Regulamin Ochrony Danych Osobowych

w Zespole Szkół Ponadpodstawowych nr 3 im. Jana Pawła II

ul. Zdunowska 81

63-700 Krotoszyn

Zawartość

1. DEFINICJE

1.1. **ADO** - Administrator Danych Osobowych

Zespół Szkół Ponadpodstawowych nr 3

Jana Pawła II

w Krotoszynie, reprezentowany przez Panią dyrektor Izabelę Kossakowską;

1.2. **ASI** – Administrator Systemu Informatycznego;

1.3. **Dane osobowe** – informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej w rozumieniu Art. 4 ust. 1. RODO, umożliwiające zidentyfikowanie, pośrednio lub bezpośrednio osoby fizycznej, której one dotyczą. Osobą możliwą do zidentyfikowania jest osoba fizyczna, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak:

- imię i nazwisko,
- numer identyfikacyjny (login),
- dane o lokalizacji,
- identyfikator internetowy,
- jeden bądź kilka szczególnych czynników określających: fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;

1.4. **Hasło** – ciąg znaków cyfrowych, literowych i specjalnych, znany jedynie upoważnionemu użytkownikowi, będący zgodny z polityką haseł ADO;

1.5. **Identyfikator użytkownika (login)** – nadawany indywidualnie ciąg znaków literowych, cyfrowych i specjalnych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych w systemie informatycznym;

1.6. **Poufność danych** - własność zapewniająca, że dane nie są udostępniane osobom i podmiotom do tego celu nieupoważnionym;

1.7. **Przetwarzanie danych osobowych** – zgodnie z Art. 4 ust. 2 RODO oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;

1.8. **RODO** - rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych;

1.9. **System** – oznacza przekazany Użytkownikowi przez ADO / ASI system informatyczny na podstawie upoważnienia;

1.10. **Usuwanie danych** – unicestwienie danych lub ich modyfikacja po której nie można zapoznać się z informacją;

1.11. **Uwierzytelnianie** - pozwala na zweryfikowanie tożsamości użytkownika;

1.12. **Użytkownik** – posiada upoważnienie do przetwarzania danych w postaci papierowej, w systemie informatycznym, unikalny identyfikator oraz hasło;

2. OŚWIADCZENIE STRON

2.1. Niniejszy dokument określa zasady udostępniania Użytkownikowi przez ADO Systemu stosowanego do pracy w placówce oświatowej.

3. KORZYSTANIE Z SYSTEMU

3.1. ADO powierza Użytkownikowi dane osobowe celem przetwarzania ich zgodnie z prawem i niniejszym dokumentem.

3.2. ADO udostępnia Użytkownikowi System wraz z normą jego stosowania do właściwego wykonywania zadań lub czynności wykonywanych na rzecz ADO. Użytkownik zobowiązuje się do korzystania z Systemu zgodnie z określonymi zasadami.

3.3. Niewłaściwe korzystanie przez Użytkownika z Systemu przez wprowadzanie błędnych lub niekompletnych danych może stanowić naruszenie obowiązków pracowniczych lub zasad współpracy, co będzie niosło za sobą dalsze konsekwencje.

3.4. Użytkownik zobowiązują się korzystać z Systemu wyłącznie do celów dla niego przeznaczonych oraz nie udostępniać go osobom nieupoważnionym.

4. DOSTĘP DO SYSTEMU

4.1. System jest udostępniony Użytkownikowi przez ADO/ASI na czas współpracy.

4.2. Dla zapewnienia bezpieczeństwa Danych Osobowych, ADO/ASI udostępnia Użytkownikowi system przez nadanie loginów i haseł mając na celu uwierzytelnienie użytkownika Systemu.

4.3. Użytkownik zobowiązuje się do nieudostępniania swoich loginów i haseł innym osobom.

4.4. W przypadku rozwiązania współpracy, Użytkownikowi zostaje odebrany dostęp do Systemu, w tym zablokowane będą dane uwierzytelniające.

4.5. Użytkownik ponosi pełną odpowiedzialność za wszystkie działania wykonywane w Systemie po zalogowaniu się do niego za pomocą indywidualnego loginu oraz hasła.

4.6. Zarządzanie uprawnieniami oraz polityka haseł ADO, które Użytkownik zobowiązuje się przestrzegać, zostały zawarte w Regulaminie Ochrony Danych Osobowych

4.7. W przypadku kradzieży hasła lub jego zgubienia albo ujawnienia osobie niepowołanej, UŻYTKOWNIK zobowiązany jest do bezzwłocznej zmiany hasła i powiadomienia ADO/ASI maksymalnie w ciągu 24 godzin od momentu zdarzenia.

5. OCHRONA DANYCH OSOBOWYCH

5.1. Powierzenie przez ADO Danych Osobowych obejmuje również ich przetwarzanie w Systemie. Użytkownik zobowiązuje się do zachowania należytych zasad bezpieczeństwa powierzonych danych oraz zapewnienie im ochrony w myśl obowiązujących przepisów i wspólnych ustaleń popartych odpowiednimi dokumentami w tym Regulaminem Ochrony Danych Osobowych obowiązującym u ADO .

5.2. Użytkownik zobowiązuje się do zachowania zasad bezpieczeństwa właściwego logowania do Systemu zgodnie z zasadami korzystania z Systemu.

6. NADZÓR NAD SYSTEMEM

6.1. ADO ma prawo do nadzoru i kontroli nad Użytkownikiem w zakresie korzystania z Systemu w dowolnym momencie trwania współpracy.

6.2. Każda operacja Użytkownika na danych osobowych jest rejestrowana.

6.3. Operacje na danych osobowych są monitorowane, a wzmożona aktywność jest w sposób szczególny kontrolowana.

7. ZABEZPIECZENIE DOKUMENTACJI PAPIEROWEJ Z DANYMI OSOBOWYMI

a. Osoby przetwarzające dane osobowe są zobowiązane do stosowania tzw. „**Polityki czystego biurka**”. Polega ona na zabezpieczaniu (zamykaniu) dokumentów np. w szafach, biurkach, pomieszczeniach przed kradzieżą lub wglądem osób nieupoważnionych po godzinach pracy lub podczas ich nieobecności w trakcie godzin pracy,
b. Osoby przetwarzające dane osobowe zobowiązane są do skutecznego niszczenia dokumentów i wydruków np. za pomocą niszczarek ,
c. Zabrania się pozostawiania dokumentów z danymi osobowymi poza zabezpieczonymi pomieszczeniami, np. w korytarzach, na kserokopiarkach, drukarkach,
   w pomieszczeniach konferencyjnych,
d. Zabrania się wyrzucania niezniszczonych dokumentów na śmietnik lub porzucania ich na zewnątrz, np.: na terenach publicznych miejskich lub w lesie.
e. Dane z orzeczeń i opinii Poradni Psychologiczno Pedagogicznej o uczniach mogą przetwarzać: pedagog szkolny, nauczyciele, wychowawcy. Pedagog szkolny może wykonać ksero i wydać je nauczycielom pod rygorem wprowadzenie do „Rejestru wydanych dokumentów szczególnie chronionych(wrażliwych)”.Nauczyciel podpisuje odbiór dokumentu. Od tego momentu nauczyciel jest osobiście odpowiedzialny za zabezpieczenie dokumentacji. Ewidencja jest prowadzona i zabezpieczona przez pedagoga szkolnego.

8. ZASADY BEZPIECZNEGO UŻYTKOWANIA SPRZĘTU IT, DYSKÓW, PROGRAMÓW

a. W przypadku, gdy użytkownik przetwarzający dane osobowe korzysta ze sprzętu IT, zobowiązany jest do jego ochrony przed jakimkolwiek zniszczeniem lub uszkodzeniem. Za sprzęt IT uważa się : komputery stacjonarne, monitory, drukarki, skanery, ksera, laptopy, aparaty telefoniczne, tablety i smartfony używane w celach związanych z wykonywaniem zadań lub czynności związanych z przetwarzaniem danych osobowych.

b. Osoby upoważnione do przetwarzania danych osobowych i pracujące na sprzęcie IT zobowiązane są zapoznać się z zasadami bezpiecznego użytkowania sprzętu IT, dysków, programów i bezwzględnie stosować się do tych zasad.
c. Dostęp do każdego urządzenia musi być zabezpieczony hasłem lub pinem lub zabezpieczeniami biometrycznymi.
d. Dane osobowe muszą być zaszyfrowane na dysku i zabezpieczone co najmniej 8 znakowym hasłem zawierającym co najmniej jedną dużą literę, jedną cyfrę oraz znak specjalny.
e. Użytkownik zobowiązany jest do bieżącej aktualizacji oprogramowania na sprzęcie IT.
f. Na urządzeniu powinien być zainstalowany i regularnie aktualizowany program antywirusowy.
g. Na urządzeniu powinien być zainstalowany legalny system operacyjny.
h. Użytkownik ma obowiązek natychmiast zgłosić zagubienie, utratę lub zniszczenie Sprzętu IT, na którym przetwarzane są dane osobowe do Administratora Danych Osobowych lub Inspektora Ochrony Danych.
i. Jeżeli nie jest to niezbędne, urządzenie nie powinno mieć włączonego modułu GPS, NFC, Wi-Fi i Bluetooth i innych połączeń bezprzewodowych.
j. Zabrania się z korzystania z publicznych, niezabezpieczonych sieci Wi-Fi.
k. Samowolne otwieranie (demontaż) Sprzętu IT, instalowanie dodatkowych urządzeń (np. twardych dysków, pamięci RAM) lub podłączanie jakichkolwiek niezatwierdzonych urządzeń do systemu informatycznego jest zabronione.
l. Użytkownik jest zobowiązany do uniemożliwienia osobom niepowołanym (np., pracownikom innych działów) wglądu do danych osobowych wyświetlanych na monitorach komputerowych – **tzw. Polityka czystego ekranu.**
m. Użytkownik zobowiązany jest do szczególnego zabezpieczenia urządzenia w czasie transportu. Zabrania się pozostawienia urządzeń bez nadzoru w miejscu ogólnie widocznym.
n. Korzystając z urządzeń w miejscach publicznych, użytkownik zobowiązany jest do chronienia wyświetlanych danych osobowych na ekranie przed wglądem osób nieupoważnionych.
o. Przed czasowym opuszczeniem stanowiska pracy, użytkownik zobowiązany jest wywołać blokowany hasłem wygaszacz ekranu (WINDOWS + L) lub wylogować się z systemu bądź z programu.
p. Po zakończeniu pracy użytkownik zobowiązany jest:

✓ wylogować się z systemu informatycznego - następnie wyłączyć sprzęt komputerowy

✓ zabezpieczyć stanowisko pracy, w szczególności wszelkie nośniki magnetyczne
i optyczne, na których znajdują się dane osobowe.

q. Użytkownik jest zobowiązany do usuwania plików z nośników/dysków do których mają dostęp inni użytkownicy nieupoważnieni do dostępu do takich plików (np. podczas współużytkowania komputerów).
r. Jeśli użytkownik jest uprawniony do niszczenia nośników, powinien TRWALE zniszczyć sam nośnik lub trwale usunąć z niego dane osobowe. W innym przypadku nośniki takie przekazujemy do działu IT Administratora Danych Osobowych

9. POLITYKA HASEŁ

a. Hasła powinny składać się z minimum 8 znaków.
b. Hasła powinny zawierać przynajmniej po jednym znaku: dużą literę, mała literę, cyfrę, znak specjalny.
c. Hasła nie mogą być łatwe do odgadnięcia. Nie powinny być powszechnie używanymi słowami. W szczególności nie należy jako haseł wykorzystywać: dat, imion i nazwisk osób bliskich, imion zwierząt, popularnych dat, popularnych słów, typowych zestawów np. : 123456, qwerty.
d. Hasła nie mogą być ujawnianie innym osobom. Nie należy zapisywać haseł na kartkach
i w notesach, nie naklejać na monitorze komputera, nie trzymać pod klawiaturą lub w szufladzie.
e. W przypadku ujawnienia hasła – należy natychmiast je zmienić.
f. Hasła muszą być zmieniane co 30 dni, najlepiej jak wymusza to system operacyjny.
g. Jeżeli system nie wymusza zmiany haseł, użytkownik zobowiązany jest do samodzielnej zmiany hasła.

