈) အရေးကြီးသောအချက်အလက်များအား အီးမေးလ်ဖြင့်ပေးပို့ရာတွင် အထူးသတိပြုကာကွယ်ပါ။
- (၉) ကြိုးမဲ့အင်တာနက်လိုင်းများအား ကြားဖြတ်ရယူခြင်းနှင့်ခွင့်ပြုချက်မရှိဘဲ အသုံးပြုခြင်းတို့ မပြုလုပ်နိုင်စေရန် စီစဉ်ဆောင်ရွက်ထားရှိပါ။
- (၁၀) အင်တာနက်အသုံးပြုခြင်းမှတစ်ဆင့် မလိုလားအပ်သော ဆိုက်ဘာလုံခြုံရေးပြဿနာများ မဖြစ်ပေါ်စေရေး သတိထားအသုံးပြုပါ။
- (၁၁) ဒေတာဆုံးရှုံးမှုများကိုကာကွယ်ရန်အတွက် ပုံမှန် အရန်သိမ်းဆည်းခြင်း (Backup) ပြုလုပ်ပါ။
- (၁၂) အရေးကြီးသောအချက်အလက်နှင့် စာရွက်စာတမ်းများကို သင့်တော်သည့်နည်းလမ်းဖြင့် ကိုင်တွယ်သိမ်းဆည်းဆောင်ရွက်ပါ။
- (၁၃) အရေးကြီးသောအချက်အလက်များကို ပေါက်ကြားမှုမရှိစေရေး ထိန်းသိမ်းဆောင်ရွက်ပါ။
- (၁၄) ခွင့်ပြုချက်မရှိဘဲ မည်သူမဆို ရုံးကွန်ပျူတာများ၊ ရုံးစနစ်များအသုံးပြုခြင်း မပြုလုပ်နိုင်စေရန် စီစဉ်ပါ။
- (၁၅) လုပ်ငန်းခွင်အတွင်း ဝင်ရောက်လာသော မသိသောသူများ/ လုပ်ငန်းနှင့် မသက်ဆိုင်သောသူများကို သတိပြုပါ။
- (၁၆) ရုံးလုပ်ငန်းသုံးပစ္စည်းများနှင့် ဆက်စပ်ပစ္စည်းများအား ခိုးယူခြင်းမှ ကာကွယ်ပါ။
- (၁၇) ရုံးတံခါးများသော့ခတ်ခြင်းအား ဂရုပြုဆောင်ရွက်ပါ။
- (၁၈) အရေးကြီးသော အချက်အလက်များအား ဖျက်ဆီးစွန့်ပစ်ရာတွင် ပြန်လည်ရယူ၍မရနိုင်သော ဖျက်ဆီးခြင်းနည်းလမ်းများဖြင့် ဆောင်ရွက်ပါ။

အပိုင်း (၃) လုပ်ငန်း/ကုမ္ပဏီ/အဖွဲ့အစည်းဆိုင်ရာ အစီအမံများ

- (၁၉) ဝန်ထမ်းများအား လုပ်ငန်းခွင်ဆိုင်ရာလျှို့ဝှက်ချက်များ ထိန်းသိမ်းခြင်းကဲ့သို့သော တာဝန်များကို သေချာစွာ နားလည်မှုရှိစေရန် စီစဉ်ဆောင်ရွက်ပါ။
- (၂၀) ဝန်ထမ်းများအတွက် အချက်အလက်လုံခြုံရေးနှင့်သက်ဆိုင်သော လေ့ကျင့်သင်ကြားမှုများကို ဆောင်ရွက်ပေးပါ။
- (၂၁) လုပ်ငန်းခွင်အတွင်း ကိုယ်ပိုင်စက်ပစ္စည်းများ အသုံးပြုခွင့် ပေးမပေးကြိုတင်စီစဉ်ဆုံးဖြတ်ပါ။
- (၂၂) မိတ်ဖက်အဖွဲ့အစည်းများအား လျှို့ဝှက်ချက်ထိန်းသိမ်းရန် တောင်းဆိုပါ။
- (၂၃) ယုံကြည်စိတ်ချရသော ပြင်ပဝန်ဆောင်မှုများကိုသာ အသုံးပြုပါ။
- (၂၄) ဆိုက်ဘာတိုက်ခိုက်မှုဖြစ်စဉ်များအတွက် ကြိုတင်ပြင်ဆင်ထားပါ။
- (၂၅) ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ စည်းမျဉ်းစည်းကမ်းများ ရေးဆွဲချမှတ်ပါ။