Podstawy bezpieczeństwa

i ochrony danych w sektorze ochrony zdrowia

csirt Centrum e-Zdrowia

CEZ Centrum e-Zdrowia

Spis treści

CSIRT CEZ

CSIRT CEZ

Współczesne realia cyfrowe wymagają, by każdy pracownik – niezależnie od stanowiska – posiadał podstawową wiedzę na temat bezpiecznego korzystania z systemów informatycznych.

Cyberzagrożenia, takie jak phishing, ransomware czy kradzież tożsamości, stają się coraz bardziej zaawansowane i powszechne. Dlatego tak istotne jest, aby wszyscy pracownicy byli świadomi potencjalnych ryzyk oraz potrafili właściwie reagować na pojawiające się zagrożenia.

Odpowiedzialność za bezpieczeństwo informatyczne spoczywa na nas wszystkich, nie tylko na specjalistach z działów IT. Każdy pracownik odgrywa kluczową rolę w ochronie zasobów organizacji. Zaniedbanie zasad bezpieczeństwa może prowadzić do poważnych konsekwencji, w tym utraty wrażliwych danych, naruszenia reputacji instytucji, a także poważnych strat finansowych.

Ten dokument pomoże w bezpiecznym wykonywaniu codziennych obowiązków – zwłaszcza gdy mamy do czynienia z danymi osobowymi (również medycznymi), dostępem do systemów i sytuacjami wymagającymi szybkiej reakcji. Warto stosować się do kilku prostych zasad, które znajdziesz poniżej, aby lepiej chronić dane i sprzęt w organizacji.

CSIRT CEZ

I. Zarządzanie dostępem i tożsamością

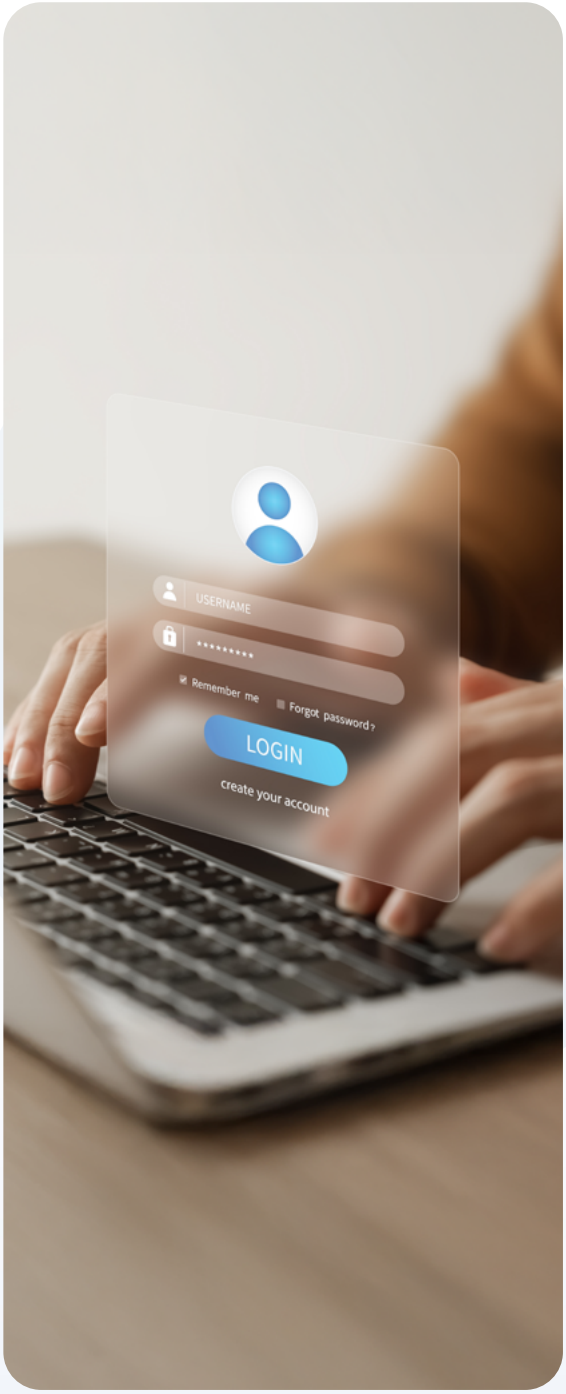
w ramach zaleceń w zakresie podstaw bezpieczeństwa i ochrony danych dla użytkowników w sektorze ochrony zdrowia

01. Tworzenie bezpiecznych haseł

- Stosuj co najmniej 16 znaków.
- Wykorzystuj różne typy znaków (wielkie i małe litery, cyfry, znaki specjalne).
- Unikaj przewidywalnych schematów (np. „P@ssw0rd”, „12345678”, „Qwerty123!”).
- Nie używaj danych osobowych (imię, nazwisko, data urodzenia, nazwa firmy).
- Odrzuć proste hasła złożone z jednego słowa, ponieważ łatwo złamać je atakiem słownikowym.
- Rozważ stosowanie fraz (passphrase) (np. „Mor$k@ Przygod&@ustr@li@”), co wydłuża hasło i utrudnia jego złamanie.
- Unikaj stosowania zbliżonych wariantów haseł („Szpit@!2024”/ „Szpit@!2025”).

