Załącznik 6
do Regulaminu przetwarzania i ochrony danych osobowych w pracy zdalnej

ZASADY BEZPIECZEŃSTWA PRZETWARZANIA DANYCH DLA UŻYTKOWNIKÓW SYSTEMÓW INFORMATYCZNYCH

PORADNIK ADMINISTRATORA DANYCH

…….
Pieczęć firmowa

……
podpis Administratora danych

INSTRUKCJE

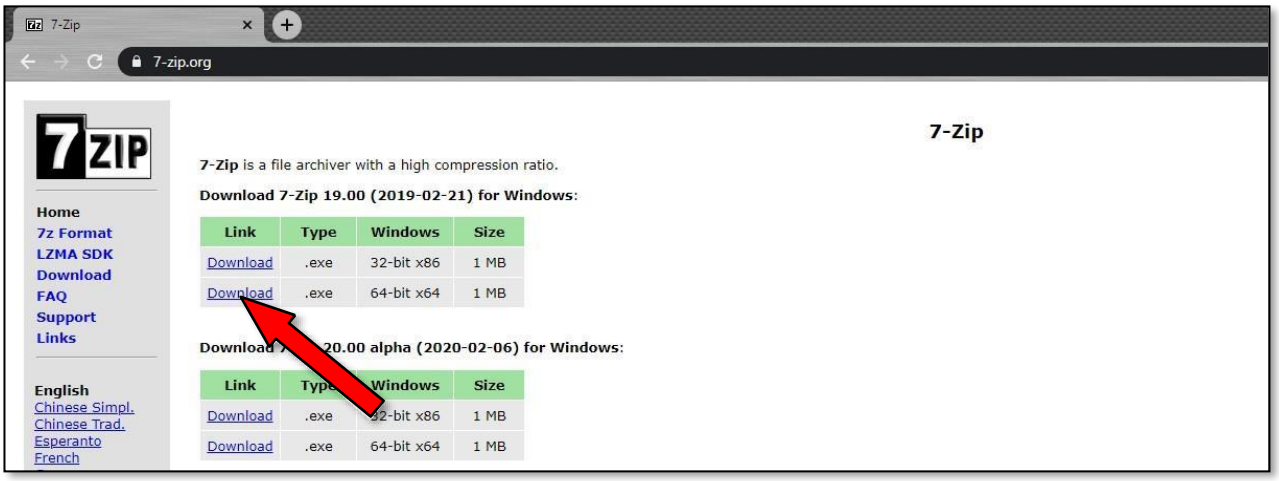
1. **SZYFROWANIE POSZCZEGÓLNYCH PLIKÓW I FOLDERÓW**
   Instrukcja nr 1 - Instrukcja instalacji oraz używania programu 7-zip
2. **SZYFROWANIE I UŻYTKOWANIE PENDRIVE'ÓW**
   Instrukcja nr 2 – Instrukcja szyfrowania pendrive'ów narzędziem BitLocker
3. **BEZPIECZNE KORZYSTANIE Z PRZEGLĄDARKI INTERNETOWEJ**
   Instrukcja nr 3 – Instrukcja bezpiecznego korzystania z przeglądarki internetowej

SZYFROWANIE POSZCZEGÓLNYCH PLIKÓW I FOLDERÓW (Instrukcja użytkowania oprogramowania)

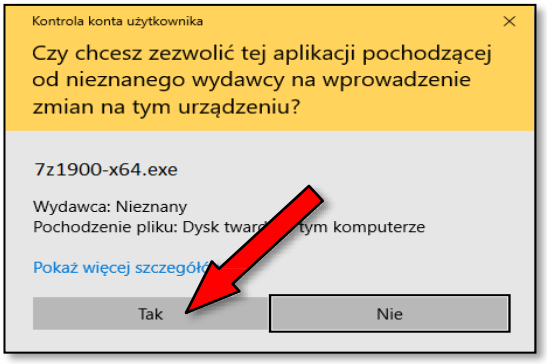
NAZWA OPROGRAMOWANIA:	*7-ZIP*
ZAKRES INSTRUKCJI:	*Instalacja, konfiguracja oraz szyfrowanie danych (plików i folderów)*