10. ZARZĄDZANIE UPRAWNIENIAMI

a. Każdy użytkownik z dostępem do danych osobowych (np. na swoim komputerze, na dysku sieciowym, w programie lub aplikacji, w poczcie elektronicznej) musi posiadać swój własny indywidualny identyfikator (login) do logowania się.
b. Użytkownik otrzymuje dostęp i odpowiednie uprawnienia do zasobów i aplikacji na polecenie przełożonych i przy realizacji działu IT.
c. Użytkownicy nie mają prawa do samodzielnej zmiany uprawnień, np. przydzielenia sobie uprawnień administratora w Windows.
d. Użytkowników obowiązuje zasada pracy na własnym koncie. Zabronione jest zatem umożliwianie innym osobom pracy na koncie innego użytkownika.

11. ZASADY WYNOSZENIA NOŚNIKÓW Z DANYMI POZA OBSZAR PRZETWARZANIA DANYCH OSOBOWYCH

a. W przypadku potrzeby wyniesienia poza obszar przetwarzania danych osobowych wymiennych elektronicznych nośników informacji z zapisanymi danymi osobowymi, dane te muszą być zaszyfrowane (szyfrowane dyski, zabezpieczone hasłem pliki).
b. Do takich nośników zalicza się: wymienne twarde dyski, pendrive, płyty CD, DVD, pamięci typu Flash.
c. Nośnikom tym jak również dokumentacji papierowej należy zapewnić bezpieczny transport w plecakach, teczkach chroniących przed zagubieniem i kradzieżą.
d. Przy wysyłce danych w wersji papierowej należy korzystać ze sprawdzonych firm kurierskich i pocztowych.

12. ZASADY KORZYSTANIA Z INTERNETU

a. Na sprzęcie na którym przetwarzane są dane osobowe, użytkownik korzysta z Internetu wyłącznie w celach służbowych.
b. Zabrania się zgrywania na dysk twardy komputera oraz uruchamiania jakichkolwiek programów nielegalnych oraz plików pobranych z niewiadomego źródła. Pliki takie powinny być ściągane tylko za każdorazową zgodą działu IT i tylko w uzasadnionych przypadkach.

c. Użytkownik ponosi odpowiedzialność za szkody spowodowane przez szkodliwe oprogramowanie instalowane przez niego z Internetu.
d. Zabrania się wchodzenia na strony, na których prezentowane są informacje o charakterze przestępczym, hackerskim, pornograficznym, lub innym zakazanym przez prawo (na większości stron tego typu jest zainstalowane szkodliwe oprogramowanie infekujące w sposób automatyczny system operacyjny komputera szkodliwym oprogramowaniem).
e. Nie należy w opcjach przeglądarki internetowej włączać opcji autouzupełniania formularzy i zapamiętywania haseł.
f. W przypadku korzystania z szyfrowanego połączenia przez przeglądarkę, należy zwracać uwagę na pojawienie się odpowiedniej ikonki (kłódka) oraz adresu www rozpoczynającego się frazą ”https:”. Dla pewności należy „kliknąć” na ikonkę kłódki
i sprawdzić, czy właścicielem certyfikatu jest wiarygodny właściciel.
g. Należy zachować szczególną ostrożność w przypadku podejrzanego żądania lub prośby zalogowania się na stronę (np. na stronę banku, portalu społecznościowego, e-sklepu, poczty mailowej) lub podania naszych loginów i haseł, PIN-ów, numerów kart płatniczych przez Internet. Szczególnie tyczy się to żądania podania takich informacji przez rzekomy bank.

13. ZASADY KORZYSTANIA Z POCZTY ELEKTRONICZNEJ SŁUŻBOWEJ

a. Użytkownik do celów służbowych zobowiązany jest wyłącznie do korzystania z adresu e-mail z domeny szkolnej.
b. Zabrania się wykorzystywania innych adresów e-mail (np. wp.pl, onet.pl, gmail.com) do przesyłania poczty służbowej , jak również przekierowywania poczty służbowej na serwery z poza infrastruktury szkolnej.
c. W przypadku przesyłania danych osobowych poza organizację szkolną należy wykorzystywać mechanizmy kryptograficzne (hasłowanie lub szyfrowanie wysyłanych dokumentów lub plików) .
d. W przypadku zabezpieczenia plików hasłem, obowiązuje minimum 8 znaków: duże i małe litery i cyfry lub znaki specjalne, a hasło należy przesłać odrębnym mailem lub inną metodą, np. telefonicznie lub SMS-em .
e. Użytkownicy powinni zwracać szczególną uwagę na poprawność adresu odbiorcy dokumentu.

f. Zaleca się, aby użytkownik podczas przesyłania danych osobowych mailem zawarł w treści prośbę o potwierdzenie otrzymania i zapoznania się z informacją przez adresata.
g. **WAŻNE:** Nie należy otwierać załączników (plików) w mailach nawet od rzekomo znanych nam nadawców bez weryfikacji tegoż nadawcy. Tego typu maile w większości przypadków zawierają załączniki ze szkodliwymi programami, które po „kliknięciu" infekują komputer użytkownika oraz często pozostałe komputery w sieci. W wyniku działania takiego szkodliwego oprogramowania może dojść do poważnych incydentów, łącznie z pełną utratą danych osobowych lub zaszyfrowaniem przez kryptowirusy
h. **WAŻNE:** Bez weryfikacji wiarygodności nadawcy, nie należy „klikać" na hiperlinki w mailach, gdyż mogą to być hiperlinki do stron zainfekowanych lub niebezpiecznych. Użytkownik „klikając" na taki hiperlink bezwiednie infekuje swój komputer oraz często pozostałe komputery w sieci. W wyniku takiej infekcji może dojść do poważnych incydentów, łącznie z pełną utratą danych osobowych lub zaszyfrowaniem przez krypto wirusy.
i. Należy zgłaszać do działu IT (informatyków) przypadki podejrzanych e-maili.
j. Użytkownicy nie powinni rozsyłać „niezawodowych" e-maili w formie „łańcuszków szczęścia", np. życzenia świąteczne adresowane do wielu osób.
k. Podczas wysyłania maili do wielu adresatów jednocześnie, należy użyć metody „Ukryte do wiadomości – UDW". Zabronione jest rozsyłanie maili do wielu adresatów z użyciem opcji „Do wiadomości"!
l. Użytkownicy nie powinni rozsyłać maili zawierających załączniki o dużym rozmiarze (powyżej 50 MB)
m. Użytkownicy powinni okresowo kasować niepotrzebne maile
n. Mail służbowy jest przeznaczony wyłącznie do wykonywania obowiązków służbowych
o. Zakazuje się wysyłania korespondencji służbowej na prywatne skrzynki pocztowe pracowników lub innych nieupoważnionych osób
p. Użytkownicy mają prawo korzystać z poczty mailowej dla celów prywatnych wyłącznie okazjonalnie i powinno być to ograniczone do niezbędnego minimum.
q. Przy korzystaniu z maila, Użytkownicy mają obowiązek przestrzegać prawa własności przemysłowej i prawa autorskiego
r. Użytkownicy nie mają prawa korzystać z maila w celu rozpowszechniania treści o charakterze obraźliwym, niemoralnym lub niestosownym wobec powszechnie obowiązujących zasad postępowania

14. OCHRONA ANTYWIRUSOWA

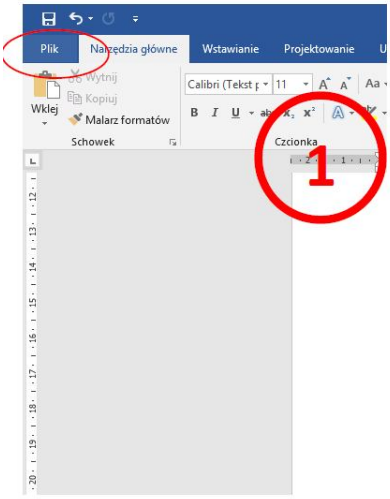
a. Użytkownicy zobowiązani są do systematycznego sprawdzania działania i aktualności programu antywirusowego
b. Każdy przypadek problemu z działaniem programu antywirusowego powinien być zgłaszany do Działu IT
c. Użytkownicy zobowiązani są do skanowania plików wprowadzanych z zewnętrznych nośników programem antywirusowym
d. Zakazane jest wyłączanie systemu antywirusowego podczas pracy systemu informatycznego przetwarzającego dane osobowe
e. W przypadku stwierdzenia zainfekowania systemu lub pojawienia się komunikatów niezrozumiałych lub wzbudzających podejrzenie np.; „Twój system jest zainfekowany!, zainstaluj program antywirusowy" , użytkownik obowiązany jest poinformować niezwłocznie o tym fakcie Dział IT.

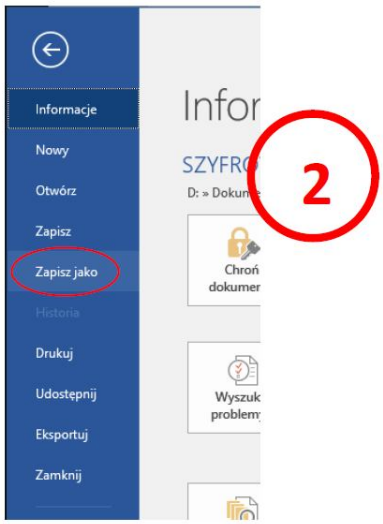
15. INSTRUKCJA SZYFROWANIA I HASŁOWANIA PLIKÓW WYSYŁANYCH DROGĄ MAILOWĄ

W celu zabezpieczenia plików można zastosować:

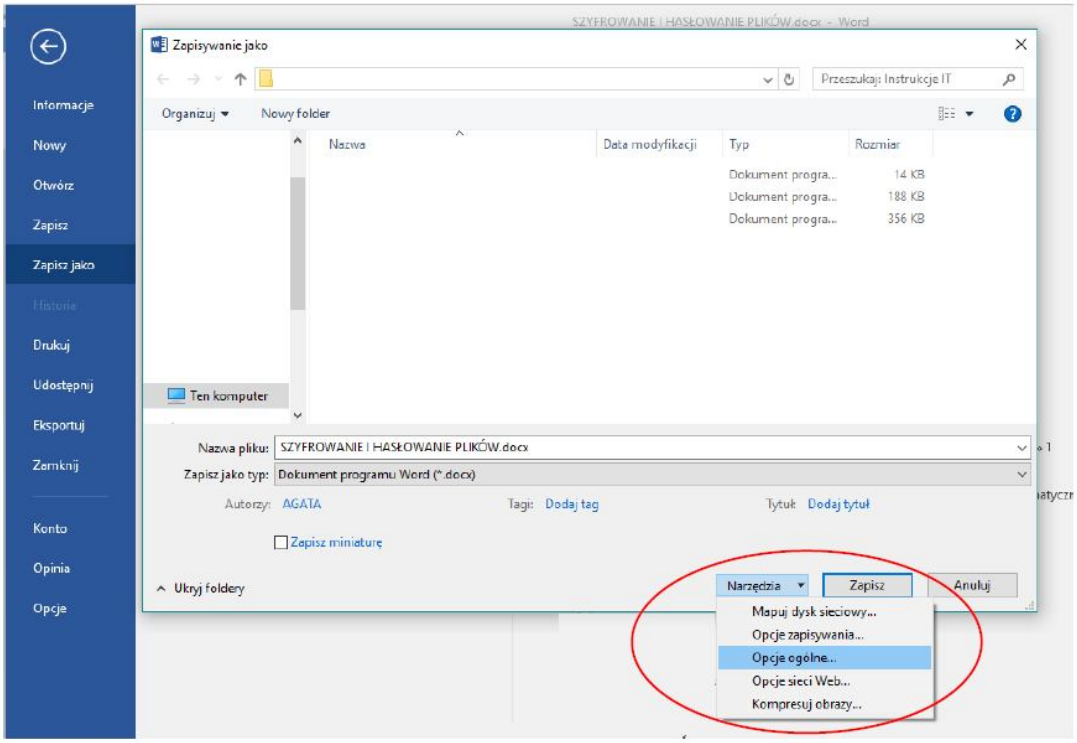
a. Zabezpieczenie hasłem pojedynczych plików pakietu MS OFfcie (Word, Excel,PowerPoint, etc.)

