Instrukcja obsługi dotycząca szyfrowania danych

UWAGA!!!!

Przed dokonywaniem szyfrowania dysku, prosimy o skopiowanie ważnych danych na nośnik zewnętrzny (pendrive, dysk zewnętrzny).

Szyfrowanie grozi utratą danych.

1. Jak sprawdzić wersję Windows

Aby dowiedzieć się, która wersja systemu Windows jest zainstalowana na komputerze, naciśnij klawisze **klawisz logo Windows** + **R**, z klawiatury wpisz **winver**, a następnie wybierz **OK**/naciśnij **ENTER**. W nowo otwartym oknie znajdziesz wszystkie informacje dotyczące aktualnie zainstalowanego systemu Windows.

Jeśli na twojej klawiaturze nie ma **klawisza logo Windows** kliknij myszką w ikonę Windows znajdującą się na pasku zadań skrajnie po lewej stronie, z klawiatury wpisz **winver**, a następnie wybierz **OK**/naciśnij **ENTER.** W nowo otwartym oknie znajdziesz wszystkie informacje dotyczące aktualnie zainstalowanego systemu Windows.

2. Instrukcja dla Windows 7,8 i 10

Windows 7,8 i 10 (z pominięciem wersji Professional) nie posiadają wbudowanego narzędzia do szyfrowania danych. Z tego powodu skorzystamy z oprogramowania VeraCrypt.

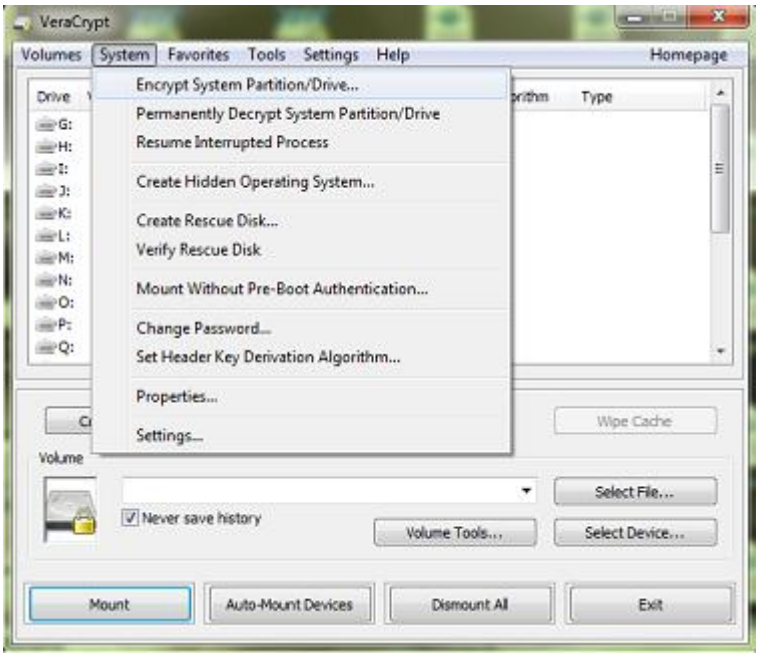
2.1 Instalacja VeraCrypt :

1. Aplikację pobieramy wchodząc na stronę : **https://sourceforge.net/projects/veracrypt/** i następnie klikając w zieloną ikonę z napisem **DOWNLOAD.** Rozpocznie się pobieranie i zapisywanie pliku instalacyjnego **VeraCrypt Setup.exe**
2. Uruchamiamy zapisany plik i postępujemy zgodnie z sugerowanymi opcjami instalacji (akceptujemy licencję, akceptujemy miejsce instalacji oraz utworzenie skrótu na pulpicie ostatecznie klikając **Install**).