ETAP I: INSTALACJA

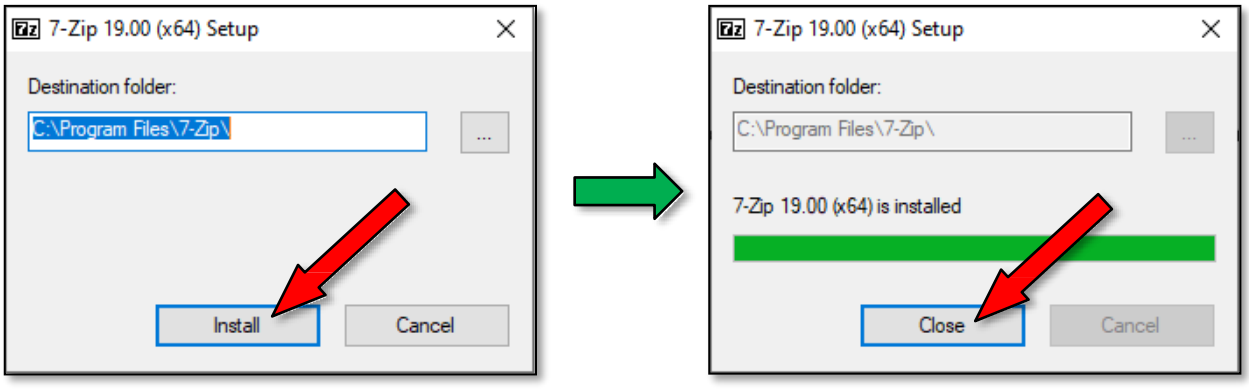
1. Otwórz przeglądarkę internetową (Chrome, Firefox, Edge itp.), następnie w pasku adresu wpisz: „**7-zip.org**” oraz naciśnij „**ENTER**”. Otworzy się następująca strona internetowa:



2. Aby pobrać program, kliknij „**Download**” dla wersji 64-bit x64. Jest to wersja programu 7-zip dla systemu operacyjnego Windows 7, 8, 8.1, 10 w wersji 64 bitowej (bardzo rzadko spotyka się już systemy Windows wersji 32 bitowej z uwagi na przestarzałą technologię).
3. Następnie uruchom program. W przeglądarce Chrome znajdziemy skrót do programu w dolnym lewym rogu. W innych przeglądarkach zazwyczaj pobrane programy znajdują się w katalogu: „**Pobrane**”. Po uruchomieniu programu może się pojawić komunikat i klikamy „**Tak**”:



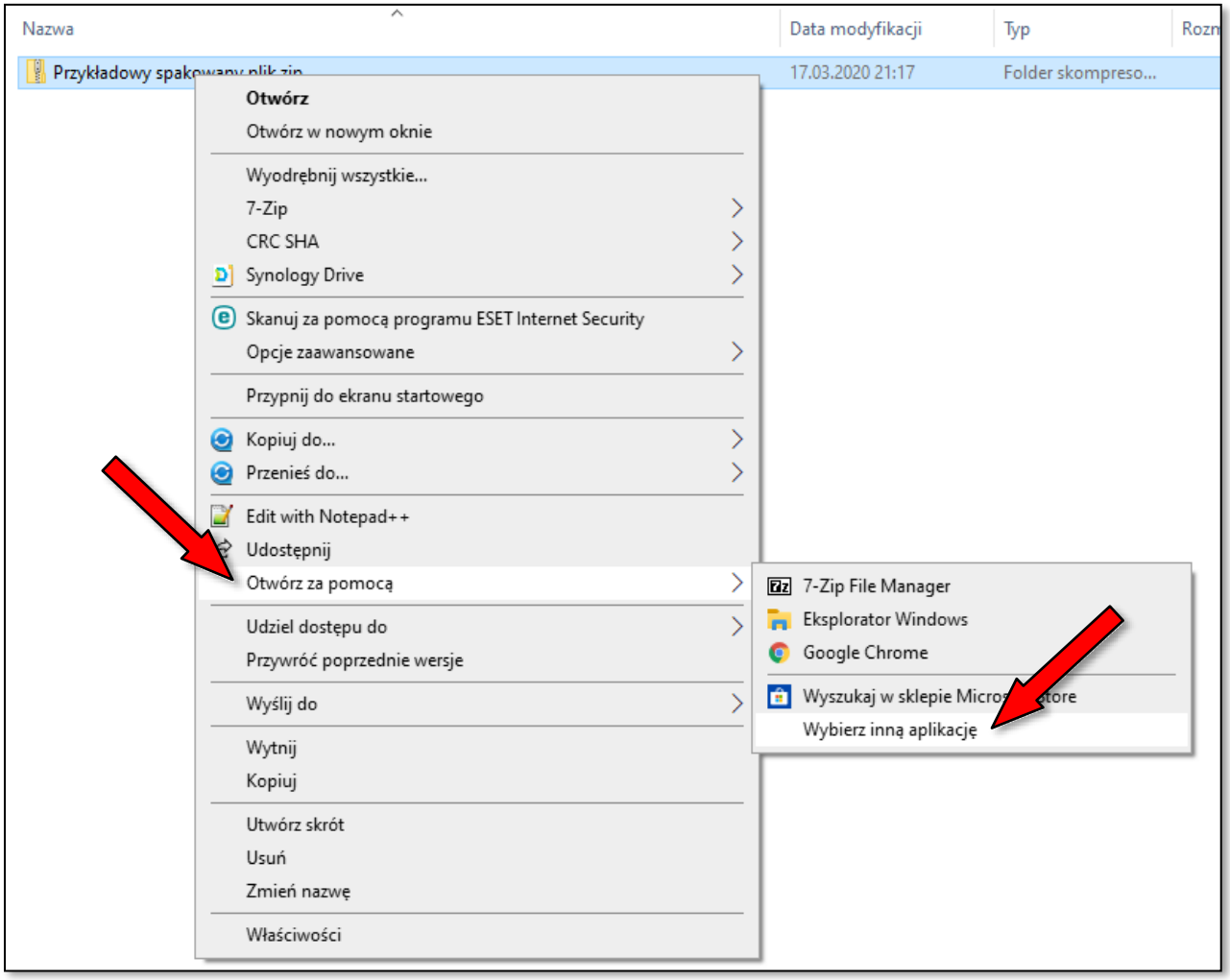
4. Następnie pojawi się okno w którym wskazujemy miejsce zainstalowania programu. Nie trzeba nic zmieniać. Klikamy tylko „**Install**”, a po zainstalowaniu programu „**Close**”:



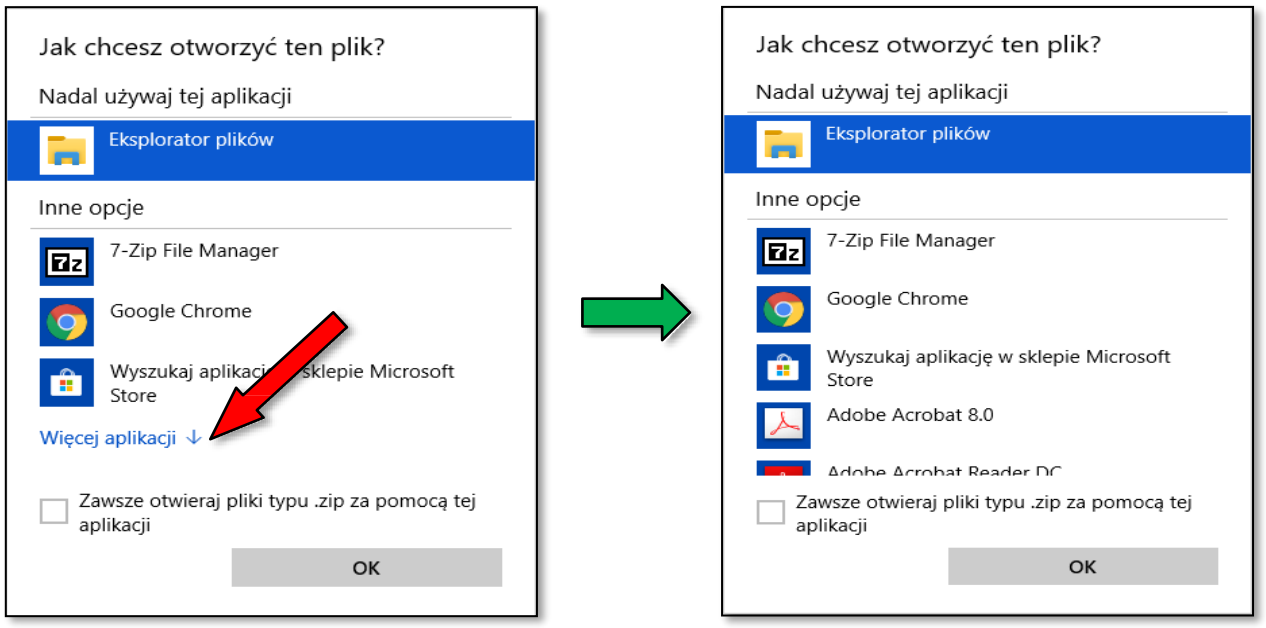
5. Od teraz masz zainstalowany program kompresujący pliki o nazwie 7-zip.

