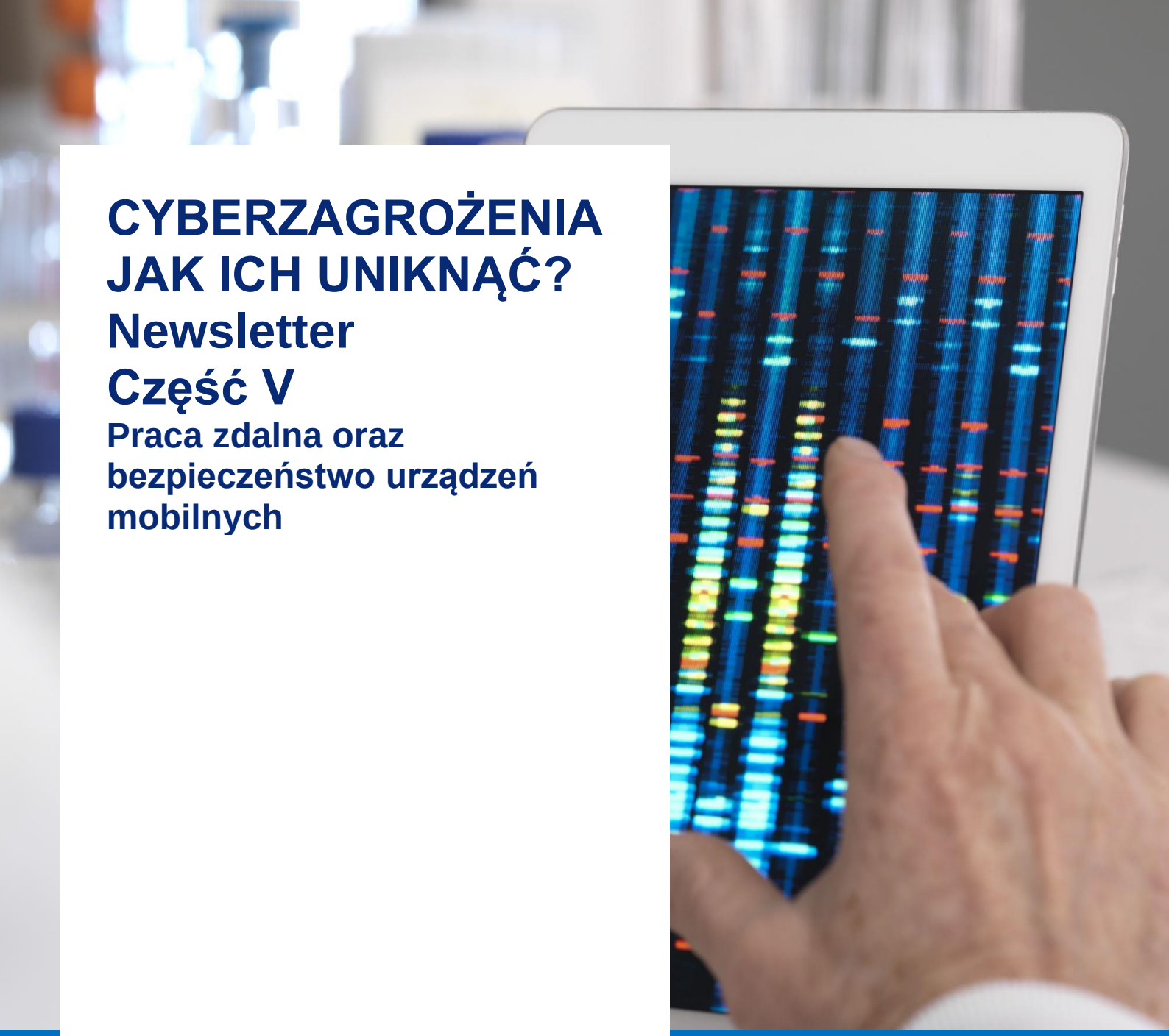


CYBERZAGROŻENIA JAK ICH UNIKNĄĆ?

Newsletter

Część V

Praca zdalna oraz bezpieczeństwo urządzeń mobilnych

Newsletter nr V

stillsec

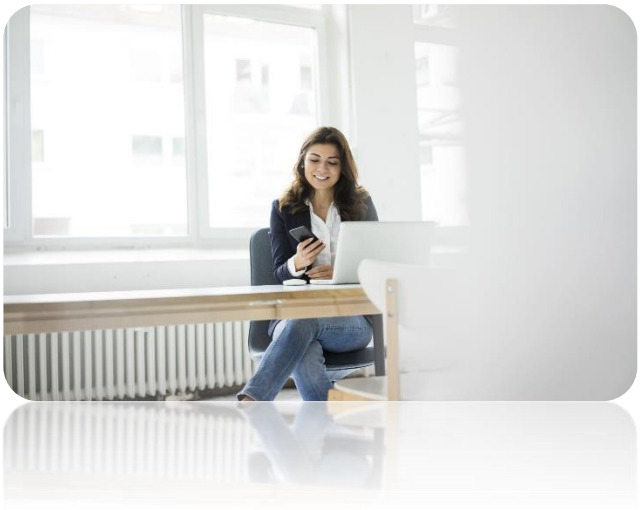
Wojewódzki Szpital Specjalistyczny nr 5 im. Św. Barbary w Sosnowcu