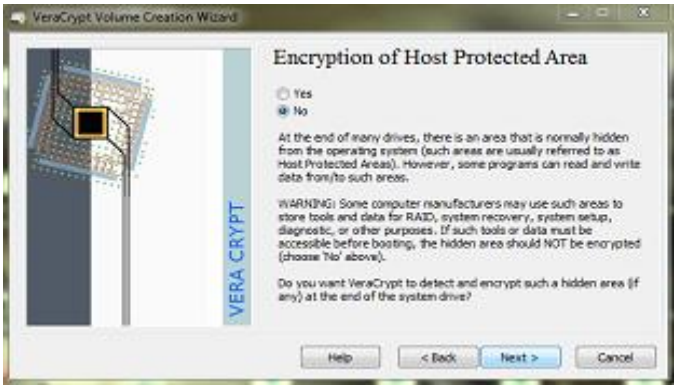
2.2 Instrukcja szyfrowania partycji systemowej :

1. Uruchamiamy program VeraCrypt (po instalacji skrót powinien znajdować się na pulpicie 

).
2. Po uruchomieniu programu VeraCrypt, z górnego menu wybieramy System a następnie Encrypt System Partition/Drive.



3. W kolejnym okienku pojawią się dwa tryby szyfrowania: Normal i Hidden. Wybieramy **Normal** i klikamy Next
4. W kolejnym okienku decydujemy o obszarze do zaszyfrowania. Wybieramy opcję **„Encrypt the whole drive”.**
5. Kolejne okno pozwala użytkownikowi zdecydować, czy dodatkowo zaszyfrować tzw Host Protected Area – wybieramy opcję **NO** jak na poniższym obrazie i klikamy Next



6. Teraz wybieramy, ile systemów operacyjnych chcemy objąć szyfrowaniem. Jeśli mamy tylko jeden system np. Windows 7, zaznaczamy **Single-boot**, jeśli więcej niż jeden – zaznaczamy **Multi-Boot** i klikamy Next.

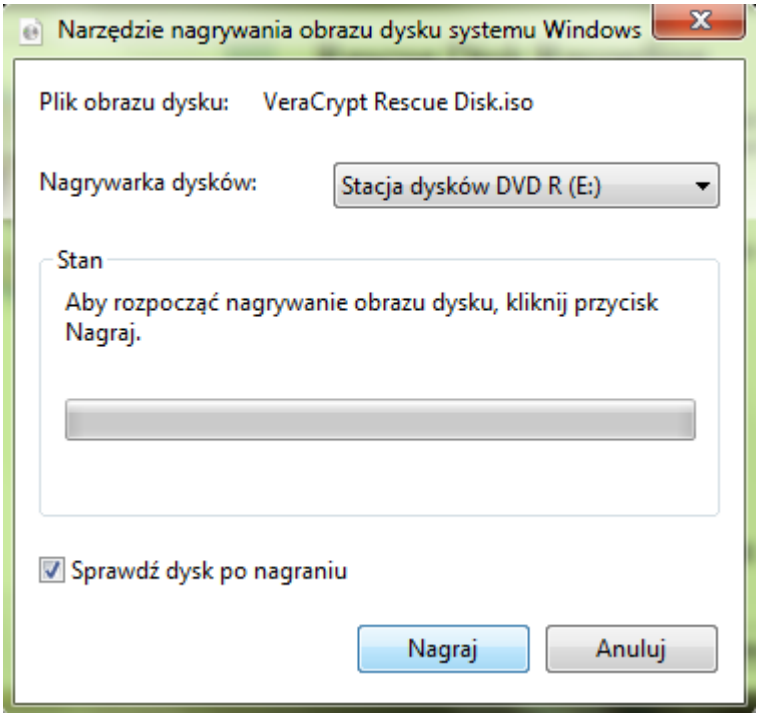
7. W kolejnym oknie decydujemy, jaki kod szyfrujący zastosujemy. Domyślnie ustawiony jest algorytm **AES** oraz poniżej **SHA-256** – jest to bardzo solidny algorytm szyfrujący zatem zostawiamy ustawienia domyślne i klikamy Next.

