`संचालनसम्बद्ध डाटा व्यवस्थापनमा डाटा सुरक्षाका लागि सुझाव पाना
अप्रिल २०२२

यस सुझाव पानाको अनुवाद CLEAR ग्लोबल र फ्रान्सको युरोप र विदेश मन्त्रालयको सहयोगमा CartONG द्वारा सहजीकरण गरिएको थियो।

परिचय
डाटा सुरक्षा डाटा उत्तरदायित्वको मुख्य भाग हो: परिचालन प्रतिक्रियाको लागि डाटाको सुरक्षित, नैतिक र प्रभावकारी व्यवस्थापन। यसले भौतिक, प्राविधिक र प्रक्रियागत उपायहरूको समूह माग गर्दछ जसले डाटाको गोपनीयता, अखण्डता र उपलब्धताको सुरक्षा गर्दछ र यसको आकस्मिक वा जानाजानी, गैरकानूनी वा अन्यथा अनधिकृत हानि, विनाश, परिवर्तन, अधिग्रहण, वा खुलासालाई रोक्न सक्छ।

यस सुझाव पानाले संचालन डाटा व्यवस्थापनमा डाटा सुरक्षाको लागि सिफारिस गरिएका कार्यहरूको सङ्ग्रह प्रदान गर्दछ। कार्यहरू सान्दर्भिक संस्थागत जनादेश, नीतिहरू, र कानुनी र नियामक ढाँचाहरू अनुरूप कार्यान्वयन गरिनुपर्छ।

राम्रो पासवर्ड व्यवस्थापन अभ्यास गर्नुहोस्
- संख्याहरू, क्यापिटल र लोअरकेस अक्षरहरू, र प्रति पासवर्ड कम्तिमा 16+ क्यारेक्टरहरू समावेश भएका बलियो पासवर्डहरूका साथ आफ्नो उपकरणहरू र खाताहरू सुरक्षित गर्नुहोस्।
- सबै खाताहरूका लागि बहु-कारक प्रमाणीकरण सक्रिय गर्नुहोस्।
- धेरै खाताहरूको लागि एउटै पासवर्ड पुन: प्रयोग नगर्नुहोस्।
- आफ्नो पासवर्डहरू भौतिक रूपमा (जस्तै नोटहरूमा) वा डिजिटल रूपमा (तपाईंको यन्त्रको फाइलमा) भण्डारण नगर्नुहोस् र अरूसँग आफ्नो पासवर्ड साझा नगर्नुहोस्।
- अनुप्रयोगहरू र ब्राउजरहरूमा 'Remember Me' कार्यक्षमता सक्रिय नगर्नुहोस्।
- यदि तपाइँको यन्त्र हराए वा चोरी भयो भने तुरुन्तै तपाइँको अनलाइन खाताहरूमा तपाइँको पासवर्डहरू परिवर्तन गर्नुहोस्।

एन्टिभाइरस/एन्टी-मालवेयर सफ्टवेयर प्रयोग गर्नुहोस्
- सुनिश्चित गर्नुहोस् कि तपाइँसँग तपाइँको उपकरणहरूमा उपयुक्त एन्टिभाइरस/एन्टि-मालवेयर सफ्टवेयर छ।
- यदि तपाइँसँग उपयुक्त उपकरणहरू वा तिनीहरूलाई कसरी कन्फिगर गर्ने भन्ने प्रश्नहरू छन् भने, तपाइँको कार्यालयमा आईटी विशेषज्ञसँग जाँच गर्नुहोस्।

सफ्टवेयर र अपरेटिङ सिस्टमहरू अद्यावधिक राख्नुहोस्
- नियमित रूपमा जाँच गर्नुहोस् कि तपाईंको उपकरण, सफ्टवेयर, अनुप्रयोगहरू, र ब्राउजर प्लग-इनहरू अप टु डेट छन् र तपाईंको अपरेटिङ सिस्टमका लागि स्वचालित अपडेटहरू सक्रिय पार्नुहोस्।
- क्रोम वा फायरफक्स जस्ता वेब ब्राउजरहरू प्रयोग गर्नुहोस् जसले स्वचालित सुरक्षा अपडेटहरू प्राप्त गर्दछन्।
- अपडेट सक्षम गर्न र आक्रमणहरूबाट जोगाउन दिनको अन्त्यमा यन्त्रहरू बन्द गर्नुहोस् ।

फिसिङ ठगीहरूबाट बच्नुहोस् र तपाईंले क्लिक गर्ने कुराहरुप्रति सावधान रहनुहोस्
- शंकास्पद इमेल वा सन्देशहरू प्राप्त गर्दा, सधैँ प्रेषकको ठेगाना/सम्पर्क जानकारी जाँच गर्नुहोस् र आफुले विश्वास गरेको प्रेषक भएमात्र लिङ्क वा संलग्न गरिएका कुराहरुमा क्लिक गर्नुहोस्।
- शंकास्पद इमेलहरूको जवाफ नदिनुहोस् वा तिनीहरूलाई आफ्ना सहकर्मीहरूलाई फर्वार्ड नगर्नुहोस्।
- आफ्नो IT सहयोग टोलीलाई कुनै पनि शंकास्पद गतिविधिको जानकारी गराउनुहोस्।