02. Posługiwanie się hasłami

- Nigdy nie używaj identycznego hasła do różnych systemów.
- Nie przechowuj haseł w notatnikach, plikach tekstowych, na telefonach czy kartkach.
- Stosuj menedżery haseł do ich tworzenia oraz przechowywania.
- Rozważ cykliczną zmianę haseł (np. co 6 miesięcy), szczególnie w przypadku krytycznych systemów.
- Nie udostępniaj haseł nikomu. Nawet pracownik działu IT nie powinien o nie prosić.
- Jeżeli hasło zostanie ujawnione lub przejęte, zmień je niezwłocznie.
- Nigdy nie przesyłaj haseł e-mailem, poprzez SMS ani inny komunikator.



03. Uwierzytelnianie wieloskładnikowe (MFA)

- Włącz MFA wszędzie tam, gdzie to możliwe. Chronisz w ten sposób konta nawet, gdy hasło wycieknie.
- Korzystaj z aplikacji uwierzytelniających (np. Google Authenticator, Microsoft Authenticator).
- Jeżeli masz taką możliwość, zmień e-maile oraz kody SMS jako metodę dodatkowego uwierzytelniania na dedykowaną aplikację TOTP (np. Authenticator).
- Nie zapisuj ani nie udostępniaj nikomu kodów jednorazowych.
- Nie wpisuj kodów MFA na podejrzanych stronach (zawsze dokładnie sprawdzaj adres strony).
- Nie używaj tego samego urządzenia do logowania i odbioru kodów MFA.
- Jeśli to możliwe, korzystaj z kluczy sprzętowych U2F (np. YubiKey) – zapewniają najwyższy poziom bezpieczeństwa. Stosuj to rozwiązanie szczególnie dla krytycznych systemów.
- Unikaj powiadomień push (wyskakujących powiadomień) dla kodów MFA, jeśli to możliwe.
- Korzystaj z biometrii, jeśli masz taką możliwość (odcisk palca, skan twarzy lub siatkówki).
- Zwracaj uwagę na nietypowe powiadomienia w aplikacjach MFA (np. sytuacja, w której dostajesz powiadomienie z kodem, a nie logujesz się do żadnego systemu).

04. Kontrola uprawnień

- Na urządzeniach służbowych loguj się wyłącznie do tych systemów, których obsługa mieści się w zakresie Twoich obowiązków.
- Zwracaj uwagę, czy nie posiadasz zbyt szerokich uprawnień, nie proś o dostęp do systemów lub danych, których nie potrzebujesz do wykonywania swoich obowiązków.
- Zachowaj ostrożność podczas przyznawania dostępu innym. Upewnij się, że osoby, którym przyznajesz dostęp, rzeczywiście go potrzebują.
- Zgłaszaj wszelkie przypadki nadmiarowego dostępu do danych oraz systemów, które nie mieszczą się w Twoim zakresie lub zakresie współpracowników.
- Nie korzystaj z kont współdzielonych ani należących do innych osób, nie przekazuj własnych danych logowania.
- Nie loguj się z niezabezpieczonych oraz nieznanych urządzeń do zasobów oraz systemów organizacyjnych.
- Nie dopuszczaj do sytuacji, w której inna osoba wykorzystuje Twoją zalogowaną sesję.

05. Monitorowanie aktywności kont i wykrywanie zagrożeń

- Jeśli zauważysz nietypowe godziny logowania lub logowanie z podejrzanych lokalizacji, szczególnie dotyczące kont z podwyższonymi uprawnieniami, natychmiast zgłoś zaistniałą sytuację do działu IT.
- Zgłaszaj próby nieautoryzowanego dostępu. Jeśli dostaniesz informację o nieudanej próbie logowania na Twoje konto, powiadom dział IT.
- Jeśli masz podejrzenie, że ktoś nieuprawniony mógł skorzystać z Twojego profilu, powiadom swojego przełożonego oraz dział IT.
- Nie ignoruj powiadomień o zmianach na koncie – jeśli dostaniesz wiadomość o zmianie hasła lub dodaniu nowego urządzenia, a tego nie robiłeś (lub nie zlecałeś), działaj natychmiast.
- Zwracaj uwagę na nietypowe zachowania systemu, takie jak spowolnienia, nagłe wylogowania czy nietypowe błędy, które mogą być oznaką naruszenia bezpieczeństwa.

06. Aktualizowanie dostępów

- Zgłaszaj posiadanie nieaktualnych lub zbędnych dostępów.
- Usuwaj dostępy byłym pracownikom.
- Jeśli ktoś odszedł z firmy, upewnij się, że jego konta zostały dezaktywowane (np. poczta, Intranet, VPN).
- Unikaj posiadania dostępu do systemów oraz zasobów niezwiązanych z Twoimi obowiązkami.
- Zachowaj czujność, jeśli bez wyraźnego uzasadnienia zyskujesz nowe funkcje w systemach.
- Aktualizuj dane kontaktowe w systemach zabezpieczeń. Po zmianie numeru telefonu lub adresu e-mail powiązanych z kontem, pamiętaj o ich aktualizacji w systemie.