ETAP II: KONFIGURACJA

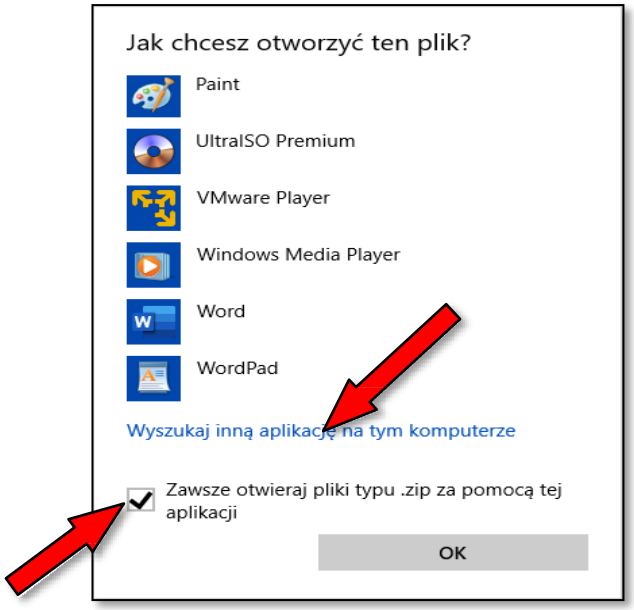
1. Czasami system operacyjny Windows pomimo instalacji programu 7-zip otwiera pliki skompresowane „spakowane” poprzez swoje zaimplementowane narzędzie do archiwów. Stwarza to częste problemy w przypadku „zahasłowanych” archiwów. Warto to zmienić. Aby to wykonać:
2. Znajdź na swoim komputerze jakikolwiek „skompresowany „spakowany” plik z rozszerzeniem *.zip.
3. Kliknij go prawym przyciskiem myszy → rozwinie się podręczne menu, w którym klikamy po kolei: „**Otwórz za pomocą**” → „**Wybierz inną aplikację**”:



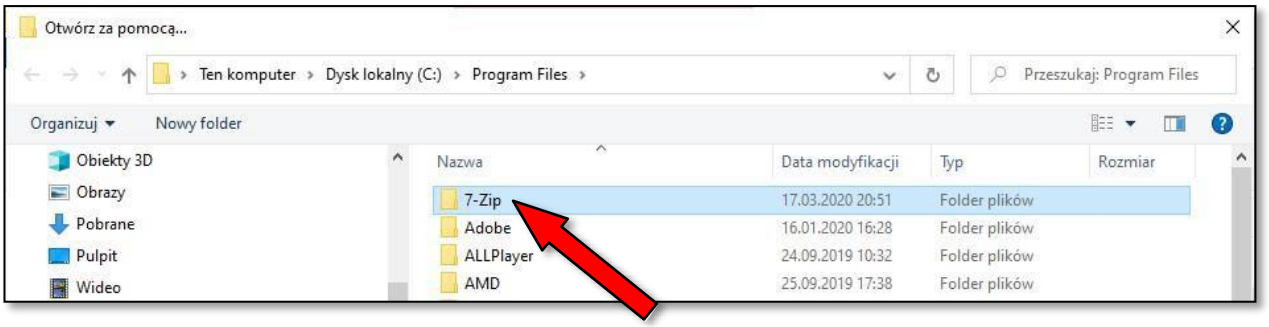
4. Otworzy się okno, w którym określasz w jaki sposób chcesz otworzyć plik. Klikamy: „**Więcej aplikacji** ˅ ”, po czym rozwinie się lista z większa ilością programów:



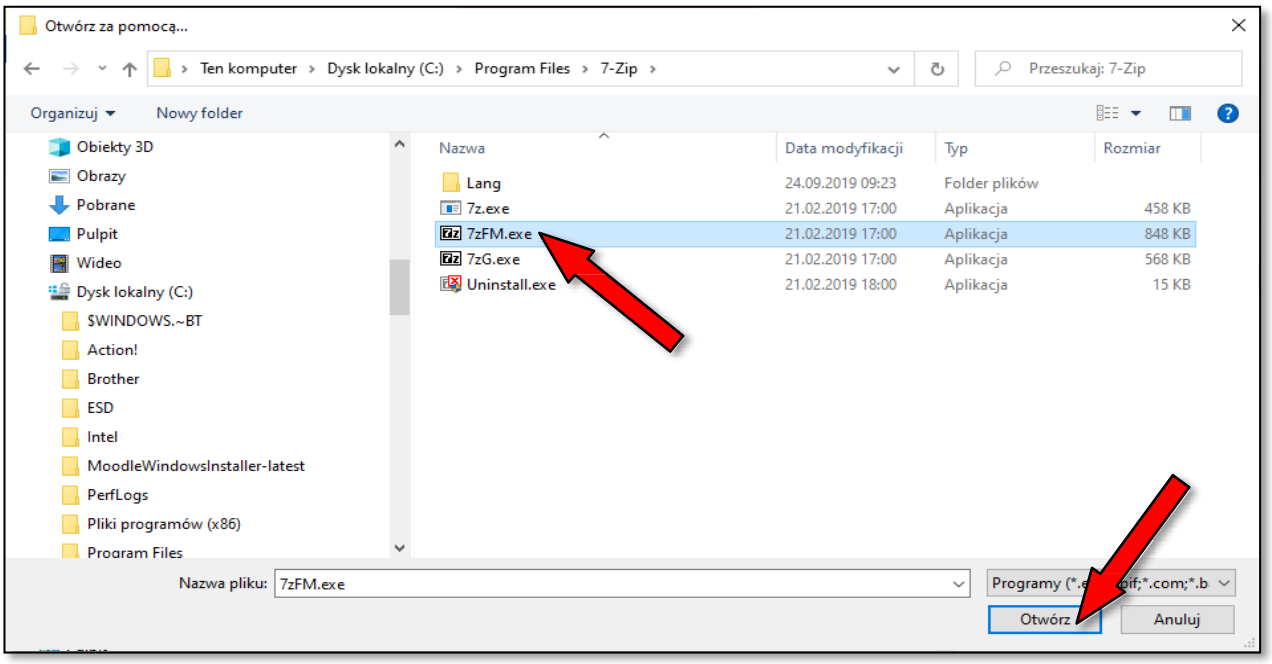
5. Następnie przewiń listę na sam dół, zaznacz „✓” checkbox „**Zawsze otwieraj pliki typu .zip za pomocą tej aplikacji**” oraz kliknij „**Wyszukaj inną aplikację na tym komputerze**”.



