13.Zabezpieczenie i dostęp do infrastruktury

Celem niniejszej procedury jest zapewnienie bezpieczeństwa i nadzorowanego dostępu do pomieszczeń i sprzętu służącego do przetwarzania danych osobowych, w celu zapobieżenia nieupoważnionego dostępu osób trzecich i ewentualnym szkodom powstałym w skutek takowego zdarzenia.

Procedura dotyczy właściwego trybu postępowania w trakcie użytkowania sprzętu i pomieszczeń jak również zabezpieczenia dostępu do nich po zakończonym dniu pracy.

Infrastruktura obejmuje:

1. budynki,
2. pomieszczenia związane z udzielaniem świadczeń zdrowotnych, np.: gabinet diagnostyczno-zabiegowy, gabinet lekarski itp.
3. pomieszczenia administracyjne,
4. sprzęt komputerowy i oprogramowanie,
5. urządzenia i aparaturę medyczną.

W pomieszczeniach, w których przechowywane i przetwarzane są dane wrażliwe, dane osobowe przebywać mogą jedynie osoby do tego upoważnione, uwzględnione w Ewidencji osób upoważnionych do przetwarzania danych osobowych.

Inni Pracownicy oraz osoby wizytujące Placówkę mogą przebywać w pomieszczeniach związanych z przechowywaniem i przetwarzaniem danych tylko w obecności osób upoważnionych.

1. Przyjmowanie gości

1. Goście są przyjmowani w pomieszczeniu, w którym nie wolno przechowywać ani zostawiać dokumentacji medycznej, dokumentacji z danymi osobowymi.

2. Goście mogą pozostać sami tylko w wydzielonym pomieszczeniu.

3. Goście nie mają dostępu do urządzeń przetwarzających danych.

2. Zasady przechowywania i wydawania kluczy do pomieszczeń

1. Przydzielanie kluczy:
    a. Po rozpoczęciu dnia pracy Pracownicy pobierają klucze do poszczególnych pomieszczeń.
    b. Upoważnieni pracownicy przechowują klucze do poszczególnych wejść. Pracownicy ci ponoszą pełną odpowiedzialność za ich należyte zabezpieczenie i utrzymanie. Zgubienie klucza należy natychmiast zgłosić Dyrektorowi.
    c. Po zakończeniu pracy klucze są zwracane.
2. Zasady przechowywania kluczy:
    a. Klucze do poszczególnych pomieszczeń przechowywane są w sekretariacie.

   b. Klucze do szafek pracowniczych są w posiadaniu Pracowników, którzy ponoszą pełną odpowiedzialność za ich należyte zabezpieczenie i utrzymanie.

   c. Pracownicy nie mogą używać dorabianych osobiście kluczy do pomieszczeń.

3. Zasady dysponowania kluczami:

   a. Klucze do archiwum są przechowywane i dysponowane zgodnie z Instrukcją postępowania z dokumentacją przechowywaną w Archiwum CUWO.

   b. Osoby które pobrały klucze z rejestracji nie mogą ich udostępniać osobom innym i są zobowiązane do osobistego ich zwrotu w dniu pobrania, po zakończeniu pracy.

   c. Osoby, które zagubiły klucz ponoszą odpowiedzialność materialną.

   d. Nie oddanie klucza powoduje po zakończeniu pracy wszczęcie poszukiwań osoby pobierającej klucz przez osoby, które wyznacza Dyrektor.

4. Wydawanie kluczy zapasowych uprawnionym pracownikom może odbywać się tylko w uzasadnionych przypadkach za zgodą Dyrektora.

5. Odpowiedzialności:

   a. Od momentu pobrania kluczy do momentu ich zwrotu, na upoważnionej osobie spoczywa odpowiedzialność za dane osobowe przechowywane w pomieszczeniu.

   b. Zabrania się wynoszenia kluczy od pomieszczeń poza CUWO.

   c. Utrzymanie skutecznego zabezpieczenia wszystkich pomieszczeń podlega nadzorowi.