CSIRT CEZ

II. Ochrona przed atakami phishingowymi

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

01. Identyfikacja podejrzanych wiadomości

- Nie otwieraj wiadomości od nieznanych nadawców.
- Jeśli nie spodziewasz się wiadomości, traktuj ją jako potencjalnie niebezpieczną.
- Zwracaj uwagę na błędy językowe i gramatyczne.
- Sprawdzaj poprawność adresu nadawcy (np. literówki sekretariat@zspital.pl czy support@micros0ft.com).
- Nie klikaj w linki i nie otwieraj załączników bez weryfikacji – zawsze sprawdzaj, dokąd prowadzi link, najeżdżając na niego kursorem (bez klikania w link).
- Ostrożnie podchodź do wiadomości z prośbą o pilne działanie. Phishing zwykle bazuje na presji czasu (np. „Twoje konto zostanie zablokowane w ciągu 24h!”).
- Zwracaj uwagę na nietypowe formaty plików. Oszuści często wysyłają zainfekowane pliki w formatach .exe, .scr, .js, .zip, a także makra w dokumentach Word oraz Excel.

02. Postępowanie w przypadku podejrzanych wiadomości

- Nie odpowiadaj na podejrzane wiadomości. Nawet, jeśli wydaje się, że pochodzą od znanej firmy, skontaktuj się z nią innym kanałem w celu weryfikacji.
- Nie podawaj loginów i haseł przez e-mail lub telefon. Żadna firma, bank ani dział IT nie powinni prosić o podanie hasła przez wiadomość lub telefon.
- W przypadku wątpliwości co do autentyczności wiadomości, zgłoś ją do działu IT.
- Nie usuwaj podejrzanych wiadomości. Mogą okazać się istotne podczas analizy w razie wystąpienia incydentu.
- Jeśli przypadkowo kliknąłeś w podejrzany link, natychmiast zgłoś to zdarzenie do działu IT.
- Jeśli e-mail zawiera link do logowania, nie używaj go. Zamiast tego wejdź na stronę ręcznie przez przeglądarkę.
- Po otrzymaniu podejrzanej wiadomości uprzedź współpracowników o możliwej próbie ataku.
- Nie ujawniaj żadnych informacji o wewnętrznych zabezpieczeniach, procedurach oraz innych wrażliwych danych.

03. Postępowanie z załącznikami

- Otwieraj wyłącznie pliki od nadawców, których tożsamość i adres e-mail możesz potwierdzić.
- Zwracaj uwagę na rozszerzenia, fałszywe pliki mogą mieć podwójne rozszerzenia (np. .pdf.exe).
- Unikaj bezpośredniego otwierania linków w e-mailach zapraszających do pobrania załącznika, jeśli nie masz pewności, że pochodzą z wiarygodnego źródła.
- Pamiętaj, że nawet obrazy (.jpg, .png, .gif) mogą zawierać złośliwy kod, zwłaszcza jeżeli pobrano je z niezaufanych stron.
- Zawsze skanuj pliki antywirusem, wykonuj to szczególnie przed otworzeniem grafik w e-mailach, które budzą Twoje wątpliwości.
- Nie klikaj w osadzone linki w grafikach, niektóre obrazy mogą przekierowywać do stron phishingowych lub pobierać złośliwe skrypty i wirusy.
- Włączaj makra wyłącznie, gdy jest to absolutnie niezbędne i tylko w przypadku plików, których źródła jesteś pewien.
- Zachowuj ostrożność przy plikach w formacie .xlsm, .docm, .pptm – to rozszerzenia dla dokumentów z domyślnie włączonymi makrami.
- Nigdy nie uruchamiaj makr, jeżeli dokument dotyczy tematu, który nie ma związku z Twoimi obowiązkami lub pochodzi od nieznanej osoby.
- Nie przesyłaj wrażliwych załączników na prywatne maile, dyski chmurowe czy komunikatory.
- Skanuj skompresowane archiwa oraz zawsze używaj antywirusa przed otwarciem plików: .zip, .rar, .7z itp.
- Weryfikuj zawartość załączników Jeśli w archiwum spodziewasz się jednego pliku .pdf, a znajdujesz wiele różnych plików (np. .exe czy .js), nie rozpakowuj pliku i skontaktuj się z działem IT.
- Jeśli wiadomość zawiera zaszyfrowany załącznik i jednocześnie w treści jest podane hasło, zachowaj szczególną ostrożność. Często w ten sposób omija się zabezpieczenia poczty.

CSIRT CEZ

III. Ochrona przed atakami socjotechnicznymi

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

01. Jak rozpoznać próbę ataku socjotechnicznego? Jak działają cyberprzestępcy?

- Wykorzystują presję czasu oraz pilność działania, twierdząc, że musisz natychmiast wykonać przelew, zmienić hasło lub przekazać dane logowania, strasząc konsekwencjami.
- Podszywają się pod przełożonych, pracowników działów IT, dostawców usług, banki lub instytucje rządowe, aby wzbudzić Twoje zaufanie.
- Próbują zdobyć Twoją sympatię lub wzbudzić strach, by zmusić Cię do działania.
- Dzwonią z nieznanych lub ukrytych numerów telefonów oraz wykorzystują fałszywe (chociaż z pozoru poprawne) adresy e-mail.
- Proszą o podanie poufnych danych, zwykle posiadając już wcześniej pewne dane ofiary np. adres zamieszkania, nazwisko przełożonego bądź prywatny nr telefonu.
- Alarmujące powinno być nieoczekiwane powiadomienie o logowaniu lub próbie dostępu, którego nie wykonałeś.
- Możesz otrzymać informację o fałszywej sytuacji kryzysowej (np. „Twoje konto zostało zhakowane, musisz natychmiast zmienić hasło" lub „Twoja firma została zaatakowana, pobierz to narzędzie do zabezpieczenia systemu").
- Wykorzystują nietypowe sposoby komunikacji np. „przełożony" nagle pisze do Ciebie przez prywatny adres e-mail lub komunikator, zamiast przez firmowe kanały komunikacji.

