CYBERBEZPIECZEŃSTWO
broszura informacyjna

Krajowe Centrum Monitorowania Ratownictwa Medycznego

Dobre praktyki pozwalające na zwiększenie poziomu bezpieczeństwa danych i informacji w miejscu pracy

Zasada czystego biurka - polega na przechowywaniu dokumentów poza zasięgiem wzroku i dłoni osób postronnych oraz niepozostawianiu dokumentów bez nadzoru. Na biurku należy przechowywać wyłącznie to, co w danym momencie jest nam niezbędne do pracy. Wspomniana zasada obejmuję również przestrzeń wokół tj.; ladę, szafki, półki czy tablice korkowe.

Zasada czystego ekranu – polega na uniemożliwieniu osobom nieupoważnionym wyświetlania zawartości ekranu komputera poprzez odpowiednie ustawienie monitora, stosowanie filtrów prywatyzujących, ustawienie automatycznego wygaszacza ekranu oraz każdorazowe blokowanie komputera po odejściu od stanowiska. Nie należy pozostawiać przyklejonych kartek z hasłami dostępu na monitorze komputera czy na biurku.

Zasada czystego wydruku – polega na zabraniu z urządzeń drukujących dokumentów zaraz po ich wydrukowaniu, skserowaniu bądź zeskanowaniu. Pamiętaj, aby po użyciu skanera usunąć plik z folderu sieciowego.

Zasada czystego kosza – polega na zniszczeniu dokumentów, na których znajdują się informacje wrażliwe bądź poufne, w taki sposób, aby ich odczytanie było niemożliwe. W tym celu najlepszym rozwiązaniem jest użycie niszczarki. Nie należy wyrzucać dokumentów do kosza znajdującego się obok biurka w celu uniknięcia dostępu osób nieupoważnionych do dokumentów.

Bezpieczne hasło – porady i wskazówki

Hasła to powszechnie wykorzystywany i znany sposób chronienia dostępu do poufnych danych i usług. Aby działały skutecznie, muszą być tworzone i stosowane w sposób prawidłowy, w tym dostosowany do aktualnych wymogów technicznych i organizacyjnych. Używanie silnych haseł jest niezbędne do ochrony Twojej tożsamości oraz informacji.

Zasady tworzenia i używania haseł

Podczas tworzenia hasła zastosuj poniższe reguły:

1. Hasło powinno składać się z co najmniej 12 znaków

2. Hasło nie powinno:

- Zawierać powszechnie używanych słów, oczywistych wyrażeń czy przewidywalnych członów;
- Być takie samo jak nazwa użytkownika lub część tej nazwy;
- Zawierać informacji o użytkowniku lub jego rodzinie np.;. Inicjałów, nazwisk, imion, pseudonimów, dat urodzenia, numeru telefonów, numerów rejestracyjnych pojazdów, nazw ulic.

3. Nie używaj sekwencji kolejnych liter, liczb czy znaków np.;. „abcd", „1234", „Qwerty12"

4. Unikaj znanych cytatów czy powiedzeń, zmodyfikowane będą stanowić silne hasło np.; „Wlazł**Kostek**Na**Mostek**i**Stuka"**

Zasady bezpieczeństwa

1. Twórz za każdym razem unikatowe hasło.
2. Nie zapisuj haseł na kartkach papieru, użyj narzędzia do zarządzania hasłami.
3. Nie używaj tego samego hasła w dwóch witrynach.
4. Nie wpisuj hasła, gdy ktoś patrzy Ci przez ramię.
5. Nie udostępniaj nikomu swoich haseł.
6. Nigdy nie wysyłaj hasła w wiadomości email.
7. Zmień hasło w trybie pilnym, gdy zostanie naruszone.
8. Nie wpisuj hasła na komputerze, który nie należy do Ciebie.

Baza wiedzy

Zrozumienie zagrożeń występujących w cyberprzestrzeni jak i stosowanie skutecznych zabezpieczania się przed tymi zagrożeniami to wiedza niezbędna każdemu użytkownikowi komputera, telefonu komórkowego czy też usług internetowych.
W związku z powyższym zachęcamy do regularnego zapoznawania się z informacjami z zakresu cyberbezpieczeństwa publikowanymi na stronach:

1.Ministerstwa Cyfryzacji https://www.gov.pl/web/cyfryzacja
2.CERT Polska: https://cert.pl
3.CSIRT NASK https://www.nask.pl/pl/dzialalnosc/csirt-nask/3424,CSIRT-NASK