



Fizyczne bezpieczeństwo stanowiska pracy

w ramach zaleceń w zakresie podstaw
bezpieczeństwa i ochrony danych dla użytkowników
w sektorze ochrony zdrowia

01. Zamykanie pomieszczeń

- Dbaj o to, aby drzwi do pokoi oraz gabinetów z wrażliwymi danymi były zawsze zamknięte.
- Sprawdzaj, czy po wyjściu z pomieszczenia drzwi zostały poprawnie zamknięte.
- Nie wpuszczaj do stref ograniczonego dostępu osób bez odpowiednich uprawnień.
- Informuj ochronę o osobach przebywających w strefach ograniczonego dostępu bez odpowiednich uprawnień.

02. Zasada „czystego biurka”

- Po zakończeniu pracy, usuń z biurka wszelkie dokumenty zawierające dane wrażliwe.
- Nie pozostawiaj karteczek z hasłami, numerami PESEL, danymi kontaktowymi czy innymi wrażliwymi danymi.
- Upewnij się, że przechowujesz dokumenty w zabezpieczonych miejscach (np. szufladach lub szafach na klucz).
- Nie wyrzucaj dokumentów do zwykłego kosza, korzystaj z niszczarek lub innych metod utylizacji danych.

03. Monitor i ekran

- Jeżeli masz taką możliwość, stosuj filtry prywatności (filtr nakładany na ekran) w sytuacjach, gdy przechodnie mogą obserwować ekran, szczególnie w miejscach publicznych takich jak komunikacja miejska, kawiarnie, uniwersytety czy szpitale.
- Blokuj ekran komputera oraz telefonu nawet podczas krótkiej rozmowy z kimś obok.
- Ograniczaj prezentowanie danych wrażliwych na rzutnikach lub ekranach widocznych dla osób postronnych.

04. Przechowywanie kluczy

- Prowadź ewidencję, kto pobiera klucze do pomieszczeń z dokumentacją lub sprzętem.
- Nie zostawiaj kluczy w drzwiach, na recepcji ani w innych ogólnodostępnych miejscach.
- Po skończeniu pracy zwracaj klucze, by zapobiec ich niekontrolowanemu obiegowi.
- Nie wykonuj samodzielnie kopii kluczy.
- Natychmiast zgłaszaj zagubienie kluczy.

05. Identyfikatory i karty dostępu

- Nie zostawiaj karty dostępu na biurku, w samochodzie czy miejscach ogólnodostępnych.
- Nie udostępniaj nikomu swojego identyfikatora, każda karta lub przepustka powinna być przypisana do jednej osoby.
- Noś identyfikator w sposób umożliwiający kontrolę jego stanu i posiadania.
- Nie wykonuj samodzielnie kopii identyfikatorów ani kart dostępu.
- Jeżeli zgubisz kartę dostępu lub identyfikator, natychmiast poinformuj dział IT. Skontaktuj się z administratorem kontroli dostępu w celu czasowej blokady karty.

06. Drukarki i urządzenia wielofunkcyjne

- Korzystaj z funkcji „secure print” podczas drukowania, wymagającego PIN-u lub innej metody autoryzacji, by uniknąć pozostawiania dokumentów bez kontroli.
- Nie zostawiaj wydrukowanych materiałów w tacy drukarki. Szczególnie takich, które zawierają dane wrażliwe.
- Uważnie wpisuj adres docelowy przy skanowaniu. Drobna literówka może spowodować niekontrolowany wyciek danych.

- Usuń oryginały z podajnika skanera czy kopiarki zaraz po zakończeniu zadania, by nie narażać ich na wgląd osób postronnych.
- Nie dokonuj samodzielnej zmiany haseł drukarek i skanerów.
- Nie instaluj samodzielnie dodatkowego oprogramowania na urządzeniach sieciowych.
- Nie zmieniaj samodzielnie konfiguracji urządzeń sieciowych, jeśli nie posiadasz odpowiednich uprawnień.
- Informuj dział techniczny o komunikatach wskazujących na potencjalne nieautoryzowane modyfikacje.
- Usuń wszelkie dokumenty i nośniki z urządzenia przed przekazaniem go serwisantowi.