02. Jak zapobiegać atakom socjotechnicznym?

- Nie podejmuj żadnych działań pod presją. Jeśli rozmówca nalega na szybkie działanie, wstrzymaj się i sprawdź sytuację.
- Weryfikuj rozmówców, zanim przekażesz jakiekolwiek informacje. Zawsze sprawdzaj tożsamość osób, które proszą o dostęp do danych lub systemów.
- Jeśli przełożony lub pracownik działu IT prosi Cię o zmianę hasła, przelew lub dostęp do systemu, potwierdź to innym kanałem.
- Korzystaj z uwierzytelniania wieloskładnikowego (MFA).
- Konsultuj się ze współpracownikami, jeśli coś budzi Twój niepokój.
- Zgłaszaj wszelkie podejrzane sytuacje do odpowiedniego działu (bezpieczeństwa lub IT).
- Nie udostępniaj w mediach społecznościowych informacji o pracy i strukturze firmy. Oszuści mogą wykorzystać takie dane do przygotowania przekonujących ataków.
- Ogranicz dostęp do poufnych informacji. Niech będą dostępne tylko dla upoważnionych osób.
- Unikaj dzielenia się informacjami przez niezabezpieczone kanały komunikacji. Do przesyłania poufnych danych używaj tylko autoryzowanych systemów firmowych.
- Stosuj zasadę minimalnych uprawnień oraz nie udostępniaj danych osobom spoza firmy.
- Nie otwieraj podejrzanych linków i załączników w e-mailach. Nawet jeśli wiadomość pochodzi od znanego nadawcy, sprawdź jej autentyczność.
- Nie pobieraj i nie instaluj oprogramowania spoza oficjalnych źródeł.Cyberprzestępcy mogą zachęcać do instalacji „aktualizacji” lub „narzędzi bezpieczeństwa”, które w rzeczywistości zawierają złośliwe oprogramowanie.

CSIRT CEZ

IV. Bezpieczne korzystanie z urządzeń i nośników danych

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

01. Blokowanie ekranu

- Zawsze blokuj komputer (np. skrótem Win+L), smartfon oraz inne urządzenia nawet, gdy tylko na chwilę odchodzisz od stanowiska pracy. W systemie macOS możesz skorzystać z kombinacji Ctrl+Cmd+Q (lub odpowiednio skonfigurować klawisz skrótu).
- Ustaw automatyczną blokadę ekranu po krótkim czasie bezczynności (np. 1-2 min).
- Reaguj, jeśli zauważysz niezablokowany komputer pozostawiony bez nadzoru.

02. Aktualizacje

- Regularnie instaluj poprawki systemowe oraz aktualizacje aplikacji.
- Akceptuj automatyczne instalowanie poprawek systemowych (Windows, Mac, przeglądarki itp.).
- Nie wyłączaj programów antywirusowych ani nie ignoruj powiadomień dotyczących bezpieczeństwa.
- Zgłaszaj brak możliwości instalacji niezbędnych aktualizacji.
- Korzystaj wyłącznie z oficjalnych źródeł – pobieraj aplikacje z zatwierdzonych repozytoriów lub sklepów, aby uniknąć złośliwego oprogramowania.

03. Pendrive oraz dyski zewnętrzne

- Ogranicz stosowanie niezaufanych nośników, nie podłączaj pendrive'ów pochodzących z niesprawdzonych źródeł.
- Szyfruj urządzenia przenośne, zwłaszcza jeśli służą do przechowywania danych osobowych lub medycznych.
- Przechowuj nośniki w zabezpieczonych miejscach (zamykane szuflady, szafy), aby utrudnić dostęp osobom postronnym.
- Usuwaj zbędne pliki w celu zmniejszenia negatywnych skutków potencjalnej kradzieży lub utraty nośnika.
- Zgłaszaj zagubienie lub kradzież nośnika danych działowi bezpieczeństwa i przełożonemu.

04. Fizyczne przechowywanie sprzętu

- Nie pozostawiaj służbowych urządzeń w samochodzie, recepcji ani innych miejscach publicznych bez nadzoru.
- Zabezpieczaj telefony i tablety hasłami lub metodami biometrycznymi.
- Blokuj urządzenie lub wyłącz je przed odłożeniem w torbie lub szafce.
- Zgłaszaj każde zaginięcie sprzętu i opisuj okoliczności, w których mogło do niego dojść.

05. Wyłączanie nieużywanych interfejsów

- Wyłączaj Bluetooth oraz Wi-Fi, jeśli aktualnie z nich nie korzystasz.
- Korzystaj z przewodowych połączeń sieciowych zawsze, gdy to możliwe.
- Nie łącz się automatycznie z sieciami Wi-Fi, szczególnie nieznanymi (np. w kawiarniach, hotelach).
- Przeglądaj listę sparowanych urządzeń i regularnie usuwaj te, których już nie używasz.