8. Teraz musimy ustalić hasło. Pamiętajmy, aby hasło było trudne. Autorzy VeraCrypt radzą używać min. 20-sto znakowych haseł z kombinacją dużych i małych liter, cyfr oraz znaków specjalnych (np. $%^). Po wprowadzeniu hasła klikamy Next

9. W kolejnym kroku powinno pojawić się okienko z ciągiem kombinacji liter i cyfr. Im szybciej poruszamy myszką, tym szybciej ciągi literowo-cyfrowe zmieniają się. Chodzi o wzmocnienie siły klucza szyfrującego, dzięki czemu trudniej będzie go złamać. Poruszamy więc energicznie myszką przez kilka, kilkadziesiąt sekund i klikamy Next

10. Kolejne okno to potwierdzenie wygenerowania klucza szyfrującego – klikamy Next

11. Następnym krokiem jest przygotowanie dysku ratunkowego. Proszę przygotować zupełnie pustą płytę. Nośnik będzie zabezpieczeniem na wypadek, gdyby coś poszło nie tak. Po włożeniu czystej płyty do stacji dysku klikamy Next. Następnie pojawi się komunikat o nagrywaniu. Zaznaczamy opcję „**Sprawdź dysk po nagraniu”** aby mieć pewność, że wszystko poszło tak, jak powinno. Następnie klikamy „Nagraj” (jak na obrazie poniżej)



Po wszystkim pojawi się komunikat o prawidłowym nagraniu danych. Klikamy Next

UWAGA – w przypadku braku napędu CD/DVD w laptopie, w oknie „Płyta ratunkowa” zaznaczamy opcję „Pomiń weryfikację dysku ratunkowego” i klikamy NEXT

12. Kolejnym oknem jest sekcja Wipe Mode (tryb wymazywania) – wybieramy domyślną funkcję **NONE** i klikamy Next

13. Ostatnia sekcja to tzw. **System Encryption Pretest.** Wykonujemy go, aby upewnić się, że wszystko jest OK. Aby wykonać taki test, klikamy przycisk **TEST.** System poprosi o zrestartowanie komputera, co oczywiście wykonujemy.

14. Jeśli poprzednie kroki wykonaliśmy poprawnie, w trakcie ładowania systemu, komputer zapyta nas (jeszcze na czarnym tle) o hasło ustalone w punkcie 8. Dodatkowo zapyta nas o tzw PIM (tutaj wciskamy po prostu **ENTER**)

15. Po zrestartowaniu systemu otrzymamy komunikat o pozytywnym wyniku Pretestu. Od teraz za każdym razem, gdy będziemy uruchamiać komputer, system wymusi wprowadzenie hasła (ustalane w punkcie 8) aby system rozpoczął ładowanie.

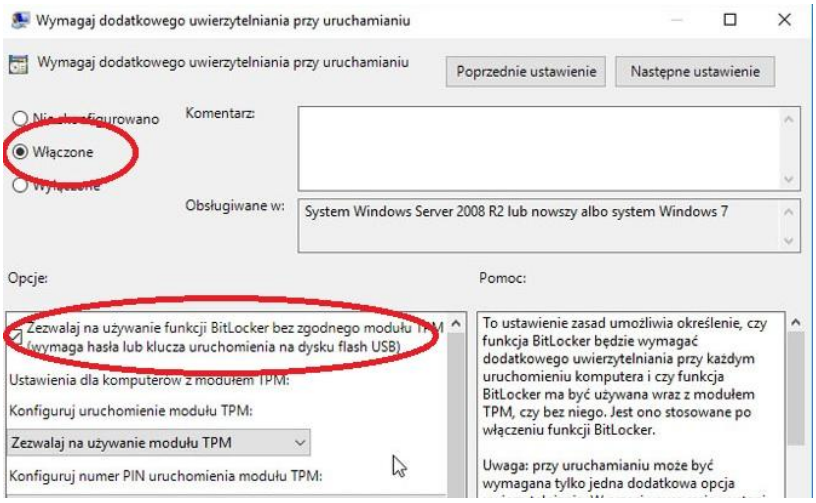
UWAGA – w przypadku niepoprawnego przebiegu Pretestu zostaniemy poinformowani komunikatem „Pretest Fail" – w takim przypadku prosimy o skontaktowanie się z Centrum Informatycznym ponieważ najprawdopodobniej jest to spowodowane zablokowaniem przez Bios możliwości dokonywania zmian rozruchowych – szczególnie często spotykane w laptopach firmy DELL.