6. Teraz otworzy się okno, w którym wskazujemy folder zawierający program 7-zip. W każdej wersji Windowsa (czy to 7, 8, 8.1 bądź 10) może być inaczej. Niniejsza instrukcja opiera się o system operacyjny Windows 10, gdzie folder z programem ma następującą ścieżkę: „/Ten komputer/Dysk lokalny (C)/Program files/7-Zip/” lub w nomenklaturze informatycznej: „C:\Program Files\7-Zip”. A więc klikamy dwa razy lewym przyciskiem myszy (aby otworzyć) folder „**7-Zip**”:



7. Następnie zaznaczamy jednym kliknięciem lewego przycisku myszy plik: „**7zFM.exe**” i klikamy przycisk „**Otwórz**”:

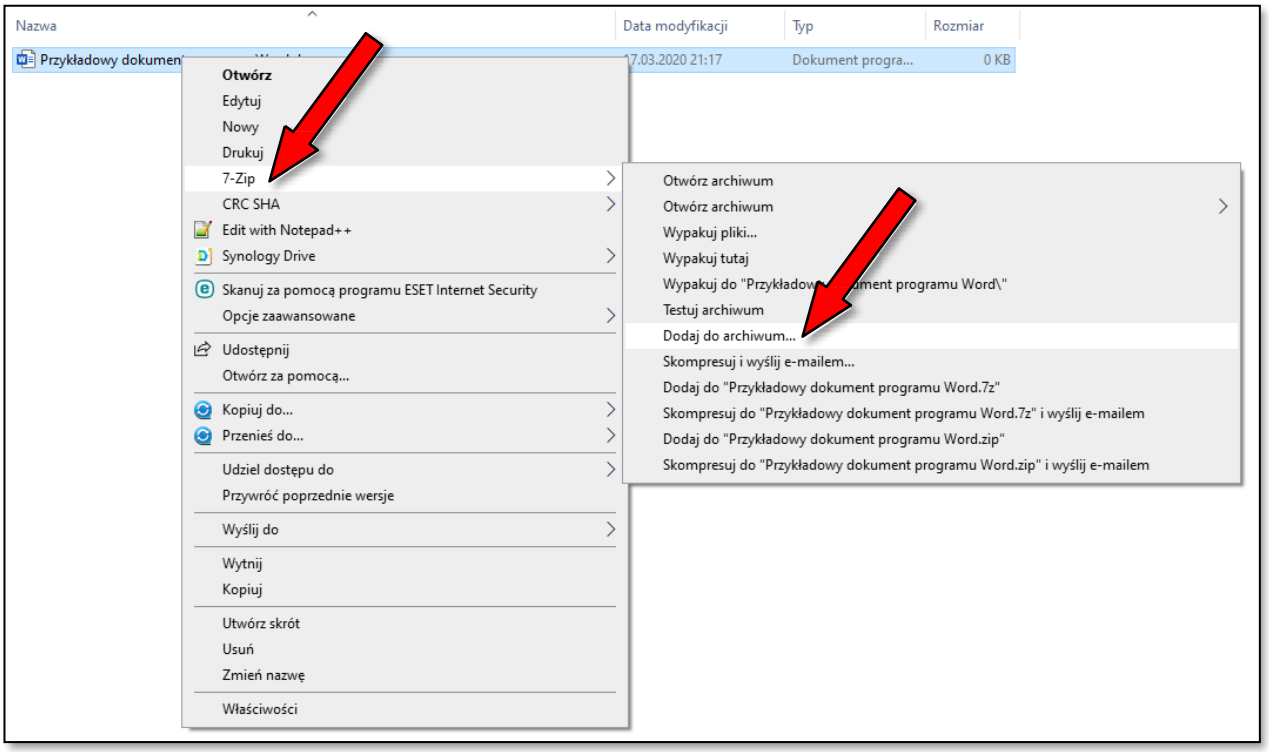


8. Od teraz każdy plik (archiwum) w formacie *.zip będzie otwierane przez program 7-Zip, co umożliwi bezproblemowe otwieranie „zahasłowanych” plików.