06. Tworzenie i zarządzanie kopiami zapasowymi

- Regularnie zapisuj ważne pliki w bezpiecznych miejscach, najlepiej na firmowym serwerze, w chmurze lub na zaszyfrowanym nośniku zgodnie z polityką firmy.
- Nie przechowuj jedynej kopii plików na swoim komputerze, ponieważ w razie awarii sprzętu wszystkie dane mogą zostać utracone. Twórz kopie zapasowe.
- Automatyzuj procesy tworzenia backupów (kopii zapasowych). Jeśli Twoja organizacja oferuje automatyczne backupy, upewnij się, że są one aktywne.
- Zapisuj kopie w odpowiednich folderach. Nie przechowuj ich w przypadkowych lokalizacjach, gdzie łatwo je usunąć lub o nich zapomnieć.
- Nie zapisuj kopii na prywatnym komputerze, telefonie czy pendrive'ach. Dane firmowe powinny być przechowywane wyłącznie w autoryzowanych systemach.
- Szyfruj kopie zapasowe. Dane powinny być zabezpieczone przed dostępem nieuprawnionych osób.
- Unikaj przechowywania kopii zapasowych na tych samych serwerach lub urządzeniach, których dotyczą.
- Nie udostępniaj nikomu haseł do swoich kopii zapasowych. Dostęp do backupów powinni posiadać wyłącznie uprawnieni użytkownicy.
- Nie ignoruj komunikatów o błędach backupu lub braku miejsca na dysku. Jeśli system nie może zapisać kopii zapasowej, zgłoś to do działu IT.
- Nie otwieraj podejrzanych plików z kopii zapasowych, jeśli nie wiesz, skąd pochodzą.
- Stosuj politykę magazynowania danych. Starsze pliki mogą zawierać nieaktualne informacje i nie powinny być przechowywane w nieskończoność.

CSIRT CEZ

V. Bezpieczne korzystanie z internetu

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

01. Weryfikacja witryn internetowych

- Sprawdź, czy adres strony (URL) wygląda autentycznie. Unikaj stron z literówkami, podejrzanymi rozszerzeniami lub imitacją znanych nazw.
- Oceń wygląd i zawartość strony. Na oszustwo mogą wskazywać: brak aktualizacji grafiki, błędy językowe czy nieaktywne przyciski na stronie.
- Bądź czujny w przypadku wyskakujących okien proszących o ponowne dane logowania. To mogą być fałszywe strony.
- W razie wątpliwości dotyczących wiarygodności witryny skonsultuj się z działem bezpieczeństwa.

02. Ustawienia przeglądarek

- Regularnie aktualizuj przeglądarkę i wtyczki.
- Wyłącz zbędne rozszerzenia i wtyczki, ograniczaj liczbę dodatków tylko do tych, które są konieczne do pracy.
- Odrzucaj prośby o instalację nieznanych rozszerzeń.
- Wyłącz automatyczne zapisywanie haseł w przeglądarce.
- Włącz blokadę wyskakujących okien.
- Włącz ochronę przed śledzeniem.
- Ogranicz dostęp do informacji o lokalizacji.

03. Media społecznościowe

- Nie korzystaj z prywatnych mediów społecznościowych na urządzeniach służbowych.
- Nie publikuj i nie przesyłaj informacji dotyczących służbowych danych ani danych pacjentów poprzez komunikatory takie jak np. Messenger czy WhatsUp.
- Korzystaj z prywatnych ustawień profilu, ogranicz widoczność postów i danych osobowych do zaufanego grona.
- Weryfikuj zaproszenia i prośby o dodanie do znajomych. Nie akceptuj pochopnie próśb od nieznanych osób, które mogą podszywać się pod współpracowników.
- Nie udostępniaj zrzutów ekranu z systemów służbowych.
- Informuj dział IT o podejrzanych aktywnościach (np. próbach wyłudzenia danych w wiadomościach prywatnych).

04. Publiczne sieci Wi-Fi

- Korzystaj z VPN w miejscach publicznych (kawiarnie, lotniska, hotele), jeśli zamierzasz łączyć się z systemami służbowymi.
- W miarę możliwości używaj tetheringu (udostępnionego Internetu z telefonu), zamiast łączyć się z przypadkowymi punktami dostępowymi.
- Nigdy nie loguj się do poczty lub systemów służbowych w nieszyfrowanych sieciach otwartych.
- Weryfikuj nazwę hotspotów, aby przypadkowo nie połączyć się z fałszywą siecią o bardzo podobnej nazwie.
- Wyłącz automatyczne łączenie z nieznanymi sieciami Wi-Fi, by uniknąć przypadkowego połączenia do niebezpiecznego punktu dostępowego.