W pierwszym kroku postępujemy tak jak przy standardowym zapisywaniu pliku na dysku. Wybieramy opcję „Plik" i klikamy „Zapisz jako"

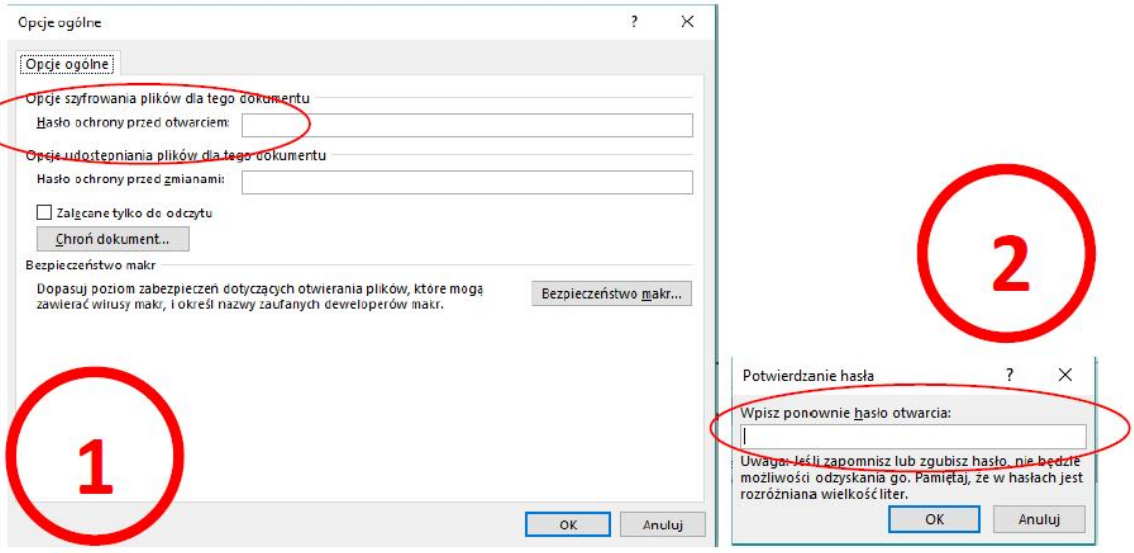




W oknie które się pojawiło rozwijamy listę menu „Narzędzia" i wybieramy „Opcje ogólne".



W odpowiednie miejsce wprowadzamy hasło zabezpieczające plik, a następnie poniżej konieczne jest powtórzenie celem potwierdzenia. Klikamy „OK.”

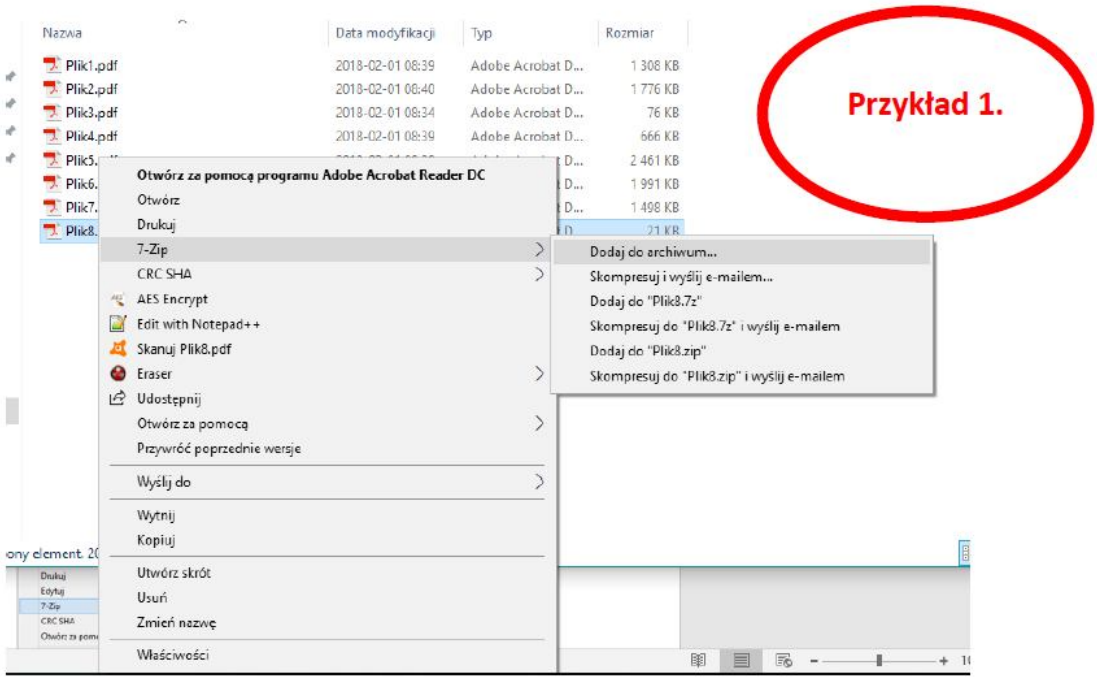


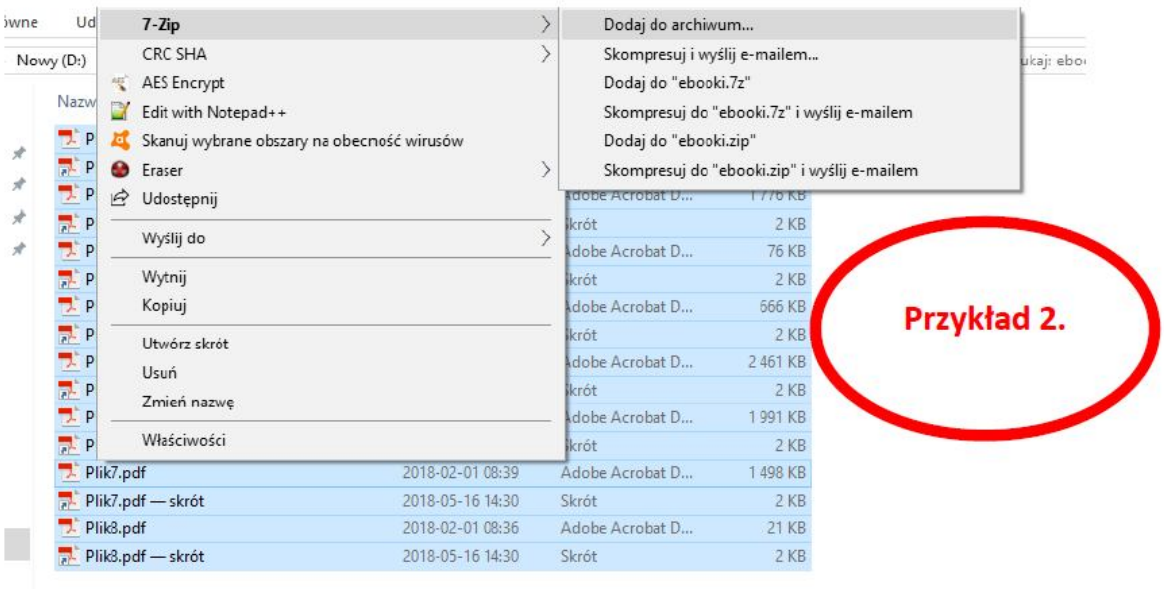
W ostatnim oknie dialogowym wybieramy miejsce zapisania pliku, nadajemy mu nazwę i klikamy „Zapisz”.

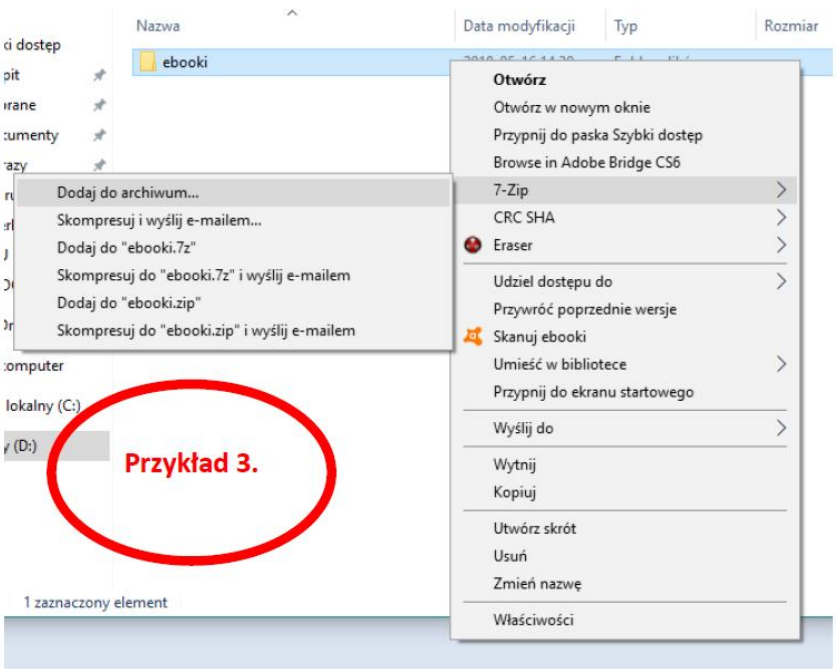
b. Zabezpieczenie hasłem zestawu plików, wysyłanych jako archiwum (tzw. „Spakowane pliki” mające rozszerzenie np. „*.rar. *.zip, *.7z”

W celu zabezpieczenia hasłem większej ilości plików należy zainstalować na swoim komputerze oprogramowanie służące do tworzenia archiwum (kompresowania plików) np. 7-zip (link do pobrania programu: https://www.7-zip.org/

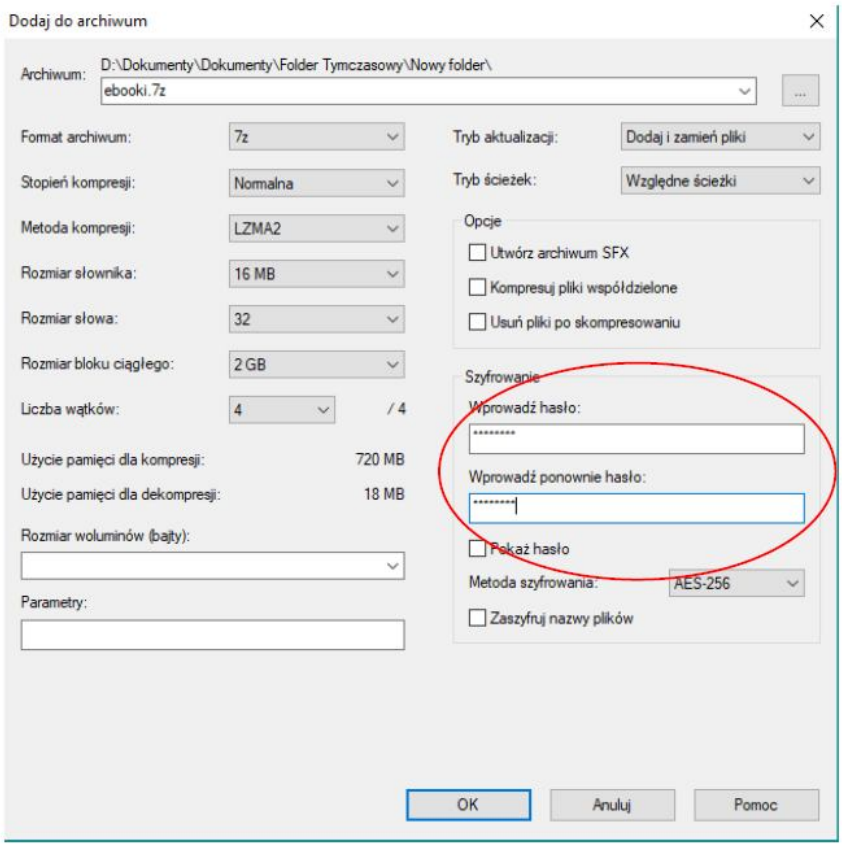
Po zainstalowaniu programu klikamy prawym przyciskiem myszy na grupę plików lub cały katalog i iż dostępnych opcji wybieramy „7-zip” ->”Dodaj do archiwum”







W odpowiednie miejsce wprowadzamy hasło i klikamy „OK.”