16. W oknie potwierdzającym pozytywny wynik Pretestu klikamy Encrypt i rozpocznie się szyfrowanie danych. Może potrwać od kilku do kilkunastu godzin. Zalecane jest nie przerywanie szyfrowania oraz utrzymywanie komputera na stałym zasilaniu sieciowym. Po zakończeniu szyfrowania zostaniemy poinformowani komunikatem.

3. Instrukcja dla Windows 10

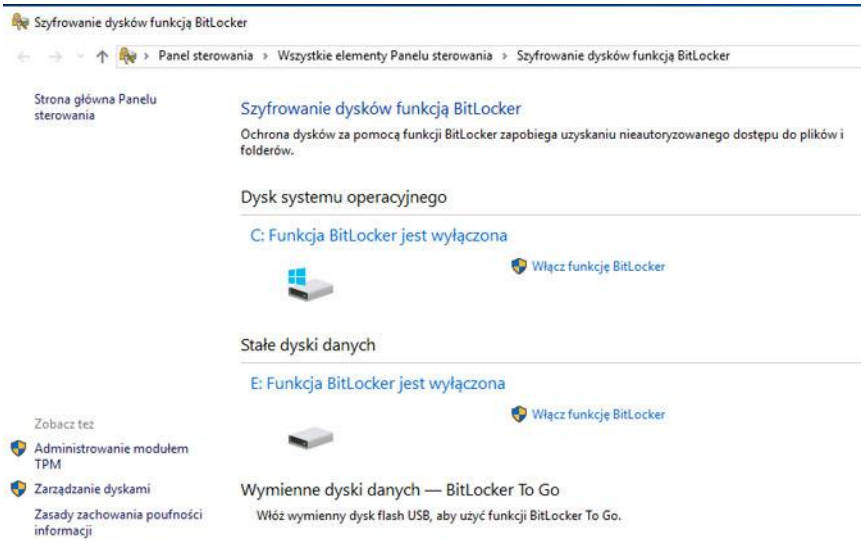
Najnowsza edycja Windows 10 PRO (Professional) posiada wbudowane narzędzie do szyfrowania danych BitLocker dzięki czemu unikamy konieczności instalacji dodatkowego oprogramowania. Szyfrowanie i odszyfrowanie odbywa się w najniższej możliwej warstwie, przez co mechanizm jest praktycznie niewidzialny dla systemu i aplikacji.

KONIECZNIE!! ZANIM PRZYSTĄPIMY DO SZYFROWANIA ustalamy zasady uwierzytelniania przy uruchomieniu. W tym celu w polu wyszukiwania Windows wpisujemy „Edytuj zasady grupy" i uruchamiamy ten aplet. W nowo otwartym oknie nawigujemy kolejno : Konfiguracja komputera -> Szablony administracyjne -> Składniki systemu Windows -> Szyfrowanie dysków funkcją BitLocker -> Dyski z systemem operacyjnym. Wybieramy z prawej strony „Wymagaj dodatkowego uwierzytelniania przy uruchamianiu". W nowo otwartym oknie musimy zaznaczyć **Włączone** i **Zezwalaj na używanie funkcji BitLocker bez zgodnego modułu TPM**



SZYFROWANIE :

1. W polu wyszukiwania Windows (lupka na dolnym pasku zadań) wpisujemy frazę BitLocker i klikamy na znaleziony element **„Zarządzaj funkcją BitLocker"**
2. Teraz przy partycji, którą chcemy zaszyfrować, klikamy na **„Włącz funkcję BitLocker"**

