অপারেশনাল ডেটা ম্যানেজমেন্টে তথ্য সুরক্ষার টিপ শীট
এপ্রিল ২০২২

ক্লিয়ার গ্লোবাল এবং ইউরোপের ফ্রেঞ্চ মিনিস্ট্রি ও পররাষ্ট্র মন্ত্রণালয়ের সমর্থনে CartONG এই টিপ শীটটির অনুবাদে সাহায্য করেছে।

ভূমিকা

তথ্য সুরক্ষা হল ডেটা রেসপনসিবিলিটি-র একটি মূল উপাদান: যার মধ্যে আছে সক্রিয় প্রতিক্রিয়ার জন্য ডেটার নিরাপদ, নৈতিক এবং কার্যকর ব্যবস্থাপনা। এতে একগুচ্ছ স্পর্শনীয়, প্রযুক্তিগত এবং পদ্ধতিগত ব্যবস্থা রয়েছে যা তথ্যের গোপনীয়তা, অখণ্ডতা এবং এর পাওয়াকে রক্ষা করে এবং এর দুর্ঘটনাজনিত বা ইচ্ছাকৃত, বেআইনি বা অন্যথায় অননুমোদিত ক্ষতি, ধ্বংস, পরিবর্তন, দখল বা প্রকাশ প্রতিরোধ করে।

এই টিপ শীট অপারেশনাল ডেটা ম্যানেজমেন্টে তথ্য সুরক্ষার জন্য প্রস্তাবিত কাজগুলো প্রদান করে। এই কাজগুলো প্রাসঙ্গিক প্রাতিষ্ঠানিক আদেশ, নীতি এবং আইনি ও নিয়ন্ত্রক কাঠামোর সাথে সামঞ্জস্য রেখে করা উচিত।

ভাল পাসওয়ার্ড ব্যবহার করা অনুশীলন করুন

- আপনার ডিভাইস এবং অ্যাকাউন্টগুলোকে শক্তিশালী পাসওয়ার্ড দিয়ে সুরক্ষিত করুন যেখানে সংখ্যা, বড় হাতের অক্ষর এবং প্রতিটি পাসওয়ার্ডে কমপক্ষে ১৬টির বেশি অক্ষর সহ চিহ্ন অন্তর্ভুক্ত থাকে।
- সমস্ত অ্যাকাউন্টের জন্য মাল্টি-ফ্যাক্টর অথেনটিকেশন ব্যবহার করুন।
- একাধিক অ্যাকাউন্টের জন্য একই পাসওয়ার্ড বারবার ব্যবহার করবেন না।
- আপনার পাসওয়ার্ডগুলো লিখিতভাবে (যেমন- নোট) অথবা ডিজিটালি (আপনার ডিভাইসের একটি ফাইলে) সংরক্ষণ করবেন না এবং অন্যদের সাথে আপনার পাসওয়ার্ড শেয়ার করবেন না।
- অ্যাপ্লিকেশন এবং ব্রাউজারগুলোয় 'Remember Me' ফাংশন চালু রাখবেন না।
- আপনার ডিভাইস হারিয়ে গেলে বা চুরি হয়ে গেলে অবিলম্বে আপনার অনলাইন অ্যাকাউন্টে আপনার পাসওয়ার্ড পরিবর্তন করুন।

অ্যান্টিভাইরাস/অ্যান্টি-ম্যালওয়্যার সফটওয়্যার ব্যবহার করুন

- আপনার ডিভাইসে উপযুক্ত অ্যান্টিভাইরাস/অ্যান্টি-ম্যালওয়্যার সফটওয়্যার ব্যবহার নিশ্চিত করুন।
- উপযুক্ত টুলস বা সেগুলো কীভাবে কনফিগার করবেন সে সম্পর্কে যদি আপনার কোন প্রশ্ন থাকে, তাহলে আপনার অফিসের আইটি বিশেষজ্ঞের সাথে যোগাযোগ করুন।

সফটওয়্যার এবং অপারেটিং সিস্টেম আপ-টু-ডেট রাখুন

- আপনার ডিভাইস, সফটওয়্যার, অ্যাপ্লিকেশন, এবং ব্রাউজার প্লাগ-ইন আপ-টু-ডেট আছে কিনা তা নিয়মিত পরীক্ষা করুন এবং আপনার অপারেটিং সিস্টেমের জন্য স্বয়ংক্রিয় আপডেট চালু করুন।
- ক্রোম বা ফায়ারফক্সের মতো ওয়েব ব্রাউজার ব্যবহার করুন যা স্বয়ংক্রিয়ভাবে নিরাপত্তা আপডেট গ্রহণ করে।
- আপডেট চালু রাখতে এবং আক্রমণ থেকে রক্ষা করতে দিনশেষে ডিভাইসগুলো বন্ধ করুন।

ফিশিং স্ক্যাম এড়িয়ে চলুন এবং আপনি কোথায় ক্লিক করছেন তা নিয়ে সতর্ক থাকুন।

- সন্দেহজনক ইমেইল বা বার্তা পেলে সর্বদা প্রেরক এবং এপিওর ঠিকানা/যোগাযোগের তথ্য চেক করুন এবং প্রেরককে বিশ্বাস করলে তবেই লিঙ্ক বা অ্যাটাচমেন্টে ক্লিক করুন।