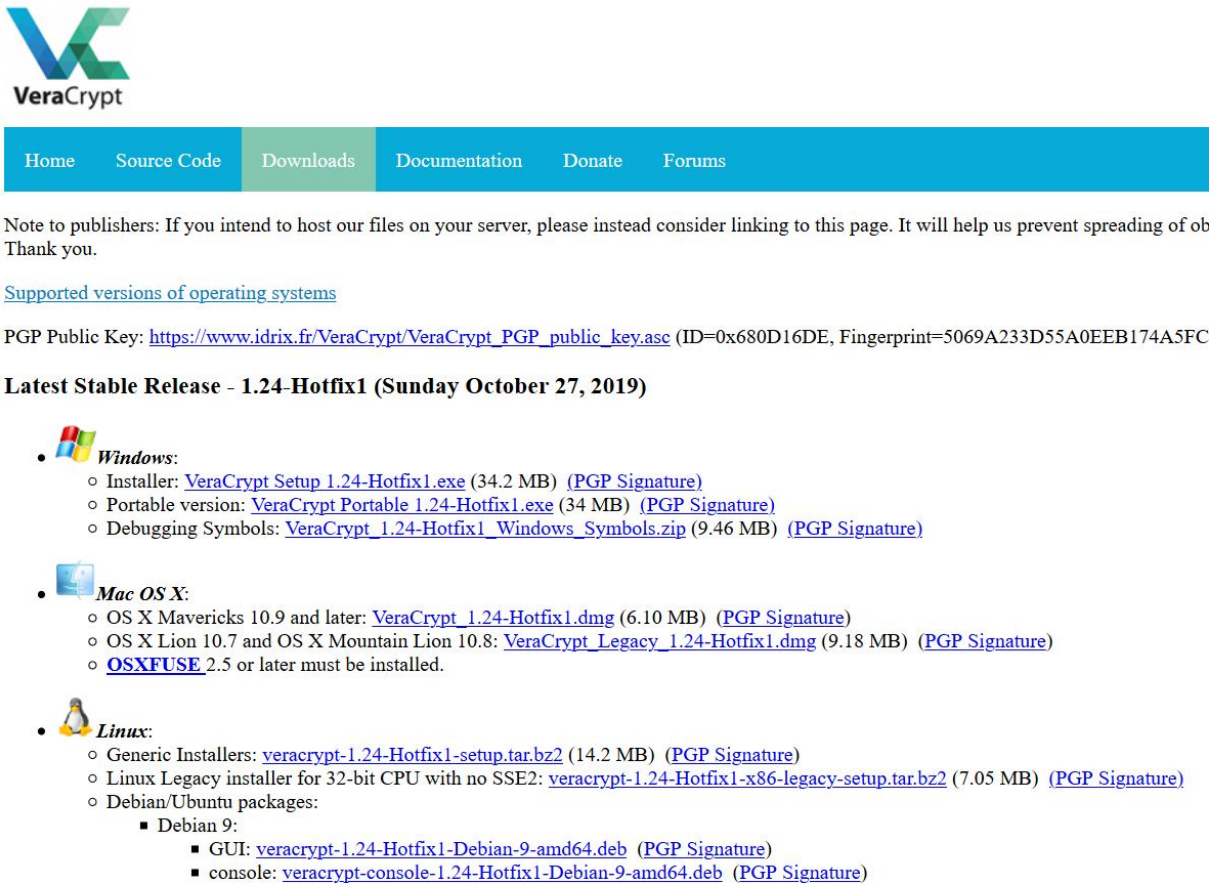


Uwaga!
Aby odbiorca mógł odszyfrować plik musi posiadać odpowiedni program umożliwiający otwarcie archiwum.

16. INSTRUKCJA SZYFROWANIA DYSKU, PAMIĘCI FLASH(PENDRIVE) ZA POMOCĄ DARMOWEGO OPROGRAMOWANIA VERACRYPT

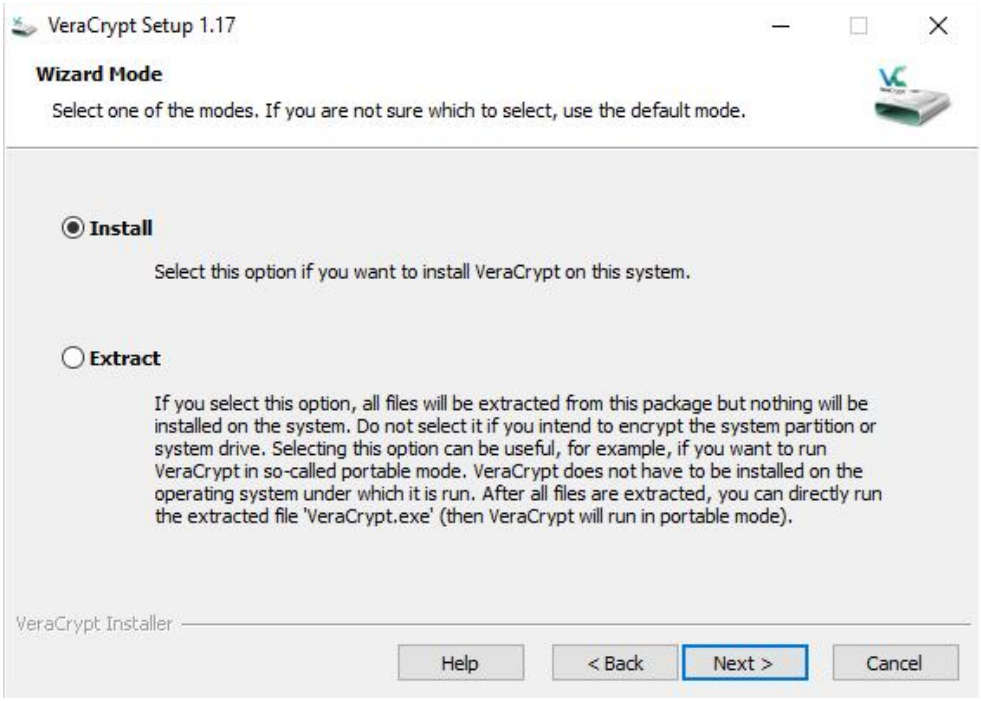
Program pobieramy ze strony producenta: https://www.veracrypt.fr/en/Downloads.html

Wybieramy odpowiednią wersją dla naszego systemu operacyjnego. VeraCrypt dostępny jest na Windowsa, MacOSa oraz Linuxa. Jest to o tyle ważne, że **nie ma potrzeby się przejmować tym z jakiego systemu korzysta osoba, u której będziemy chcieli skorzystać z tego oprogramowania.**



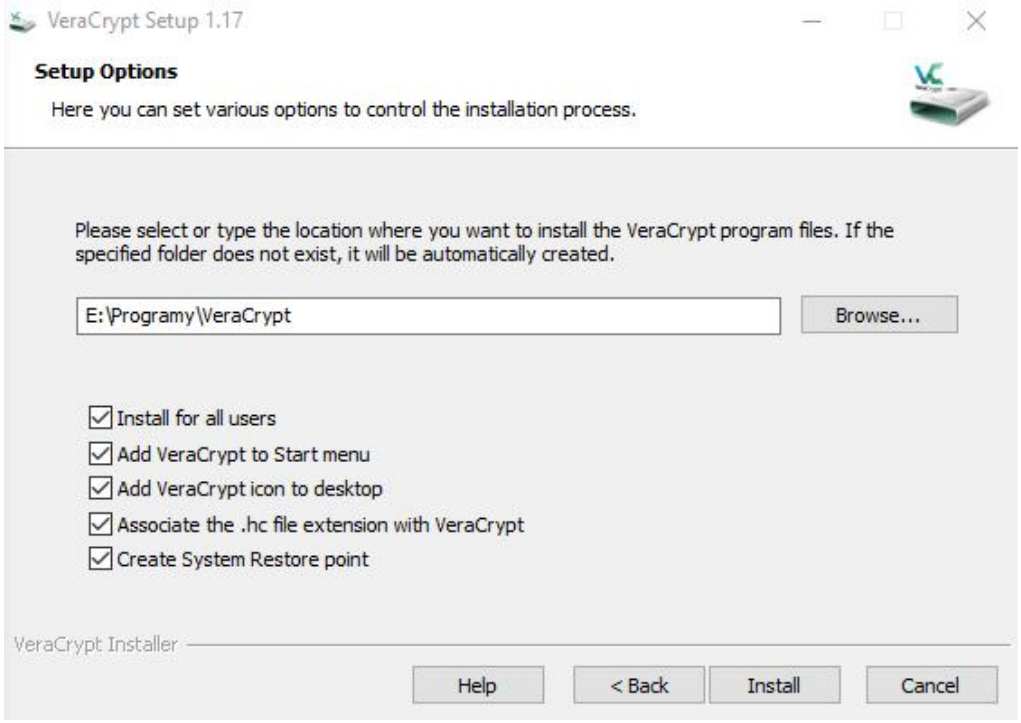
Strona z możliwymi plikami instalacyjnymi VeraCrypt.

Po ściągnięciu pliku instalacyjnego uruchamiamy go. Co ciekawe VeraCrypt daje nam możliwość pełnej instalacji bądź rozpakowania się. Ta druga pozwala na uruchomienie programu prosto z pendriva(niezaszyfrowanego). W tym samouczku skupimy się jednak na pierwszej z nich.



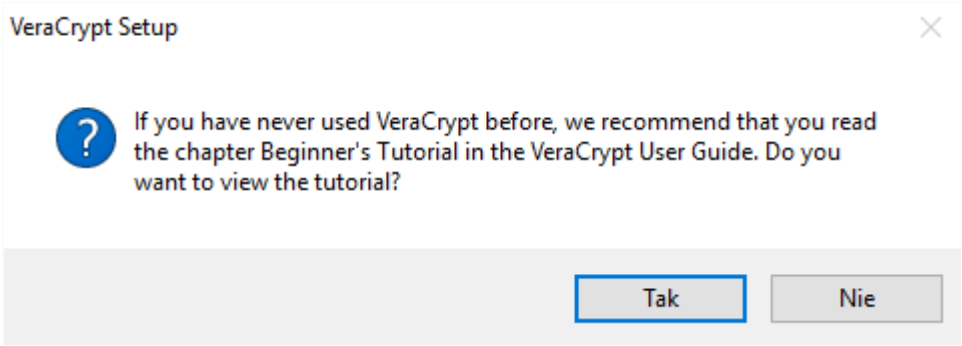
Wybieramy typ instalacji w zależności od preferencji.

