CSIRT CEZ

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.