15.03.2023 r. skopiowane ze strony <https://www.vulcan.edu.pl/strona/bezpieczenstwo-systemow-633>

**Bezpieczeństwo systemów**

**Podstawowe zasady bezpieczeństwa rekomendowane do stosowania w trakcie użytkowania systemów VULCAN**

|  |  |
| --- | --- |
| **Dostęp do systemu**  1. Każdy użytkownik systemu otrzymuje i posługuje się indywidualnym, imiennym kontem. Bez względu na sytuację nie należy dopuszczać do tworzenia lub używania kont wspólnych.  2. Informacje o koncie (identyfikator, hasło oraz klucze cyfrowe) przekazywane są użytkownikom w formie zapewniającej poufność. Jeżeli użytkownik podejrzewa naruszenie poufności zobowiązany jest niezwłocznie zgłosić ten fakt przedstawicielowi Administratora danych w Umowie przetwarzania danych lub swojemu Inspektorowi Ochrony Danych.  3. Wraz z informacją o koncie użytkownik w czasie szkolenia zostaje pouczony w zakresie odpowiedzialności za posługiwanie się kontem. Zaleca się, by użytkownik otrzymał kopię spisanych zasad bezpieczeństwa, które powinien stosować.  4. Zaleca się, by każdy użytkownik złożył oświadczenie potwierdzające znajomość zasad bezpieczeństwa i przepisów o ochronie danych osobowych oraz zobowiązanie do ich przestrzegania. Zgodnie z wymogami RODO użytkownik powinien także zobowiązać się do zachowania tajemnicy. Szczegółowe zasady w tym zakresie regulują wewnętrzne procedury Administratora danych.  **Dane dostępowe, w tym hasła**  5. Użytkownik podczas pierwszej sesji pracy z systemem, niezwłocznie po uzyskaniu dostępu do indywidualnego konta powinien dokonać zmiany hasła, chyba że procedura przyznania mu dostępu zapewniała możliwość poufnego wprowadzenia przez użytkownika własnego hasła.  6. Hasła, z którego korzystają użytkownicy powinny cechować się określonym minimalnym poziomem skomplikowania. Wymogi dotyczące długości i poziomu skomplikowania haseł określa Administrator danych. Zaleca się, by hasło składało się co najmniej z 8 znaków oraz zawierało przynajmniej jedną dużą literę, jedną małą literę oraz jedną cyfrę bądź znak specjalny.  7. Zaleca się, by użytkownicy regularnie zmieniali swoje hasła. Administrator danych może określić wymaganą minimalną częstotliwość zmiany haseł.  8. Hasło należy zapamiętać, nie należy go zapisywać. Jeśli istnieje konieczność zapisania hasła, należy przechowywać je w bezpiecznym miejscu, przy czym użytkownik, który zapisuje hasło ponosi wszelkie konsekwencje z faktu jego ujawnienia tą drogą.  9. Obowiązuje bezwzględny zakaz ujawniania haseł osobom trzecim.  10. W przypadku podejrzenia wejścia w posiadanie hasła przez osoby trzecie należy niezwłocznie:  a. podjąć próbę zmiany hasła, b. zgłosić fakt przedstawicielowi Administratora danych w Umowie przetwarzania danych lub swojemu Inspektorowi Ochrony Danych.  11. W przypadku zapomnienia bądź utraty hasła należy skorzystać z opcji odzyskiwania hasła (jeżeli taka jest dostępna w systemie) lub zgłosić się do administratora systemu (w zależności od tego, jakiego systemu problem dotyczy, może być to administrator na poziomie danej jednostki bądź administrator na poziomie jednostki nadrzędnej w stosunku do jednostki, do której przypisany jest użytkownik).  12. Administrator dokonuje zmiany hasła jedynie na osobisty wniosek właściciela konta, po potwierdzeniu jego tożsamości.  **Rozpoczęcie i zakończenie pracy z systemem**  13. Przed rozpoczęciem procedury logowania się do systemu użytkownik powinien sprawdzić stan urządzenia, na którym pracuje, w szczególności pod kątem dokonanych podczas jego nieobecności ewentualnych ingerencji w sprzęt lub oprogramowanie. W przypadku wątpliwości co do bezpieczeństwa logowania nie należy wykonywać tej procedury, tylko zgłosić wątpliwości administratorowi systemu informatycznego.  14. Przed wprowadzeniem danych logowania należy upewnić się, że połączenie z systemem odbywa się kanałem szyfrowanym z wykorzystaniem aktualnego certyfikatu wystawionego przez zaufaną instytucję.  15. Użytkownik wprowadzając hasło powinien mieć pewność, że nie zostanie ono podejrzane przez osoby trzecie.  16. Kończąc lub przerywając pracę z systemem należy się bezwzględnie wylogować. Dotyczy to w szczególności sytuacji, w której użytkownik oddala się od komputera, na którym pracował.  **Sprzęt i system operacyjny**  17. System operacyjny komputerów, za pomocą których użytkownicy korzystają z systemu powinien być na bieżąco aktualizowany o wszystkie poprawki dotyczące bezpieczeństwa udostępniane przez producenta systemu operacyjnego.  18. Korzystanie z systemu powinno odbywać się za pomocą jednej z rekomendowanych przeglądarek internetowych. Użytkownik powinien korzystać z najnowszej, oficjalnej wersji danej przeglądarki.  19. Należy upewnić się, że przeglądarka internetowa jest skonfigurowana w taki sposób, by nie zapisywała wprowadzanych haseł dostępu do systemu.  20. Komputery, za pomocą których użytkownicy korzystają z systemu powinny być chronione za pomocą oprogramowania antywirusowego.  21. Komputery, za pomocą których użytkownicy korzystają z systemu powinny być chronione systemem firewall.  22. Pobierając dane z systemu w formie plików użytkownik powinien zapisywać je w miejscach przeznaczonych do przechowywania danych osobowych.  23. Zaleca się, aby nie instalować na komputerze oprogramowania z nieznanych źródeł.  24. Zaleca się, aby dane przechowywane na nośnikach mobilnych były szyfrowane. |  |