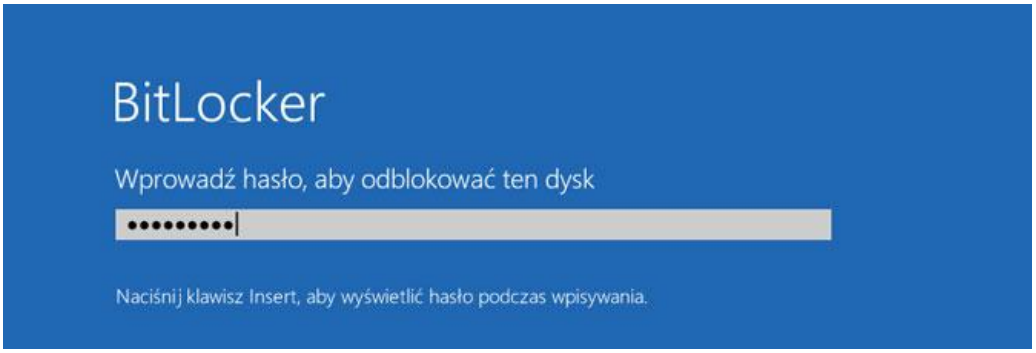


UWAGA - Jeśli będziemy chcieli zaszyfrować partycję systemową, może pojawić się informacja o braku modułu TPM. W takim przypadku prosimy o skontaktowanie się z Centrum Informatycznym.

3. W nowo otwartym oknie zostaniemy zapytani o metodę odblokowywania dysku podczas uruchamiania. Wybieramy „Wprowadź numer PIN (zalecane)". PIN to szereg zawierający od 6 do max 20 cyfr.

   UWAGA – Po zaszyfrowaniu danych, komputer każdorazowo przy logowaniu będzie wymagał podania PIN'u. Prosimy PIN zapamiętać i dodatkowo zapisać i przetrzymywać w bezpiecznym miejscu!!

4. W kolejnym oknie zostaniemy zapytani w jaki sposób chcemy wykonać kopię zapasową klucza odzyskiwania. **Jest to szczególnie ważny klucz który prosimy przechowywać w bezpiecznym miejscu! W przypadku uszkodzenia laptopa, tylko posiadając ten klucz, możliwe będzie odzyskanie danych z dysku!**
   Polecamy „drukuj klucz odzyskiwania" i przechowywanie wydruku
5. Kolejny krok to wybór części dysku do zaszyfrowania – wybieramy „Zaszyfruj cały dysk" i klikamy Dalej
6. W kolejnym kroku system poprosi nas o wybór sposobu szyfrowania. Pierwsza (**Zaszyfruj tylko zajęte miejsce na dysku**) przeznaczona jest dla nowo zainstalowanych systemów. Druga (**Zaszyfruj cały dysk**) dla systemów, które już pracowały dłuższy czas. Polecamy Zaszyfruj cały dysk
7. W kolejnym kroku rozpoczynamy szyfrowanie klikając przycisk „Rozpocznij".
   Zanim rozpoczniemy szyfrowanie jest możliwość przeprowadzenia testu zaznaczając odpowiednią opcję.
8. Jeśli wszystko zrobiliśmy dobrze, podczas uruchamiania komputera, od razu po ekranie BIOS-u powinien pojawić się ekran z prośbą o podanie PIN Bitlocker