मोबाइल उपकरणहरू जिम्मेवारीपूर्वक प्रयोग गर्नुहोस्

- **जहाँ सम्भव छ, कार्यात्मक उद्देश्यका लागि अलग उपकरणहरू प्रयोग गर्नुहोस्। आफ्ना कामका यन्त्रहरूलाई सधैं सुरक्षित ठाउँमा राख्नुहोस् र अनावश्यक रूपमा वरपर लैजान नदिनुहोस्।**
- **तपाईंको संगठनद्वारा अनुमोदित सन्देश उपकरणहरू प्रयोग गर्नुहोस् जसले अन्त-देखि-अन्त इन्क्रिप्सन प्रदान गर्दछ।**
- **सम्भव भएसम्म ब्लुटुथ जडान बन्द गर्नुहोस् र ब्लुटुथ जडान कम गर्नुहोस्।**
- **अनलाइन काम गर्दा आफ्नो संगठन द्वारा अनुमोदित भर्चुअल निजी नेटवर्क (VPN) प्रयोग गर्नुहोस्। यदि तपाइँ सामुदायिक कम्प्युटर वा उपकरण प्रयोग गर्दै हुनुहुन्छ भने सधैं आफ्नो खाता(हरू) बाट साइन आउट गर्नुहोस्।**
- **बायोमेट्रिक अनलक सुविधाहरू असक्षम पार्नुहोस्—विशेष गरी ट्रान्जिटमा हुँदा।**

संवेदनशील डाटा सुरक्षित गर्नुहोस् र डाटा न्यूनीकरण अभ्यास गर्नुहोस्

- **तपाईंको कार्यालयद्वारा व्यवस्थित प्रत्येक डाटा प्रकारका लागि संवेदनशीलताको स्तरलाई संकेत गर्ने डेटा सम्पत्ति रजिस्ट्री राख्नुहोस्। सन्दर्भ विकसित हुँदै जाँदा संवेदनशीलता स्तरहरू नियमित रूपमा समीक्षा गर्नुहोस्।**
- **दिइएको डाटा व्यवस्थापन गतिविधिको लागि लक्ष्य र उद्देश्यहरू प्राप्त गर्न आवश्यक डाटाको न्यूनतम मात्रा मात्र सङ्कलन गर्नुहोस्।**
- **संवेदनशील तथ्याङ्कहरू आवश्यक भएमात्र त्यसलाई व्यवस्थित गर्ने उद्देश्य पूरा गर्नका लागि र प्रयोगात्मक मार्गदर्शन, कानून र नियमहरूद्वारा आवश्यक मात्र राख्नुहोस्।**
- **तपाईंको संगठनद्वारा अनुमोदित उपकरणहरू र च्यानलहरू प्रयोग गरेर डाटा स्थानान्तरण र भण्डारण गर्नुहोस् (स्थानीय रूपमा संगठन सर्भर, कम्प्युटर वा ल्यापटपमा; वा OneDrive, SharePoint र Teams जस्ता अनुप्रयोगहरू मार्फत टाढाबाट संचालित सर्भरहरू र प्रणालीहरूमा)।**
- **संवेदनशील डाटा समावेश फाइलहरू (वर्ड, एक्सेल, पीडीएफ)पासवर्ड सुरक्षित गर्नुहोस् रकागजात पासवर्डहरू अलग च्यानलहरू मार्फत साझेदारी गर्नुहोस् (अर्थात् इमेल गरिएको कागजातका लागि पासवर्ड पठाउनुहोस्)।**
- **संवेदनशील डाटामा पहुँच भएका व्यक्तिहरूको संख्या सीमित राख्नुहोस् र सावधानीपूर्वक निगरानी गर्नुहोस्।**
- व्यवस्थित गरिएको सबै डाटाको लागि एक अवधारण र विनाश तालिका परिभाषित गर्नुहोस् र डेटाको विनाशको लागि उपयुक्त उपकरणहरू प्रयोग गर्नुहोस्।
- तपाईंको इमेल सन्देशहरू इन्क्रिप्ट गर्नुहोस्।

<u>प्रमुख स्रोतहरू</u>

- मानवीय कार्यमा डाटा उत्तरदायित्वमा IASC परिचालन मार्गदर्शन
- डाटा घटना व्यवस्थापन मा मार्गदर्शन नोट
- अनलाइन सम्मेलन उपकरणहरूको जिम्मेवार प्रयोगमा सुझाव पाना

मानवीय कार्यहरूमा संवेदनशील डाटा प्रबन्ध गर्ने बारे थप जानकारीको लागि, केन्द्रको वेबसाइटमा डाटा उत्तरदायित्व पृष्ठमा जानुहोस् वा हाम्रो टोलीलाई *centrehumdata@un.org मा सम्पर्क गर्नुहोस्*।