Centrum Urazowe

BEZPIECZEŃSTWO PRACY ZDALNEJ

Praca zdalna (*home office*) to wyzwanie dla Szpitala oraz jego personelu. Domowe środowisko pracy nie zapewnia zwykle takich samych zabezpieczeń, co praca w miejscu zatrudnienia. Przed rozpoczęciem pracy zdalnej warto zapoznać się obowiązującymi procedurami i zasadami bezpieczeństwa, do których należy się stosować. Pozwoli to na lepszą kontrolę nad danymi Szpitala i zabezpieczenia ich przez zagrożeniami. Z tego *newslettera* dowiecie się Państwo, jak zadbać o bezpieczną pracę zdalną oraz bezpieczeństwo urządzeń mobilnych.

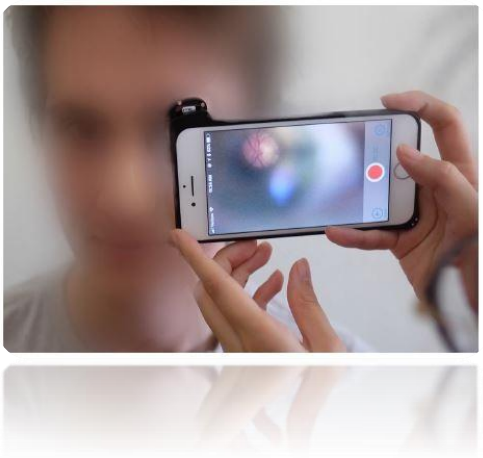
Zasady bezpieczenej pracy zdalnej



- **Pracę zdalną można wykonywać na podstawie wniosku** o udzielenie dostępu zdalnego (numer zatwierdzonego druku-D-370).
- **Nie należy podłączać się do otwartych sieci Wi-Fi, podłączenie do sieci LAN WSS5 odbywa się za pośrednictwem VPN.**
- Należy pracować w miejscach **nie powodujących ryzyka wglądu do przetwarzanych danych lub stosować nakładki prywatyzujące**.
- Nie należy wykonywać pracy zdalnej w miejscach, w których występuje ryzyko uszkodzenie sprzętu służbowego.
- Korzystając z prywatnego sprzętu, należy upwenić się, że dostęp do systemu jest szyfrowany, a połączenie odbywa się przy użyciu VPN.
- Korzystając z prywatnego sprzętu należy pamiętać, aby posiadać zainstalowane oprogramowanie antywirusowe, które jest regularnie aktualizowane oraz posiadać skonfigurowany firewall.
- Nie należy zostawiać sprzętu w miejscach widocznych (np. na siedzeniu w aucie), gdyż powoduje to ryzyko kradzieży.
- Nie należy używać komputera służbowego do grania, czy oglądania filmów.
- Należy zamykać komputer po zakończonej pracy (pamiętaj o “zamykaniu” nie “usypianiu” czy “hibernowaniu”).
- Należy blokować dostęp do systemu po każdym odejściu od komputera (**skrót klawiaturowy Win + L**).
- Nie należy udostępniać służbowego sprzętu osobom trzecim (np. żonie, dzieciom, innym osobom).

Urządzenia przenośne stanowią wrażliwy punkt w systemie bezpieczeństwa informacji, gdyż bardzo często nośniki pendrive, płyty CD, czy dyski zewnętrzne nie są w żaden sposób zaszyfrowane oraz niejednokrotnie są pozostawiane w miejscach, do których dostęp mają osoby nieupoważnione do przetwarzania zawartości zapisanej na wskazanych nośnikach.

Zasady bezpiecznego korzystania ze smartfonów służbowych



- Pamiętaj, aby służbowy smartfon zawsze miał ustawiony kod PIN.
- Smartfon powinien posiadać zainstalowane oprogramowanie antywirusowe.
- Nie korzystaj z Internetu w celach innych niż służbowe. Nie narażaj w ten sposób smartfona na działanie szkodliwego oprogramowania.

Obowiązki użytkowników przenośnych nośników danych

- Masz obowiązek zapobiegania fizycznej kradzieży urządzenia – zabrania się pozostawiania urządzeń mobilnych w miejscach publicznych bez opieki.
- Masz obowiązek blokować dostęp do systemu przy każdorazowym oddaleniu się od niego.
- Masz obowiązek ustawiania ekranu w sposób uniemożliwiający odczyt osobom postronnym w miejscy publicznym lub publicznym środku transportu.
- Nie masz prawa dokonywać samodzielnie napraw i modernizacji sprzętu komputerowego, a także ingerowania w oprogramowanie i ustawienia systemu operacyjnego bez zgody pracowników Obszaru Zarzadzania Informacją.
- Minimum raz w miesiącu masz obowiązek dokonania aktualizacji systemu operacyjnego.