CSIRT CEZ

VI. Praca zdalna

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

01. VPN i zdalny dostęp

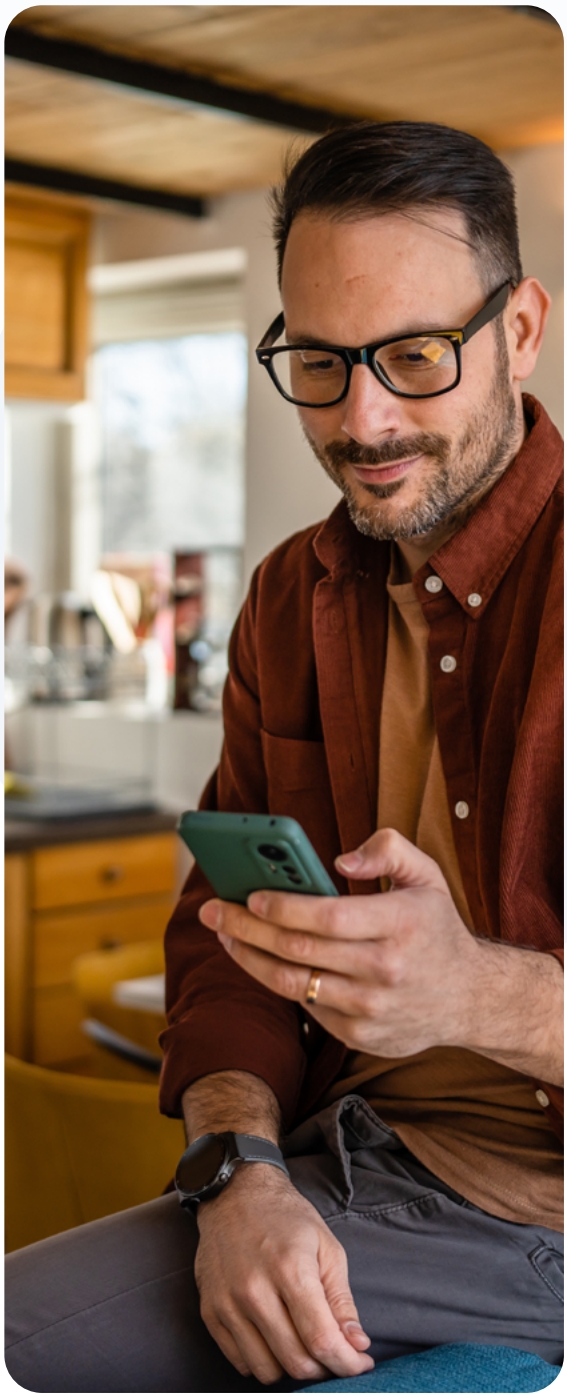
- Korzystaj wyłącznie z oficjalnych rozwiązań VPN zatwierdzonych przez organizację, aby zapewnić szyfrowanie i ochronę przesyłanych danych.
- Nie twórz prywatnych tuneli zdalnych (np. samodzielnie zainicjowanych połączeń typu RDP czy VNC) bez zgody działu IT.
- Zawsze włączaj VPN przed rozpoczęciem pracy zdalnej, szczególnie podczas łączenia się z sieciami publicznymi lub domowymi.
- Upewnij się, że VPN automatycznie odnawia połączenie w przypadku chwilowego zerwania sieci.
- Unikaj korzystania z VPN na niezaufanych lub publicznych urządzeniach.
- Zawsze pracuj z VPN w trybie „pełnego tunelowania" (full tunnel), aby cały ruch internetowy przechodził przez zabezpieczoną sieć organizacji.
- Unikaj przesyłania poufnych danych, jeśli VPN nie działa lub jest wyłączony – poczekaj na jego ponowne uruchomienie.
- Zgłaszaj wszelkie problemy z VPN, by nie pracować bez ochrony szyfrowania.
- Zamykaj sesję VPN po zakończeniu pracy.

02. Bezpieczeństwo w domu

- Skonfiguruj domowy router z bezpiecznym hasłem WPA2/WPA3, nigdy nie pozostawiaj ustawień fabrycznych (login/hasło typu „admin").
- Nie udostępniaj służbowego sprzętu domownikom do prywatnych celów.
- Korzystaj z ustronnego miejsca pracy, by ograniczyć ryzyko podsłuchania rozmów czy wglądu w monitor.
- Blokuj ekran nawet we własnym domu, zapobiegając niezamierzonemu dostępowi.
- Korzystaj wyłącznie z zatwierdzonych urządzeń i aplikacji do pracy zdalnej.
- Nie instaluj na służbowym sprzęcie prywatnego oprogramowania, które może stanowić zagrożenie bezpieczeństwa.
- Nie podłączaj do sieci służbowej niezaufanych urządzeń (np. smart home, telewizorów czy konsol do gier).
- Nie pozostawiaj dokumentów służbowych w ogólnodostępnych miejscach.
- Nie drukuj dokumentów służbowych w domu, jeśli nie jest to absolutnie konieczne.