- সন্দেহজনক ইমেইলের উত্তর দেবেন না বা আপনার সহকর্মীদের কাছে সেগুলো পাঠাবেন না।
- যেকোন সন্দেহজনক কার্যকলাপের ক্ষেত্রে আপনার আইটি সাপোর্ট টিমকে রিপোর্ট করুন।

দায়িত্বের সাথে মোবাইল ডিভাইস ব্যবহার করুন

- **সম্ভব হলে কাজের জন্য আলাদা ডিভাইস ব্যবহার করুন। আপনার কাজের ডিভাইসগুলো সব সময় নিরাপদ স্থানে রাখুন এবং সেগুলো বিনা প্রয়োজনে বহন করবেন না।**
- **আপনার সংস্থার দ্বারা অনুমোদিত মেসেজিং টুল ব্যবহার করুন যাতে এন্ড-টু-এন্ড এনক্রিপশন আছে।**
- **সম্ভব হলে ব্লুটুথ সংযোগ বন্ধ রাখুন এবং ব্লুটুথ সংযোগের ব্যবহার কমিয়ে দিন।**
- **অনলাইনে কাজ করার সময় আপনার প্রতিষ্ঠান কর্তৃক অনুমোদিত ভার্চুয়াল প্রাইভেট নেটওয়ার্ক (VPN) ব্যবহার করুন। আপনি যদি কমিউনিটি কম্পিউটার বা ডিভাইস ব্যবহার করেন তাহলে সব সময় আপনার অ্যাকাউন্ট(গুলো) থেকে সাইন আউট করুন।**
- **বায়োমেট্রিক আনলক ফিচার বন্ধ রাখুন-বিশেষ করে ট্রানজিটে থাকার সময়।**

সংবেদনশীল তথ্য রক্ষা করুন এবং তথ্য মিনিমাইজেশন অনুশীলন করুন

- **একটি ডেটা এসেট রেজিস্ট্রি বজায় রাখুন যা আপনার অফিস দ্বারা ব্যবহৃত প্রত্যেক ধরণের তথ্যের জন্য সংবেদনশীলতার স্তর নির্দেশ করে। প্রযুক্তির বিকাশের সাথে সাথে সংবেদনশীলতার মাত্রাগুলো নিয়মিত পর্যালোচনা করুন।**
- **শুধুমাত্র নির্দিষ্ট ডেটা ব্যবস্থাপনা কার্যকলাপের উদ্দেশ্যে এবং উদ্দেশ্য অর্জনের জন্য প্রয়োজনীয় ন্যূনতম পরিমাণ তথ্য সংগ্রহ করুন।**
- **প্রযোজ্য নির্দেশিকা, আইন এবং প্রবিধান দ্বারা যে উদ্দেশ্যে এটি পরিচালনা করা হচ্ছে তা পূরণ করতে যতটুকু প্রয়োজন এবং যতক্ষণ প্রয়োজন, ততটুকু এবং ততক্ষণের জন্য সংবেদনশীল তথ্য সংরক্ষণ করুন।**
- **আপনার সংস্থার দ্বারা অনুমোদিত টুল এবং চ্যানেলগুলো ব্যবহার করে তথ্য স্থানান্তর এবং সঞ্চয় করুন (স্থানীয় ভাবে একটি সংস্থার সার্ভার, কম্পিউটার বা ল্যাপটপে; অথবা OneDrive, SharePoint এবং Teams এর মতো অ্যাপ্লিকেশনগুলোর মাধ্যমে দূর থেকে পরিচালিত সার্ভার এবং সিস্টেম গুলোয়)।**
- **সংবেদনশীল তথ্যসহ ফাইলগুলো (ওয়ার্ড, এক্সেল, পিডিএফ) পাসওয়ার্ড দিয়ে সুরক্ষিত রাখুন এবং আলাদা চ্যানেলের মাধ্যমে ডকুমেন্টের পাসওয়ার্ড শেয়ার করুন (যেমন ইমেইল করা ডকুমেন্টের পাসওয়ার্ড টেক্সট মেসেজের মাধ্যমে পাঠান)।**
- **সংবেদনশীল তথ্য অ্যাক্সেস সহ ব্যক্তিদের সংখ্যা সীমিত রেখে তাদের মনিটর করুন।**
- ব্যবহৃত সব তথ্যের জন্য তথ্য ধারণ এবং ধ্বংসের সময়সূচি নির্ধারণ করুন এবং তথ্য ধ্বংসের জন্য যথাযথ টুলস ব্যবহার করুন।
- আপনার ইমেইল বার্তা এনক্রিপ্ট করুন।

মূল প্রয়োজনীয় উপকরণসমূহ

- হিউম্যানিটারিয়ান অ্যাকশনে ডাটা রেসপনসিবিলিটি সম্পর্কে আইএএসসি-এর অপারেশনাল গাইডেন্স
- ডেটা ইনসিডেন্ট ম্যানেজমেন্টের বিষয়ে নির্দেশিকা নোট
- অনলাইন কনফারেন্সিং টুলের দায়িত্বশীল ব্যবহারের উপর টিপ শীট

মানবিক কার্যক্রমের সংবেদনশীল ডেটা পরিচালনার বিষয়ে আরও জানতে কেন্দ্রের ওয়েবসাইটে ডেটা রেসপনসিবিলিটি পেজে যান বা centrehumdata@un.org এ আমাদের দলের সাথে যোগাযোগ করুন।