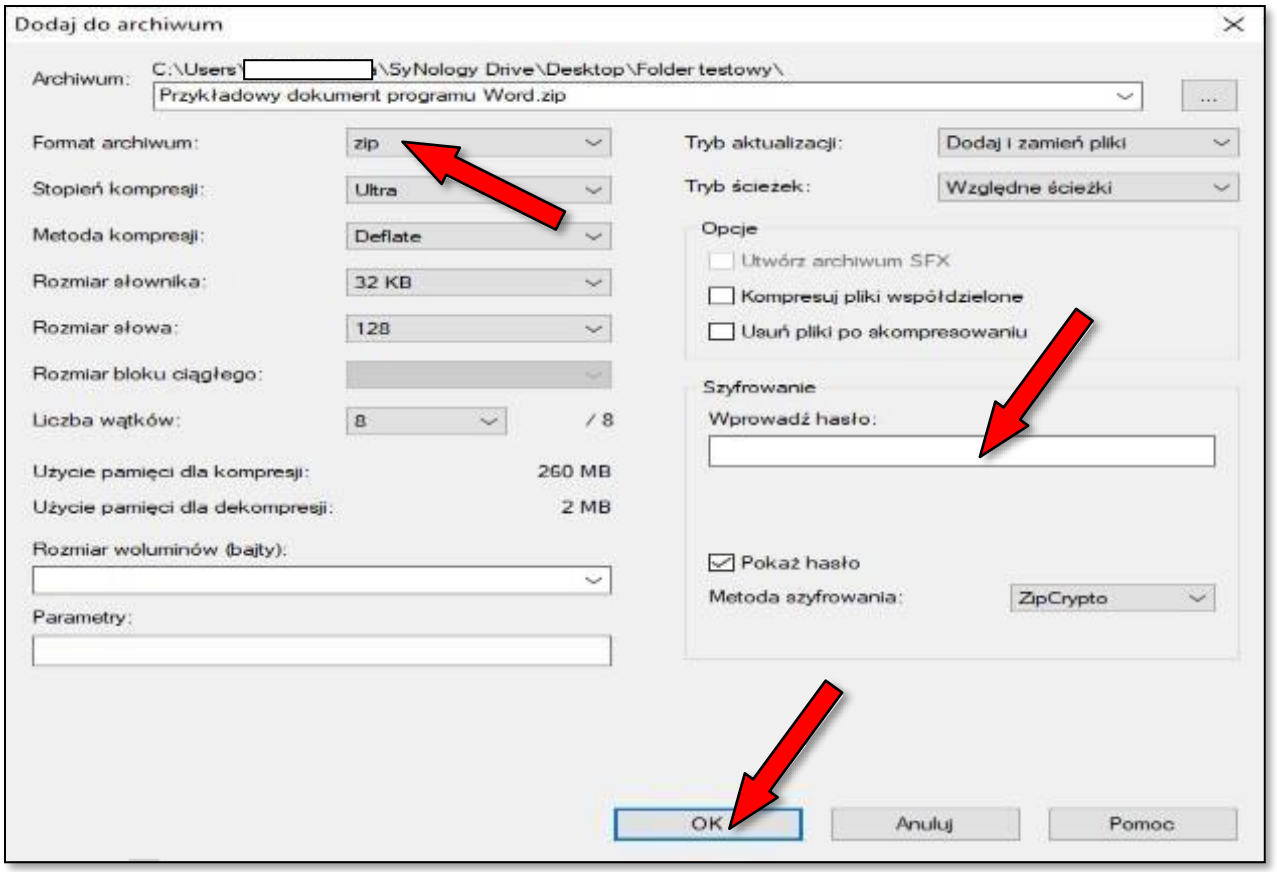
ETAP III: SZYFROWANIE DANYCH (PLIKÓW I FOLDERÓW)

Chcąc zaszyfrować plik lub cały folder, musisz wykonać następujące czynności:

1. Kliknij prawym przyciskiem myszy na wybrany plik(i) lub folder(y). Następnie kliknij w menu „**7-Zip**” oraz „**Dodaj do archiwum…**”:



2. Teraz otworzy się okno konfiguracji kompresji i szyfrowania dla wybranego przez Ciebie pliku(ów) lub folderu(ów). Warto ustawić format archiwum na „**ZIP**”. W przyszłości automatycznie każda czynności kompresji i szyfrowania będzie zapamiętana dla tego ustawienia. Oczywiście w polu „**Wprowadź hasło**” wpisujemy je. Następnie klikamy „**OK**”. Po skompresowaniu („spakowaniu”) pliku(ów) lub folderu(ów) plik z rozszerzeniem *.zip zapisze się w macierzystym katalogu, w którym były źródłowe dane. Wszystko gotowe :



SZYFROWANIE I UŻYTKOWANIE PENDRIVE'ÓW (Instrukcja użytkowania oprogramowania)

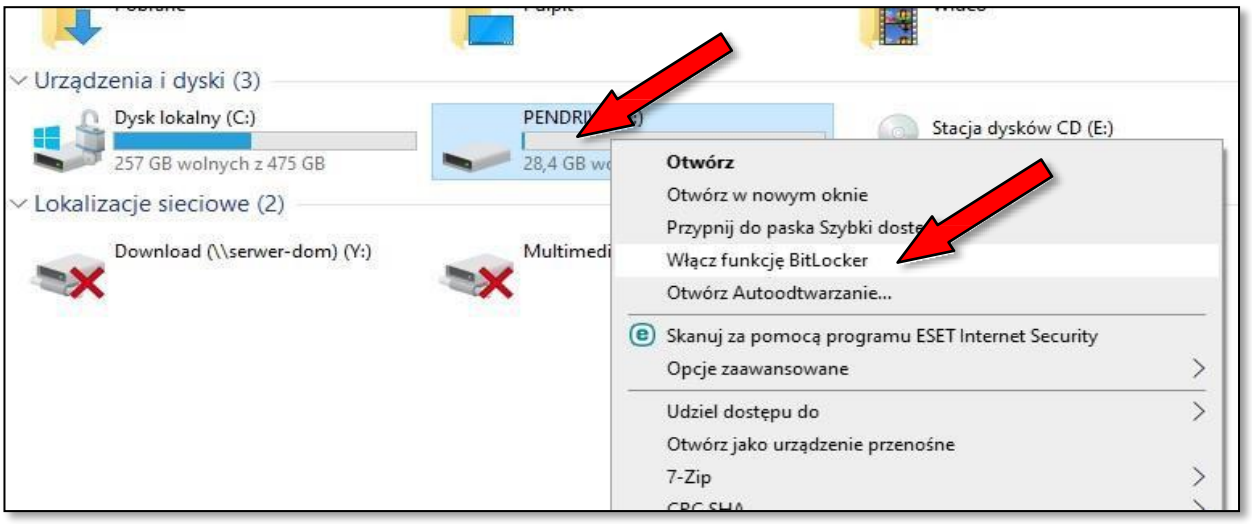
NAZWA OPROGRAMOWANIA:	*BitLocker*
ZAKRES INSTRUKCJI:	*Warunki techniczne, proces pierwszego szyfrowania, użytkowanie zaszyfrowanego penrive'a, odzyskiwanie pendrive'a poprzez „klucz odzyskiwania".*