03. Przechowywanie danych na urządzeniach mobilnych

- Włącz szyfrowanie dysku w laptopie, tablecie lub telefonie.
- Używaj silnych metod uwierzytelniania – hasła, PIN-u lub biometrii (odcisku palca, rozpoznawania twarzy).
- Nie polegaj na podstawowych metodach zabezpieczenia, takich jak proste przesunięcie palca po ekranie.
- Ustaw automatyczne blokowanie ekranu po krótkim czasie nieaktywności.
- Unikaj instalacji aplikacji spoza oficjalnych sklepów (Google Play, App Store, Microsoft Store).
- Regularnie aktualizuj system operacyjny i aplikacje, aby eliminować luki bezpieczeństwa.
- Nie przechowuj danych służbowych w prywatnych chmurach (Google Drive, Dropbox, OneDrive, iCloud).
- Korzystaj wyłącznie z firmowych rozwiązań do przechowywania danych i synchronizacji plików.
- Nie przesyłaj poufnych danych za pomocą prywatnych komunikatorów oraz e-maili.
- Jeśli urządzenie przestaje być używane do celów służbowych, upewnij się, że wszystkie dane zostały bezpiecznie usunięte.
- Nie zapisuj plików zawierających dane wrażliwe na komputerze prywatnym.
- Usuwaj lokalne kopie dokumentów zaraz po ich wykorzystaniu.
- Sprawdzaj, czy poufne dane nie pozostały w folderach tymczasowych (np. „Pobrane”).



CSIRT CEZ

VII. Reagowanie na incydenty

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

01. Rozpoznanie nietypowych objawów

- Zwracaj uwagę na niecodzienne komunikaty, spowolnione działanie komputera lub inne niepokojące zachowania systemu.
- Bądź wyczulony na podejrzane wiadomości e-mail, prośby o hasło czy nieoczekiwane alerty antywirusowe.
- Stosuj się do zasady, że w przypadku wątpliwości zawsze lepiej zgłosić podejrzane zdarzenie, niż przeoczyć zagrożenie.

02. Wstępne działania

- Jeżeli podejrzewasz atak (np. wirus, ransomware) lub zauważysz nieautoryzowaną aktywność, bezzwłocznie wyłącz Wi-Fi lub odłącz kabel sieciowy, aby zatrzymać ewentualne rozprzestrzenianie się zagrożenia.
- Zapisz dokładny czas wystąpienia niepokojących zdarzeń, które zwróciły Twoją uwagę, oraz podjęte czynności przed pojawieniem się incydentu i w trakcie jego trwania.
- Unikaj samodzielnego usuwania plików czy formatowania dysku, możesz zatrzeć ślady istotne dla analizy incydentu. Nie otwieraj ponownie podejrzanych plików.
- Unikaj dalszych działań, które mogłyby zatrzeć istotne informacje potrzebne do ustalenia przyczyny incydentu.
- Jeśli to możliwe utrwal dowody, błędy systemu (zrzuty ekranu), aby pomóc w analizie.
- Ustal, czy problem dotyczy jedynie Twojego stanowiska, czy ma szerszy zasięg.

03. Zgłaszanie incydentu

- Skontaktuj się z przełożonym i/lub działem IT w celu zgłoszenia incydentu.
- Przekaż krótki opis zdarzenia – co się stało, kiedy wystąpiło i jakie zauważyłeś/łaś symptomy.
- Ostrzeż współpracowników, żeby nie otwierali podobnych wiadomości czy plików.

CSIRT CEZ

VIII. 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.
- Usuwaj oryginały z podajnika skanera czy kopiarki zaraz po zakończeniu zadania, by nie narazić 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.

CSIRT CEZ

IX. Zasady postępowania w razie braku sieci lub awarii systemu

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

01. Działania podczas awarii

- Zachowaj spokój i zgłoś problem do działu IT lub osobie odpowiedzialnej za infrastrukturę techniczną w firmie.
- Sprawdź podstawowe przyczyny problemu. Upewnij się, czy problem dotyczy tylko Twojego urządzenia (np. restartując komputer), czy całej sieci lub systemu.
- Odłącz się od sieci i ponownie połącz. Problem może wynikać z chwilowego błędu połączenia.
- Korzystaj z alternatywnych metod pracy, jeśli to możliwe, używaj dokumentacji papierowej lub zapasowych systemów offline.
- Jeśli masz dostęp do innego działającego systemu, skorzystaj z niego, często awaria dotyczy tylko jednego segmentu sieci.
- Zapisuj kluczowe informacje, aby wprowadzić je do systemu po jego przywróceniu.
- Stosuj się do procedur awaryjnych organizacji (każda firma powinna mieć plan działania na wypadek awarii).

02. Czego unikać podczas awarii?

- Nie próbuj resetować systemu na własną rękę bez polecenia czy instrukcji działu IT. Nieodpowiednie działania mogą doprowadzić do utraty danych lub wydłużenia awarii.
- Nie próbuj samodzielnie rekonfigurować ustawień sieciowych. Jeśli problem leży po stronie infrastruktury, nieautoryzowane zmiany mogą pogorszyć sytuację.
- Nie zapisuj poufnych informacji na prywatnych urządzeniach. Brak dostępu do firmowego systemu nie jest powodem do przenoszenia danych na osobiste laptopy, telefony czy pendrive'y.
- Nie korzystaj z publicznych sieci Wi-Fi do obchodzenia problemu.
- Nie ignoruj komunikatów działu IT. Jeśli dostaniesz konkretne instrukcje dotyczące postępowania, stosuj się do nich, nie działaj na własną rękę.
- Nie próbuj wielokrotnie logować się do systemu, jeśli nie działa. Może to doprowadzić do blokady konta i dodatkowych utrudnień.
- Nie przesyłaj wrażliwych danych przez prywatne komunikatory. Jeśli firmowa poczta lub systemy nie działają, nie oznacza to, że można używać np. WhatsApp czy prywatnych e-maili.
- Nie rozpowszechniaj niesprawdzonych informacji o awarii. Jeśli nie posiadasz oficjalnych informacji z działu IT, nie spekuluj na temat przyczyn i konsekwencji problemu.

