CSIRT CEZ

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.

CSIRT CEZ

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”).