Na następnej stronie możemy wybrać miejsce instalacji oraz kilka dodatkowych opcji, czyli gdzie zostanie umieszczony skrót, czy dana nam będzie możliwość stworzenia punktu przywracania systemu.



Wybieramy interesujące nas opcje dodatkowe podczas instalacji.

Klikamy Install, a gdy program się zainstaluje wybieramy Finish. Powinna się pojawić wiadomość proponująca nam skierowanie do strony www z instrukcją działania programu. Jeśli macie ochotę możecie ją przejrzeć-WARTO!.



Pytanie o chęć skorzystania z tutorialu programu.

Przygotowany pusty dysk USB, podłączamy do komputera, a następnie uruchomiamy program. Tworzymy nowy wolumin. W tym celu klikamy na Create Volume. Pojawi się takie okno:

Okno z możliwymi opcjami nowego woluminu.

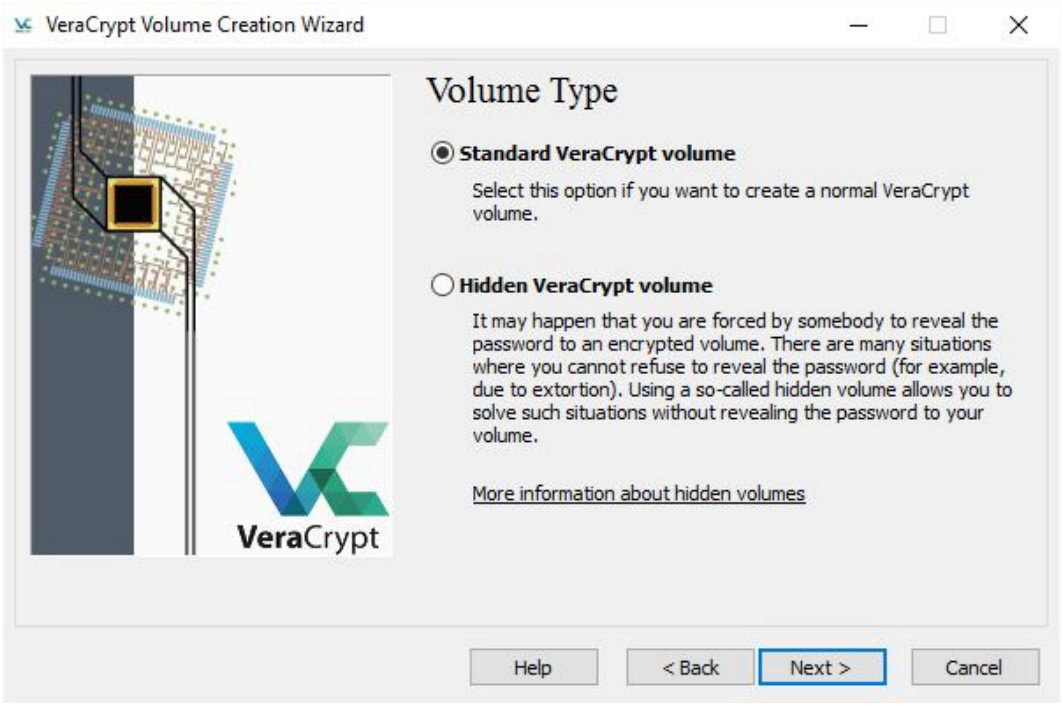
W tym miejscu mamy do wyboru, czy chcemy utworzyć pewien obszar na dysku/partycji, którego będziemy chcieli zaszyfrować (pierwsza opcja).

Druga opcja dotyczy szyfrowania pamięci flash driver (pendrive).

Trzecia z kolei opcja dotyczy zaszyfrowania całego dysku z zainstalowanym system operacyjnym (opcja dla zaawansowanych użytkowników).

Jako, że w tym poradniku interesują nas tylko dyski zewnętrzne klikamy na Next, po zaznaczeniu drugiej pozycji.

Musimy następnie zadecydować czy nasz pendrive będzie widocznie zaszyfrowany, czy może nie chcemy aby ktokolwiek wiedział, że coś na nim się znajduje. My stworzymy standardowo zaszyfrowany dysk. Klikamy na Next.

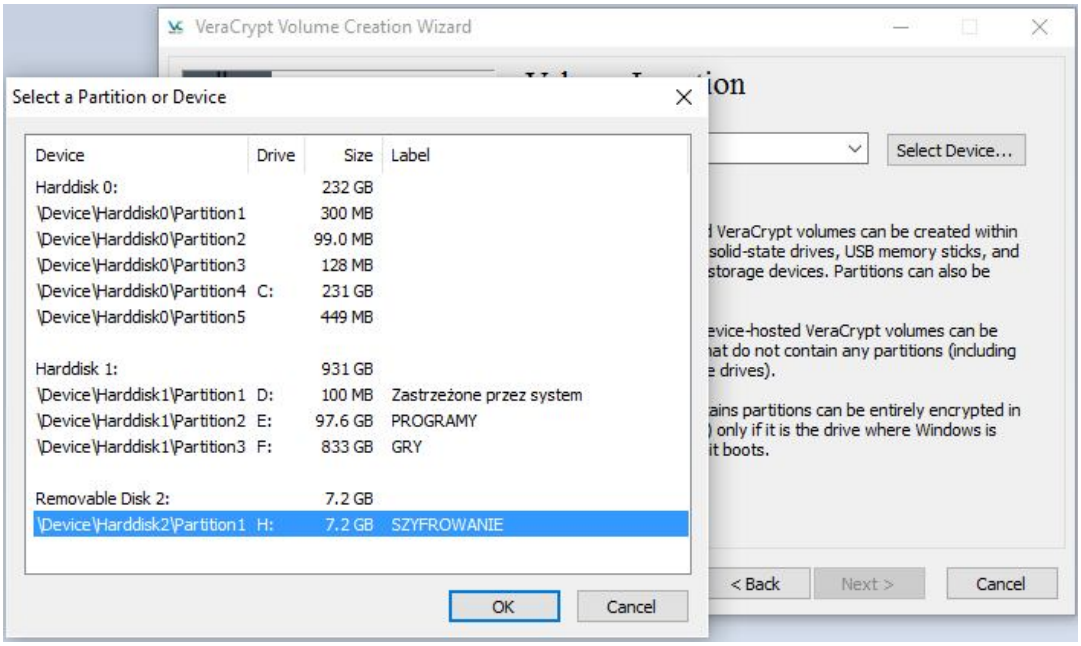


Wybieramy pomiędzy jawnym a niewidocznym szyfrowaniem.

Wybieramy urządzenie, które chcemy zaszyfrować. Klikamy na Select Device…

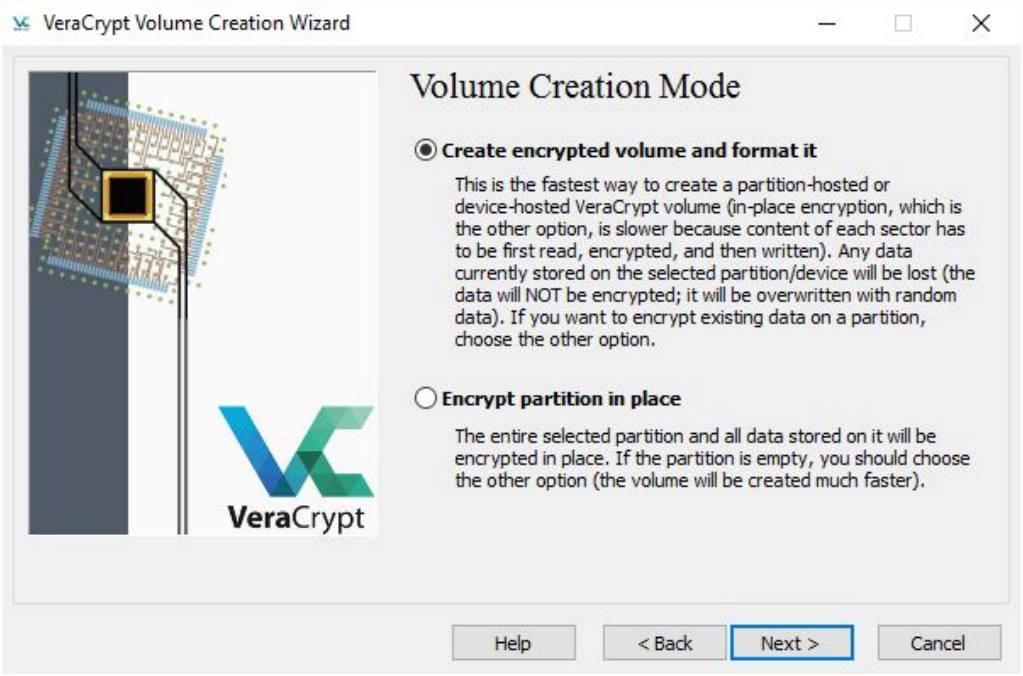
Musimy podać dysk USB, który chcemy zaszyfrować.

W naszym przypadku będzie do pendrive „Szyfrowanie”. Zaznaczmy wybrane urządzenie i klikamy OK. A następnie na Next.



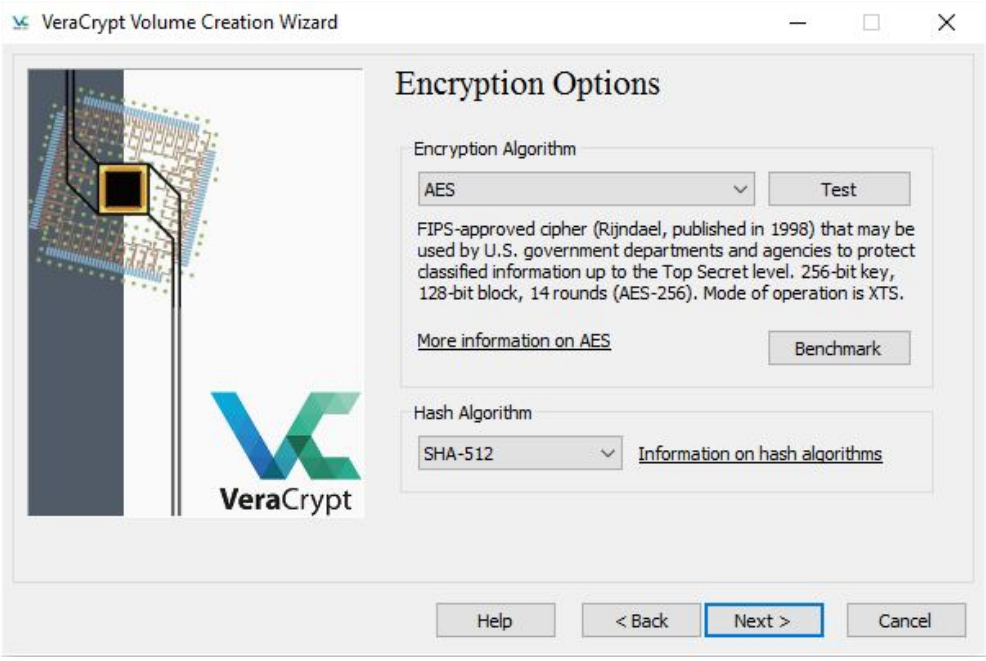
Wybieramy z listy interesujący nas pendriv’e.