CSIRT CEZ

X. Bezpieczeństwo teleporad i wideokonsultacji

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

01. Wybór odpowiedniego oprogramowania

- Korzystaj wyłącznie z zatwierdzonych przez placówkę platform do wideokonferencji. Powinny one gwarantować szyfrowane połączenia i zgodność z regulacjami dotyczącymi ochrony danych.
- Nie używaj do pracy prywatnych komunikatorów (np. WhatsApp, Messenger, Skype).
- Regularnie aktualizuj użytkowane oprogramowanie.
- Nie instaluj nieznanych aplikacji na urządzeniach służbowych. Używaj wyłącznie oficjalnych narzędzi rekomendowanych przez dział IT.
- Korzystaj z wersji biznesowych systemów lub platform medycznych, jeśli są dostępne (np. Microsoft Teams dla firm czy systemów dedykowanych dla telemedycyny).
- Nie próbuj na własną rękę instalować dodatkowych programów do poprawy jakości połączeń. Mogą one naruszać bezpieczeństwo systemów.

02. Zapewnienie prywatności rozmów

- Przeprowadzaj teleporady i wideokonsultacje w pomieszczeniu bez osób postronnych.
- Używaj słuchawek, aby zapobiec przypadkowemu podsłuchowi, szczególnie w miejscach, gdzie znajdują się inni pracownicy lub domownicy.
- Z wyprzedzeniem ustal, czy rozmowa może być nagrywana i na jakich warunkach. Nagrania powinny być przechowywane zgodnie z polityką placówki.
- Zamykaj okna i drzwi w trakcie konsultacji. Minimalizuje to ryzyko naruszenia prywatności pacjenta.
- Unikaj przeprowadzania teleporad w miejscach publicznych – kawiarnie, pociągi czy poczekalnie nie są odpowiednimi miejscami do omawiania poufnych informacji pacjentów.
- Nie używaj publicznych sieci Wi-Fi do przeprowadzania teleporad.

03. Weryfikacja pacjenta lub rozmówcy

- Zachowaj ostrożność, jeśli pacjent łączy się z nieznanego numeru lub adresu e-mail. Jeśli masz wątpliwości, potwierdź jego tożsamość innym kanałem.
- Nie podawaj wrażliwych informacji, dopóki nie potwierdzisz tożsamości rozmówcy. Nawet jeśli ktoś twierdzi, że jest pacjentem lub współpracownikiem.
- Przed rozpoczęciem konsultacji potwierdź tożsamość rozmówcy np. poprzez podanie numeru PESEL, daty urodzenia lub innego unikalnego identyfikatora.
- Nie udostępniaj pacjentowi lub klientowi jego własnych danych w celu potwierdzenia tożsamości. To pacjent powinien podać swoje dane w celu weryfikacji.
- Uważaj na przypadki podszywania się pod pacjentów (tzw. vishing). Jeśli rozmówca zachowuje się podejrzanie lub nie jest w stanie podać poprawnych danych, rozważ zakończenie rozmowy i skontaktowanie się z nim innym sposobem.
- Jeśli pacjent chce, aby inna osoba uczestniczyła w rozmowie, wymagana jest jego wyraźna zgoda. Najlepiej zapisana w dokumentacji medycznej i potwierdzona przez pacjenta na piśmie.
- Nie udostępniaj informacji medycznych osobom nieupoważnionym.

04. Bezpieczne przechowywanie dokumentacji z teleporad

- Przetwarzaj informacje z teleporady tak, jak w przypadku tradycyjnej wizyty, zachowując zgodność z przepisami i wewnętrznymi procedurami placówki.
- Nie przechowuj nagrań i dokumentów na prywatnym komputerze lub telefonie. Dane medyczne i służbowe muszą być archiwizowane w zatwierdzonych systemach.
- Korzystaj wyłącznie z firmowych systemów do przechowywania danych.
- Regularnie sprawdzaj uprawnienia dostępu do dokumentacji. Upewnij się, że tylko uprawnione osoby mają do niej dostęp.
- Nie udostępniaj raportów z wideokonsultacji przez niezabezpieczone kanały np. prywatne e-maile, niezaufane chmury czy komunikatory.

Podsumowanie

Zachęcamy do wykorzystania tego dokumentu jako punktu wyjścia do stworzenia efektywnych wewnętrznych zasad i procedur w sektorze ochrony zdrowia. Z uwagi na to, że każdy podmiot ma indywidualny charakter – unikalne zadania, przetwarzane dane i systemy. W związku z tym rekomendujemy dokładną analizę własnych potrzeb oraz konsultacje z ekspertami prawa i technologii przed implementacją opisanych tu wytycznych. Wdrożenie tych zasad wzmocni ochronę danych obywateli i pacjentów. Przyczyni się też do utrzymania wysokiego standardu usług oraz pozytywnie wpłynie na wizerunek instytucji. Ze względu na ciągłą ewolucję zagrożeń w sieci, konieczne jest systematyczne sprawdzanie i dostosowywanie zalecanych działań do aktualnych warunków, w oparciu o obowiązujące przepisy i najlepsze praktyki.