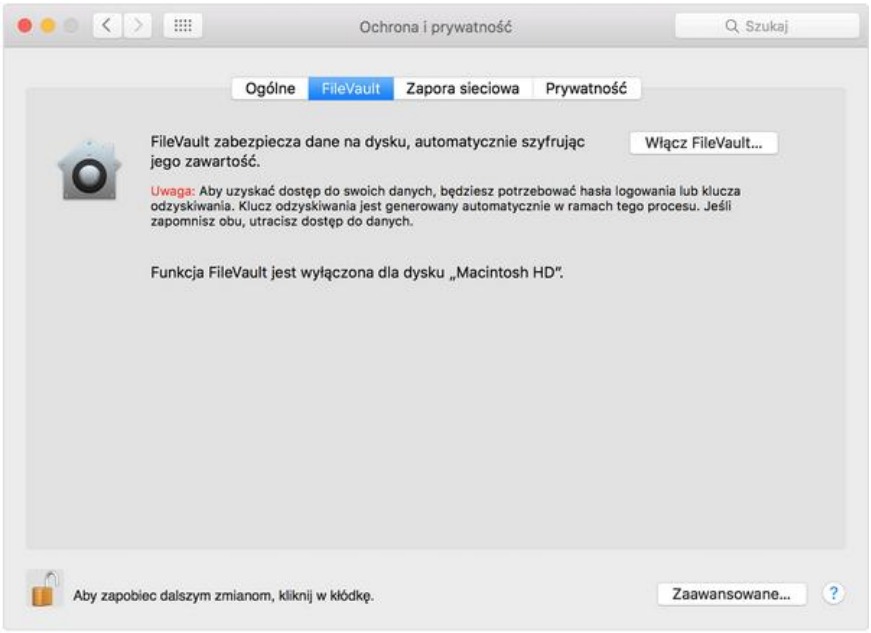
Oznacza to, że nasza partycja systemowa jest zabezpieczona i nikt niepowołany nie uzyska do niej dostępu.

UWAGA : Czas szyfrowania może okazać się długi. Nie można w tym czasie wyłączyć ani restartować komputera. Szyfrowanie jest czynnością jednorazową i musi wykonać się w całości!

4. Instrukcja dla MAC OS

W przypadku komputerów z grupy Apple MAC, możemy skorzystać z wbudowanej funkcji FileVault.

1. Wybierz kolejno opcje menu Apple > Preferencje systemowe, a następnie kliknij opcję Ochrona i prywatność.
2. Klikamy kartę FileVault
3. Klikamy opcję (dolny lewy róg karty) , a następnie podajemy nazwę administratora i hasło.
4. Klikamy opcję **Włącz funkcję FileVault**



5. W kolejnej karcie wybieramy sposób odblokowania dysku i resetowania hasła. Proponujemy skorzystać z funkcji „utwórz klucz odzyskiwania". Wygenerowany klucz zostanie wyświetlony na ekranie. **WAŻNE** – wygenerowany klucz przechowujemy na innym nośniku niż zaszyfrowany dysk lub drukujemy go i przechowujemy w bezpiecznym miejscu. Tylko na podstawie tego klucza możliwe będzie odzyskanie danych z ewentualnie uszkodzonego laptopa.

   JEŚLI ZGUBISZ KLUCZ ODZYSKIWANIA FileVault, NIE BĘDZIE MOŻLIWOŚCI UZYSKAĆ DOSTĘPU DO DANYCH NA ZASZYFROWANYM DYSKU

6. Szyfrowanie następuje w tle podczas korzystania z komputera Mac, gdy jest on wybudzony i podłączony do zasilania. Możemy sprawdzić postęp w sekcji funkcji FileVault w preferencjach opcji Ochrona i prywatność. Wszystkie nowo utworzone pliki są automatycznie szyfrowane w momencie zachowania ich na dysku startowym.
7. Po ukończeniu konfiguracji funkcji FileVault wymagane będzie logowanie przy pomocy hasła przy każdym uruchomieniu komputera Mac. Nie będzie możliwe logowanie automatyczne.

8. Jeśli zgubisz klucz odzyskiwania lecz nadal pamiętasz hasło logowania, wyłącz funkcję FileVault w preferencjach opcji Ochrona i prywatność. Następnie włącz ją ponownie aby wygenerować nowy klucz i dezaktywować wszystkie stare klucze.