Teraz mamy dwie możliwości. Pierwsza – szybsza – tworzymy czysty, zaszyfrowany dysk. Druga – wolniejsza – szyfrujemy dane już zapisane na pendrivie. My wybieramy pozycję numer jeden i klikamy Next.



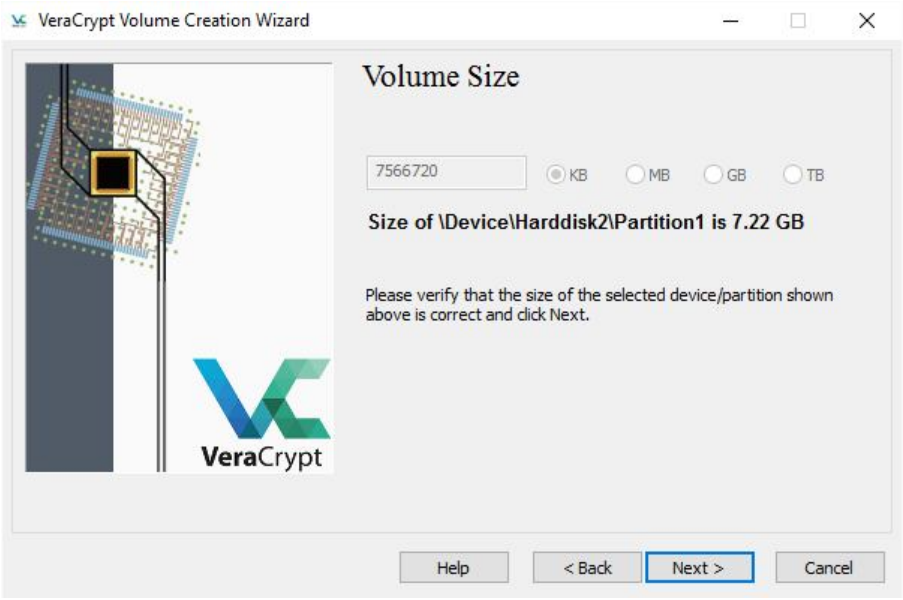
Wybieramy pomiędzy stworzeniem nowego dysku a zaszyfrowaniem już istniejącego.

W kolejnym kroku wybieramy odpowiednie szyfrowanie. Jeśli nie wiemy co wybrać domyślne ustawienia są w zupełności satysfakcjonujące. Klikamy na Next.



Wybieramy rodzaj zabezpieczeń naszego szyfrowania.

Teraz program zapyta nas czy pojemność szyfrowanego dysku jest poprawna. Jako, że u nas jest to klikamy Next.

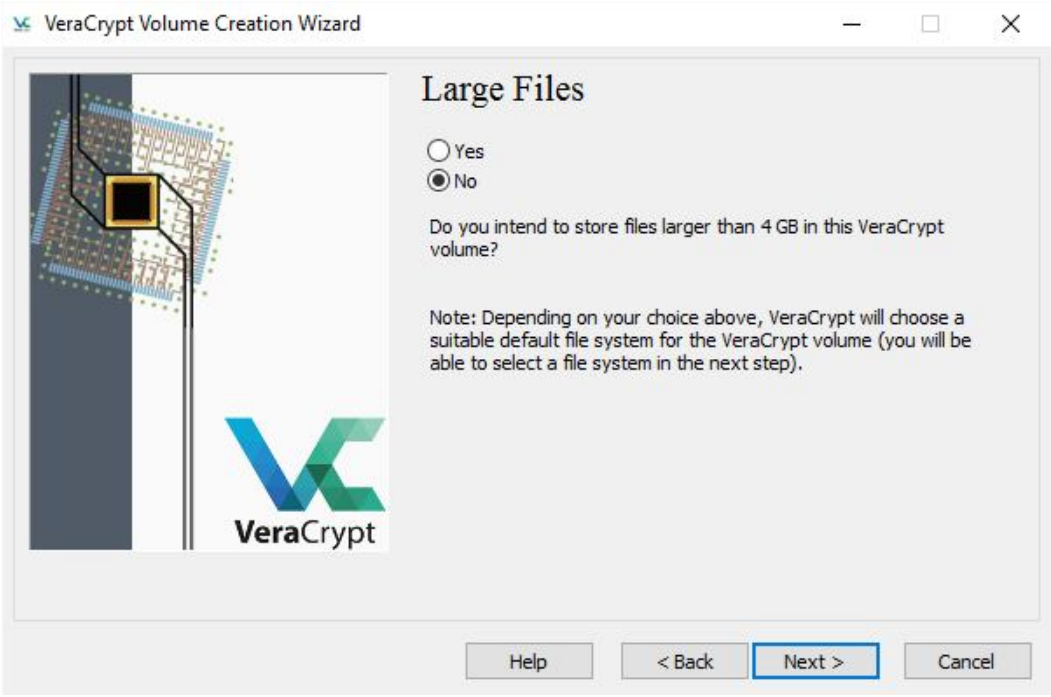


Sprawdzamy zgodność pojemności wybranego dysku USB.

Przed nami jeden z najważniejszych kroków. Wybór silnego hasła. Poniżej miejsc do wprowadzenia znajduje się podpowiedź co powinno zawierać silne hasło. Przypomnimy, że odradza się używania słów z dowolnego języka, hasło powinno być długie, najlepiej na ponad 20 znaków, zawierać małe i duże litery, cyfry oraz znaki specjalne. Klikamy Next.

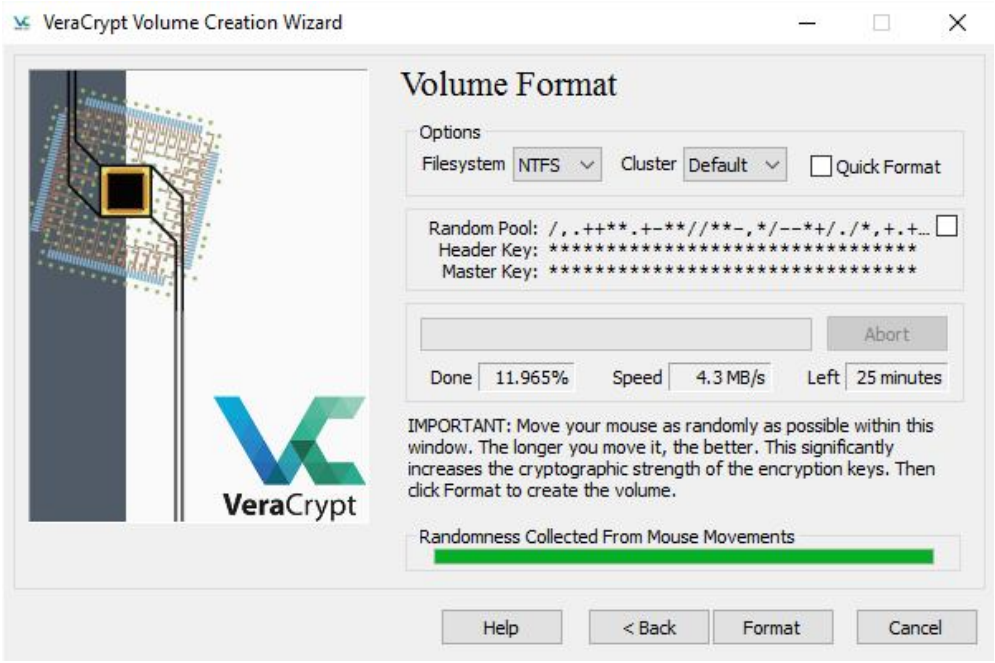
Pamiętajmy o tym by hasło było odpowiednio długie i skomplikowane.

Dodatkowe pytanie ma pomóc programowi lepiej dostosować się do naszych potrzeb. Jeśli zamierzamy trzymać na pendrive pliki powyżej 4 GB należ zaznaczyć Yes. Większość z nas jednak wybierze No, jako że zdjęcia czy dokumenty zajmują dużo mniej miejsca. Klikamy Next.



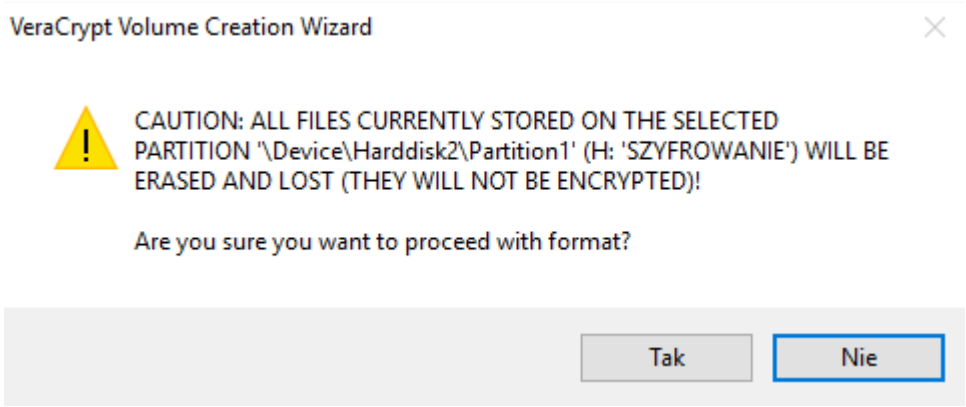
W zależności od potrzeb i użytkowania wybieramy odpowiednią opcję.

Musimy teraz zdecydować jaki system plików będzie dla nas korzystniejszy. Szybszy jest i bardziej funkcjonalny jest system plików NTFS, jest obsługiwany przez systemy Windows oraz Linux. Parametr Cluster pozostawmy jako Default. Teraz musimy się troszkę najeździć myszką, najlepiej powyżej 30 sekund, w celu stworzenia silnego szyfrowania. Minimalnie jednak należy zakolorować pasek na zielono. Gdy to zrobimy klikamy Format.



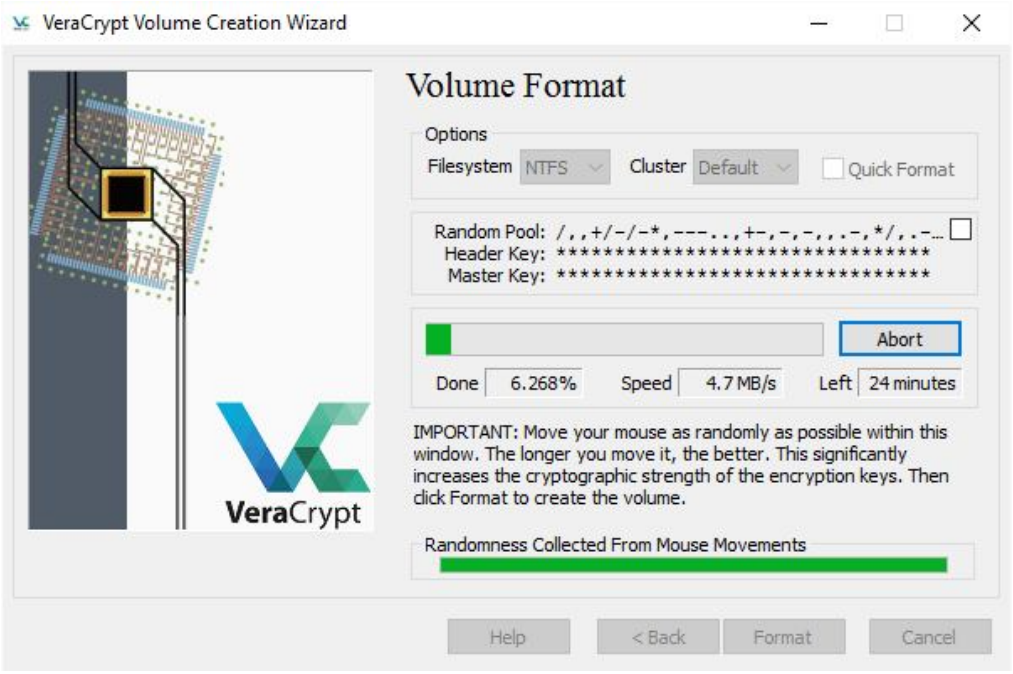
Tworzymy szyfrowanie na podstawie losowych ruchów myszką. Wybieramy także system plików dla naszego dysku.

