Порадник з питань безпеки даних в управлінні операційними даними

березень 2024

Переклад виконано CartONG завдяки підтримці CLEAR Global та Міністерства закордонних та європейських справ Франції.

Вступ

Безпека даних є ключовим компонентом **відповідальності за дані** — безпечного, етичного та ефективного управління даними для оперативного реагування. Це комплекс фізичних, технологічних і процедурних заходів, які забезпечують конфіденційність, цілісність і доступність даних та запобігають їх випадковій або навмисній, незаконній або іншій несанкціонованій втраті, знищенню, зміні, здобуттю або розкриттю.

У цьому пораднику пропонується низка рекомендованих заходів для забезпечення безпеки даних в управлінні операційними даними. Ці заходи повинні здійснюватися згідно з відповідними інституційними повноваженнями, положеннями та нормативно-правовою базою.

Практикуйте належне налаштування паролів

- Захищайте свої пристрої та облікові записи за допомогою надійних паролів, які включають цифри, великі та малі літери, а також символи. У кожному паролі має бути щонайменше 16 знаків.
- Увімкніть багатофакторну автентифікацію для всіх облікових записів.
- Не використовуйте один і той самий пароль для кількох облікових записів.
- Не зберігайте свої паролі на фізичних (наприклад, на нотатках) або цифрових носіях (у файлі на вашому пристрої) і не повідомляйте свій пароль іншим людям.
- Не використовуйте функцію "Запам'ятати мене (Remember Me)" в застосунках і браузерах.
- Негайно змінюйте паролі до своїх облікових записів у мережі інтернет, якщо ви загубили свій пристрій або його було викрадено.

Використовуйте антивірусне/захисне програмне забезпечення

- Переконайтеся, що на ваших пристроях встановлено належне антивірусне/захисне програмне забезпечення.
- Якщо у вас є питання про відповідні інструменти або про їх налаштування, зверніться до IT-спеціаліста у вашому офісі.

Оновлюйте програмне забезпечення та операційні системи

- Регулярно перевіряйте, щоб ваш пристрій, програмне забезпечення, застосунки і плагіни для браузерів були оновленими, та увімкніть автоматичне оновлення операційної системи.
- Використовуйте веббраузери, що отримують автоматичні оновлення безпеки, такі як Chrome або Firefox.
- Вимикайте пристрої в кінці робочого дня, щоб забезпечити оновлення та захиститися від атак.

Уникайте фішингу і пильнуйте, куди ви переходите за посиланням

- Отримуючи підозрілі електронні листи або повідомлення, завжди перевіряйте адресу/контактну інформацію відправника і переходьте за посиланнями або відкривайте вкладення лише, якщо ви довіряєте відправнику.
- Не відповідайте на підозрілі електронні листи та не пересилайте їх колегам.
- Повідомляйте про підозрілу активність службі IT-підтримки.

Відповідально використовуйте мобільні пристрої

- За можливості використовуйте для роботи окремі пристрої. Завжди зберігайте робочі пристрої в безпечному місці та не носіть їх з собою без потреби.
- Використовуйте схвалені організацією месенджери, що забезпечують наскрізне шифрування.
- За можливості вимикайте з'єднання Bluetooth і мінімізуйте його використання.
- Використовуйте схвалену організацією віртуальну приватну мережу (VPN), коли працюєте в Інтернеті. Завжди виходьте зі своїх облікових записів, якщо користуєтеся загальнодоступним комп'ютером чи пристроєм.
- Вимкніть функції біометричного розблокування, особливо під час подорожі.

Захищайте конфіденційні дані та мінімізуйте використання даних

- Ведіть **реєстр активів даних**, в якому вказано рівень конфіденційності для кожного типу даних, якими користується ваш офіс. Регулярно переглядайте рівні конфіденційності, оскільки умови змінюються.
- Збирайте лише мінімальний обсяг даних, необхідний для досягнення мети та виконання конкретних завдань з управління даними.
- Зберігайте конфіденційні дані лише стільки, скільки необхідно для досягнення мети, для якої вони обробляються, а також відповідно до вимог чинних інструкцій, законів та нормативних актів.
- Передавайте та зберігайте дані за допомогою інструментів і каналів, схвалених організацією (локально на сервері, комп'ютері або ноутбуці організації; або на віддалених серверах і системах за допомогою таких додатків, як OneDrive, SharePoint і Teams).
- Захищайте паролем файли (Word, Excel, PDF), що містять конфіденційні дані, та повідомляйте ці паролі до документів через окремі канали (наприклад, відправляйте через месенджер пароль до документа, надісланого електронною поштою).
- Обмежте та ретельно контролюйте кількість людей, які мають доступ до конфіденційних даних.
- Визначте графік зберігання та знищення всіх даних, якими користуєтеся, і застосовуйте відповідні інструменти для знищення даних.
- Шифруйте ваші електронні повідомлення.

Ключові ресурси

- **IASC Operational Guidance on Data Responsibility in Humanitarian Action [Операційний посібник Міжвідомчого постійного комітету щодо відповідальності за дані в гуманітарній діяльності англійською мовою]**
- **Guidance Note on Data Incident Management [Керівництво з реагування на інциденти, пов'язані з використанням даних англійською мовою]**
- **Tip Sheet on the Responsible Use of Online Conferencing Tools [Порадник щодо відповідального використання інструментів для онлайн-конференцій англійською мовою]**

Щоб дізнатися більше про управління конфіденційними даними в гуманітарних операціях, відвідайте сторінку **Відповідальність за дані** на вебсайті Центру або зв'яжіться з нашою командою за адресою: **centrehumdata@un.org**.