CSIRT CEZ

Zarządzanie dostępem i tożsamością

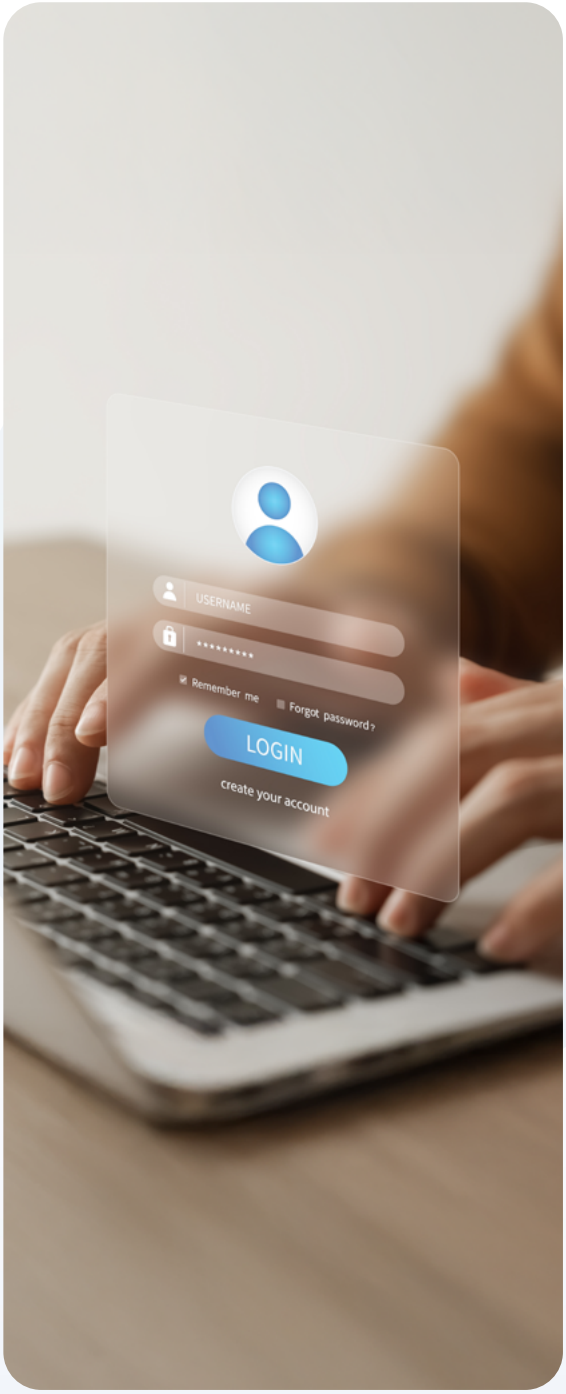
w ramach zaleceń w zakresie podstaw bezpieczeństwa i ochrony danych dla użytkowników w sektorze ochrony zdrowia

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.



CSIRT CEZ

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.