Program ostrzeże nas jeszcze przed utratą wszystkich plików. Zgadzamy się klikając Tak.



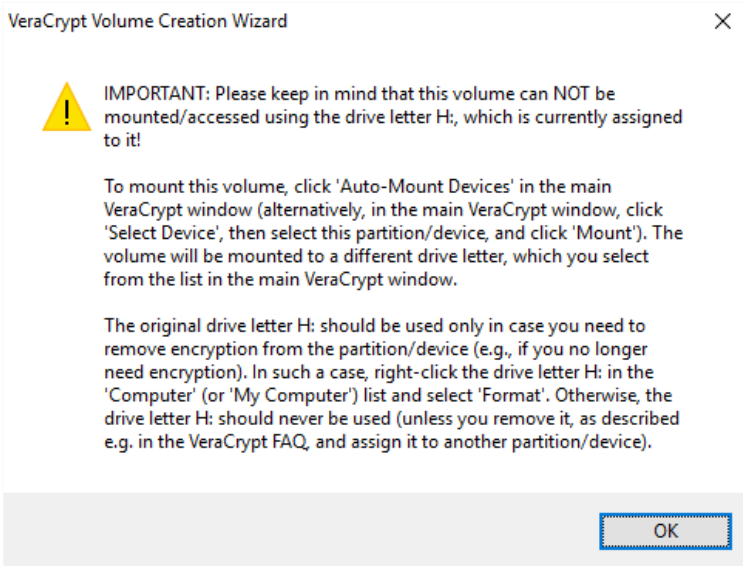
Ostrzeżenie przed utratą plików.

Następnie musimy poczekać aż dysk USB zostanie zaszyfrowany.



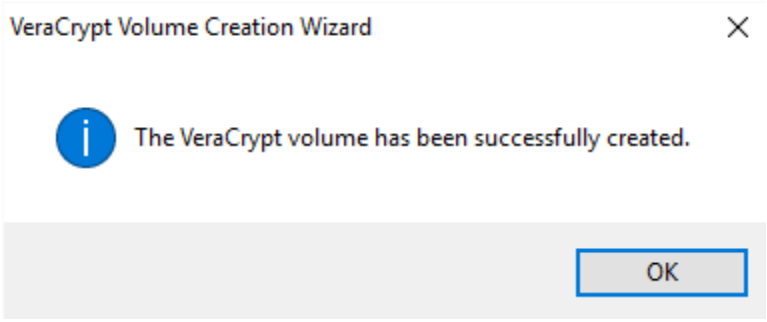
Nie martwcie się jeśli to chwilę trwa, efekt jest tego wart!

Gdy szyfrowanie się zakończy otrzymamy jeszcze jeden komunikat tłumaczący nam jak należy poprawnie korzystać ze świeżo stworzonego dysku oraz czego nie robić. Po zapoznaniu się z nim klikamy OK.



Krótka instrukcja korzystania z nowo zaszyfrowanego dysku USB.

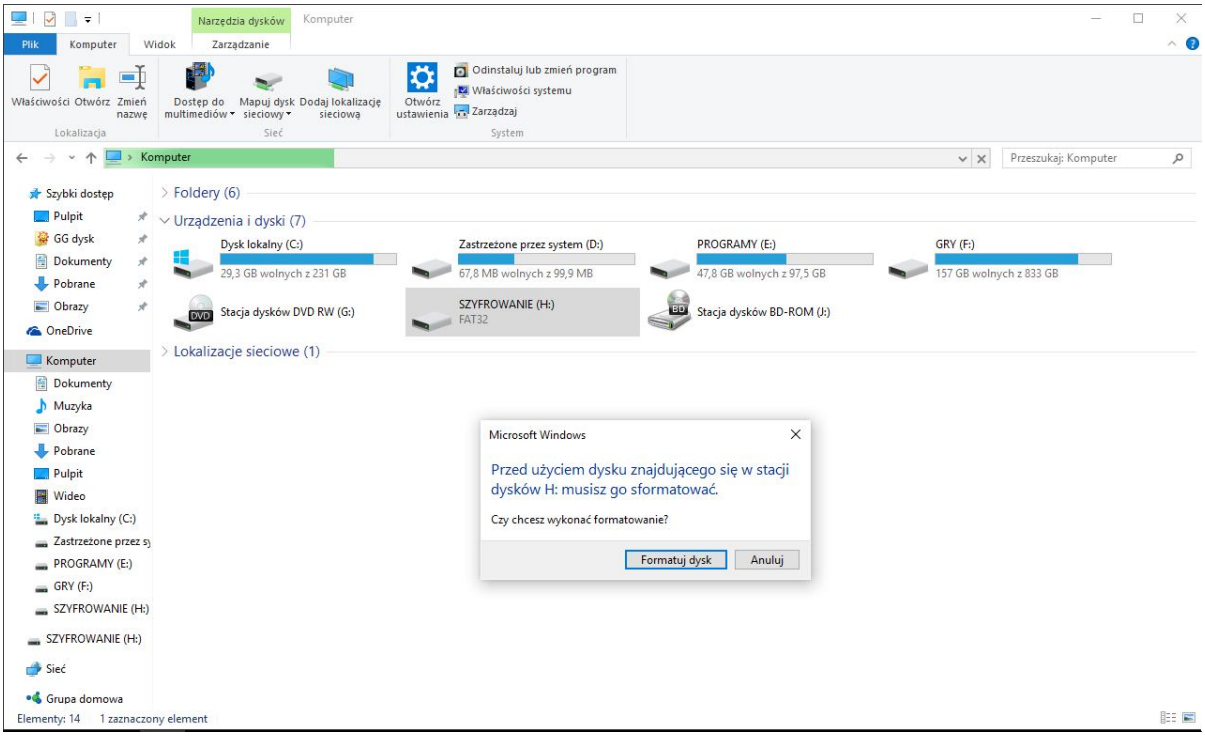
Jeśli wszystko poszło pomyślnie otrzymamy wiadomość o sukcesie. Klikamy OK.



Gdy wszystko się udało.

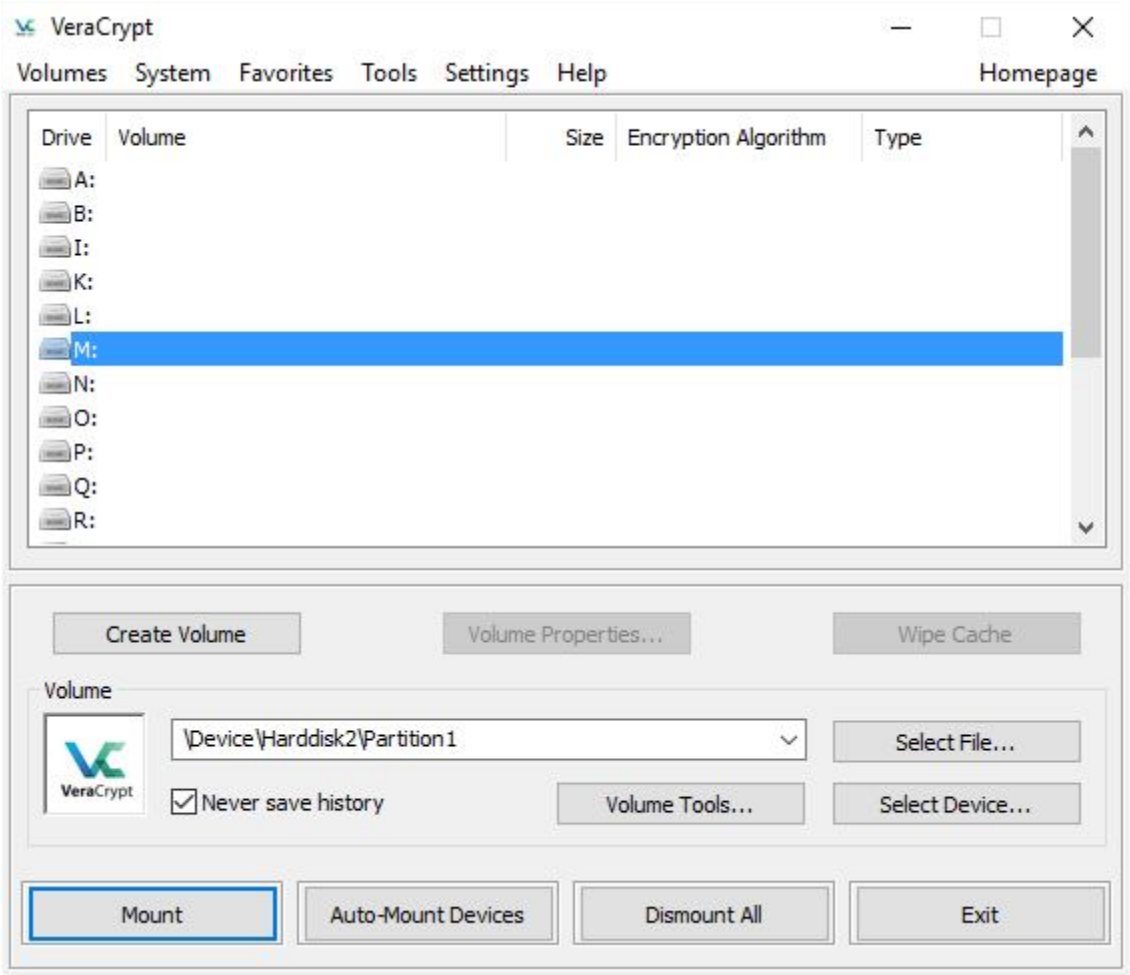
Teraz możemy albo stworzyć nowy zaszyfrowany dysk klikając na Next, albo zakończyć pracę szyfratora wybierając Exit.

Aby móc skorzystać teraz z dysku musimy go zamontować w programie. Wybieramy dowolną literę, różną od tej, która widnieje w moim komputerze dla tego dysku (w naszym przypadku H:). Jeśli go nie zamontujemy otrzymamy powiadomienie.



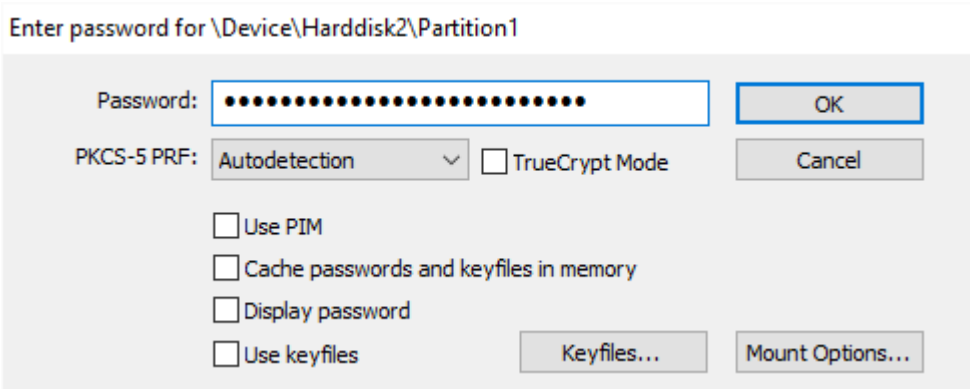
Gdy nie zamontujemy zaszyfrowanego dysku nie dostaniem się do jego plików.

Wracamy do VeraCrypt. Klikamy Select Device… i wybieramy nasz zaszyfrowany dysk H: i klikamy Mount.