3. Zasady zarządzania kluczami kryptograficznymi

1. W CUWO stosowane są następujące klucze kryptograficzne:

   a) podpis elektroniczny (cyfrowy) wraz z certyfikatem klucza publicznego, lub bez certyfikatu jeśli odbiorca danych tego nie wymaga - służący do potwierdzania i ochrony autentyczności dokumentów przechowywanych oraz wychodzących z CUWO, a zawierających dane osobowe.

2. Dostęp do ww. kluczy posiadają jedynie upoważnione do tego osoby. Klucze kryptograficzne chronione są przed modyfikacją, zniszczeniem, utratą lub ujawnieniem.

3. W przypadku podejrzenia, iż dany klucz został ujawniony lub w inny sposób doszło do naruszenia jego bezpieczeństwa, klucz takowy zostaje unieważniony oraz zarchiwizowany.

4. W umowach z dostawcą usług kryptograficznych (np. ośrodkiem cyfryzacji) określono odpowiedzialność cywilnoprawną, niezawodność usług i czas reakcji w trakcie świadczenia usług.

4. Odpowiedzialność personelu

1. Na sprzęcie używanym w CUWO instalowane jest tylko legalne oprogramowanie. Nie wolno instalować i przechowywać na terenie CUWO nielegalnego oprogramowania.

2. Nie należy samowolnie, bez zgody ASI instalować programów.

3. Na sprzęcie komputerowym CUWO nie wolno przechowywać muzyki, filmów, itp. materiałów, których legalnego pochodzenia nie można udowodnić.

4. Ze sprzętu komputerowego CUWO nie wolno korzystać w celach prywatnych.
5. Każdy Pracownik jest obowiązany do zachowania poufności podczas i po zakończeniu stosunku pracy.
6. Osoba zamykająca dane pomieszczenie wychodząc z niego sprawdza:
    a) czy są zamknięte okna,
    b) czy wyłączone są urządzenia elektryczne, które nie muszą funkcjonować systematycznie.

5. Przekazywanie i wynoszenie sprzętu

Pamięci masowe:

- nie wolno korzystać z prywatnych nośników,
- nośniki służbowe należy opróżniać po użyciu,
- wyniesienie i powrót pamięci masowej poza teren Placówki należy ewidencjonować.

Komputery:

- komputerów zawierających wrażliwe dane nie wolno przekazywać,
- przekazując komputer do serwisu należy wymontować dysk twardy,
- dostęp do komputerów musi wymagać uwierzytelnienia.

6. Zabezpieczenie sprzętu komputerowego

1. Opis zastosowanych w danym pomieszczeniu zabezpieczeń dla poszczególnych urządzeń biurowych i komputerowych oraz pozostałych aktywów zawarto w dokumencie Inwentaryzacja aktywów.
2. Wyposażenie jest obsługiwane przez przeszkolony i upoważniony do tego personel.
3. Każdy element wyposażenia jest jednoznacznie etykietowany, oznakowany lub zidentyfikowany w inny sposób.
4. Wyposażenie komputerowe stosowane w CUWO jest przechowywane i eksploatowane w warunkach zapewniających jego prawidłowe funkcjonowanie, zgodnie z wytycznymi producentów.
5. Urządzenia poddaje się kontroli z częstotliwością wynikającą z ich rodzaju i wskazań wytwórców, zgodnie z opracowanym harmonogramem.
6. Zapisy z dokonywanych przeglądów wyposażenia dokonywane są w protokołach, świadectwach, książkach gwarancyjnych oraz kartach przeglądu.
7. W CUWO stosowane jest tylko i wyłącznie oprogramowanie licencjonowane.
8. Wszystkie komputery i laptopy działające w systemie informatycznym posiadają zainstalowane oprogramowanie antywirusowe, dodatkowo sprzęt posiadający połączenie z Internetem chroniony jest zaporą sieciową (firewall) programową lub sprzętową.
9. Przynajmniej raz w miesiącu przeprowadza się sprawdzenie oprogramowania i nośników za pomocą aktualnego programu antywirusowego.

10. Pomieszczenia, w których przechowywany jest sprzęt komputerowy i nośniki informacji są zabezpieczone przed dostępem osób postronnych.
11. Wyposażenie komputerowe zabezpieczone jest przed utratą danych spowodowanych awarią zasilania lub zakłóceniami w sieci zasilającej poprzez zastosowanie listwy antyprzepięciowej.