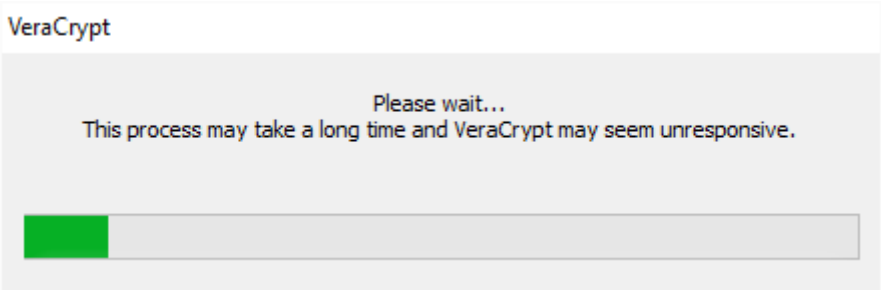


Wybieramy literę dysku, pod jaką pojawi się zawartość zaszyfrowanego pendriva.

Zostaniemy poproszeni o podanie hasła. Po wpisaniu klikamy OK.

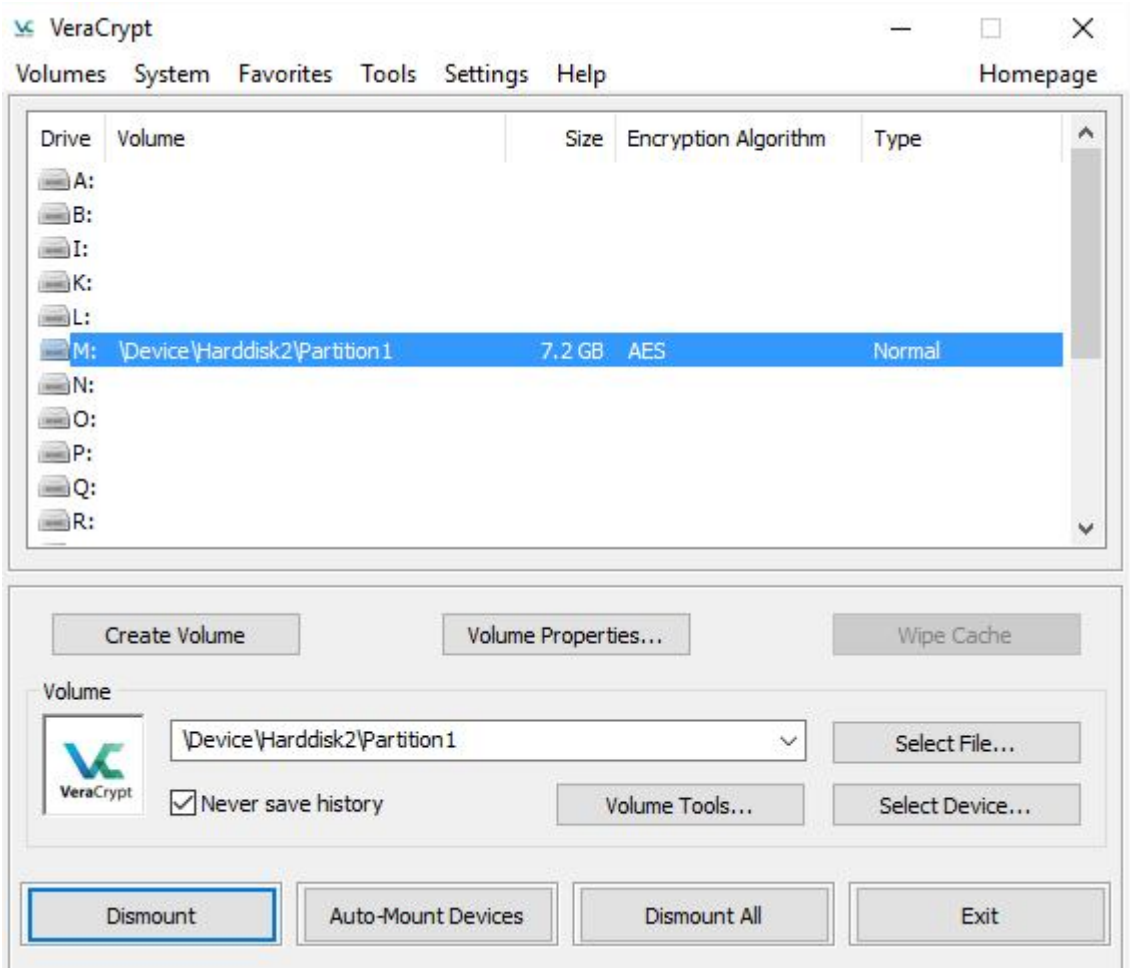


Podajemy hasło w celu odszyfrowania dysku USB.

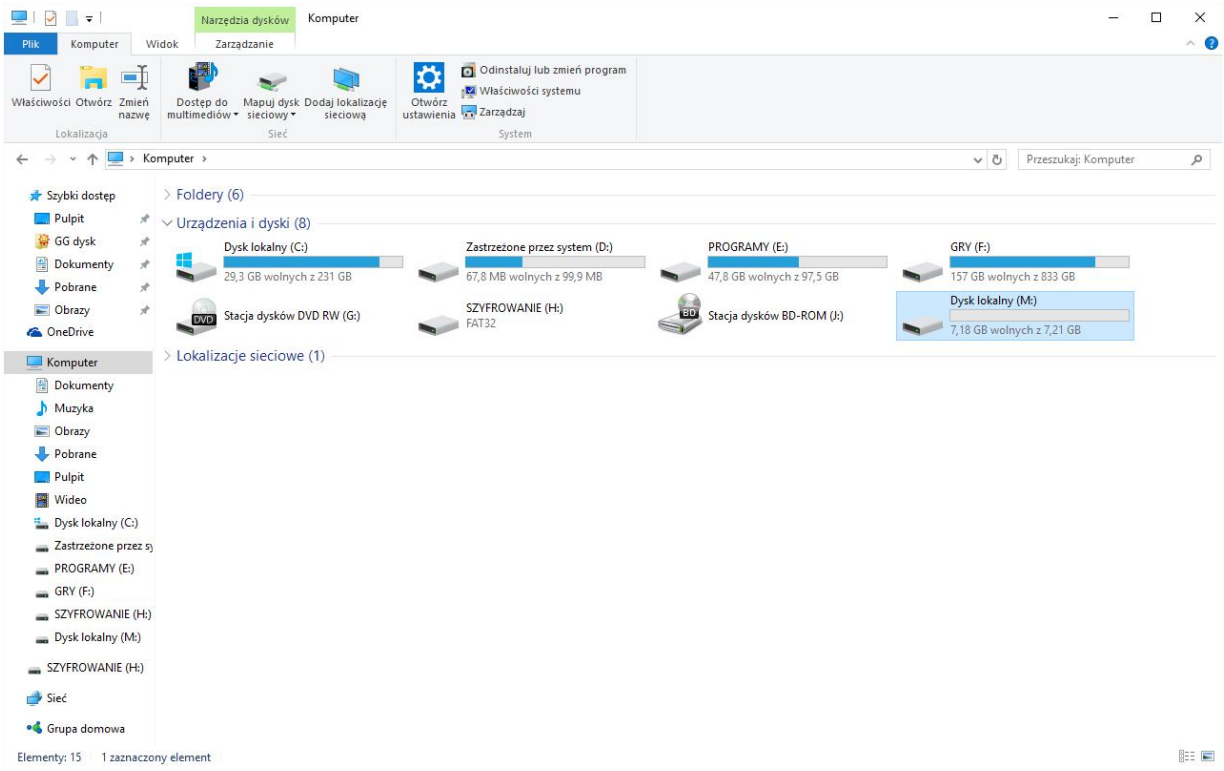


Czekamy na odszyfrowanie zawartości.

Gdy proces montowania dobiegnie końca możemy pod literką M: korzystać z pendriva normalnie, a każdy plik, który na nim umieścimy automatycznie się zaszyfruje.



Gdy wszystko poszło poprawnie zamontowany dysk pojawi się na liście.



Korzystamy normalnie z pendriva, a pliki same się szyfrują.

17. SKRÓCONA INSTRUKCJA POSTĘPOWANIA W PRZYPADKU NARUSZENIA OCHRONY DANYCH OSOBOWYCH

a. w przypadku stwierdzenia lub podejrzenia naruszenia ochrony danych osobowych każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest niezwłocznie do powiadomienia Administratora Danych Osobowych oraz Inspektora Ochrony Danych :
   - ✓ osobiście,
   - ✓ e-mailowo na adres: ……. oraz do wiadomości: iod@cudk.pl,
   - ✓ w przypadku braku możliwości dokonania powiadomienia e-mailowego z przyczyn technicznych dopuszcza się możliwość zgłoszenia telefonicznego pod numer: 663614820;.

b. do sytuacji wymagających powiadomienia, należą:
   - ✓ niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów,
   - ✓ niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą
     i utratą danych osobowych,
   - ✓ nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka / ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek).

c. do incydentów wymagających powiadomienia, należą:
   - ✓ zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności),
   - ✓ zdarzenia losowe wewnętrzne (awarie serwera, komputerów twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata/zagubienie danych),
   - ✓ umyślne incydenty (włamania do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania),
   - ✓ ślady na drzwiach, oknach i szafach wskazują na próbę włamania,
   - ✓ niszczenie dokumentacji w nieskuteczny sposób,
   - ✓ fizyczna obecność w budynku lub pomieszczeniach osób zachowujących się podejrzanie,
     otwarte drzwi do pomieszczeń, szaf gdzie przechowywane są dane osobowe,

- ✓ ustawienie monitorów pozwalające na wgląd osób postronnych w dane osobowe,
- ✓ wynoszenie danych osobowych w wersji papierowej i elektronicznej na zewnątrz organizacji bez upoważnienia,
- ✓ udostępnienie danych osobowych osobom nieupoważnionym w formie papierowej, elektronicznej i ustnej,
- ✓ telefoniczne próby wyłudzenia danych osobowych,
- ✓ maile zachęcające do ujawnienia identyfikatora i/lub hasła,
- ✓ pojawienie się wirusa komputerowego lub niestandardowe zachowanie komputerów,
- ✓ umieszczanie haseł do systemów w pobliżu komputera.

18. OBOWIĄZEK ZACHOWANIA POUFNOŚCI I OCHRONY DANYCH OSOBOWYCH

a. Każda z osób dopuszczona do przetwarzania danych osobowych jest zobowiązana do:

   - ✓ przetwarzania danych osobowych wyłącznie w zakresie i celu przewidzianym w powierzonych przez Administratora Danych Osobowych
   - ✓ zachowania w tajemnicy danych osobowych, do których ma lub będzie miał/a dostęp w związku z wykonywaniem zadań powierzonych przez Administratora Danych Osobowych
   - ✓ niewykorzystywania danych osobowych w celach niezgodnych z zakresem i celem zadań powierzonych przez
   - ✓ zachowania w tajemnicy sposobów zabezpieczenia danych osobowych
   - ✓ ochrony danych osobowych przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją danych osobowych, nieuprawnionym ujawnieniem danych osobowych, nieuprawnionym dostępem do danych osobowych oraz przetwarzaniem.

b. Osoba dopuszczona do przetwarzania odbywa szkolenie z zasad ochrony danych osobowych
c. Zabrania się przekazywania bezpośrednio lub przez telefon danych osobowych osobom nieupoważnionym lub osobom których tożsamości nie można zweryfikować lub osobom podszywającym się pod kogoś innego
d. Zabrania się przekazywania lub ujawniania danych osobom lub instytucjom, które nie mogą wykazać się jasną podstawą prawną do dostępu do takich danych.