ETAP I: WARUNKI TECHNICZNE

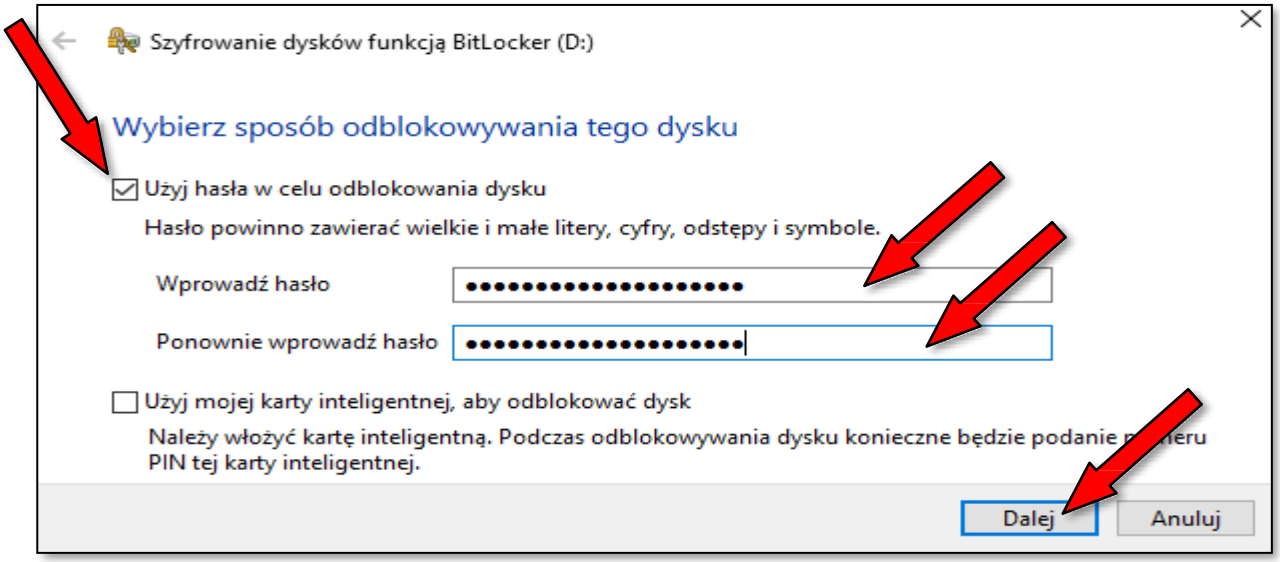
1. Chcąc korzystać z szyfrowania urządzeń zewnętrznych (np. pendrive'ów) na rynku IT jest wiele dostępnych narzędzi płatnych oraz bezpłatnych. Warto zauważyć, że większość z nich wymaga specjalistycznego oprogramowania oraz aby umożliwić odczyt zaszyfrowanego urządzenia na każdym komputerze → wymaga się zainstalowanego „agenta" lub innej formy dostępu do danych (w tym też dodatkowych plików „rozruchowych" na pendrive'ie). Jest to uciążliwe i w praktyce nie zawsze zapewniające w 100% bezpieczeństwo (chociażby z uwagi na częste praktyki dzielenia przestrzeni pamięci pendrive'a na zaszyfrowaną i niezaszyfrowaną, co skłania użytkowników do częstego zapisu w tej części nieszyfrowanej). Obecne techniki szyfrowania opierają się algorytmy szyfrowania typu AES-256, które gwarantują bardzo wysoki poziom bezpieczeństwa.
2. Zalecaną forma szyfrowania jest wbudowana funkcja BitLocker w system operacyjny Microsoft Windows, jednakże tylko niektóre wersje potrafią szyfrować przy czym każda obsługuje (odczyt i zapis) zaszyfrowany pendrive (oczywiście są wyjątki, ale mowa tu o bardzo przestarzałych wersjach sprzed parunastu lat).
3. Systemy operacyjne Microsoft Windows, które maja wbudowaną funkcję szyfrowania urządzeń zewnętrznychto:
   - **a)** Windows 7 Ultimate oraz Enterprise,
   - **b)** Windows 8 Pro oraz Enterprise,
   - **c)** Windows 10 Pro Enterprise oraz Education
   - **d)** Windows 11 Pro Enterprise oraz Education.
4. Jeżeli posiadamy chociażby jeden komputer z system operacyjnym spośród wyżej wymienionych, możemy zaszyfrować wszelakie pendrive i będą one działały na wszystkich systemach operacyjnych Microsoft Windows w tym na wersjach „Home", które niestety dość często są używane w sektorze publicznym i niepublicznym z uwagi na koszt zakupu wraz z nowym sprzętem (warto zauważyć, iż podczas zakupu sprzętu poleasingowego, zjawisko to właściwie nie występuję).
5. Warto rozważyć 2 scenariusze:
   - **a)** zakup pendrive'ów oraz ich zaszyfrowanie (proces ten nie musi się nawet odbyć na sprzęcie organizacji → oczywiście z zachowaniem najwyższej staranności w zakresie bezpieczeństwa informacji). Na obecna chwilę, ceny rynkowe pendrive'ów są bardzo niskie. Wystarczająca pojemność oscyluje w granicach od 2 do 4 GB pamięci.
   - **b)** wypracowanie z pracownikami organizacji wspólnego stanowiska co do zaszyfrowania ich prywatnego pendrive'a, co nie ograniczy swobody i prywatności pracownika (nadal ma pełny dostęp do danych), a wręcz polepszy ich prywatne bezpieczeństwo.
6. Urządzenie (pendrive) zaszyfrowane ww. metodą jest nadal w pełni funkcjonalne, sam proces szyfrowania jest bardzo krótki (parę minut), a dodatkowo podłączanie do komputera ogranicza się do włożenia urządzenia do portu USB, oraz wpisania hasła w wyskakującym okienku. Po wyciagnięciu urządzenia, pendrive jest w 100% zaszyfrowany, co uchroni organizację przez utratą poufności danych.

ETAP II: PROCES PIERWSZEGO SZYFROWANIA

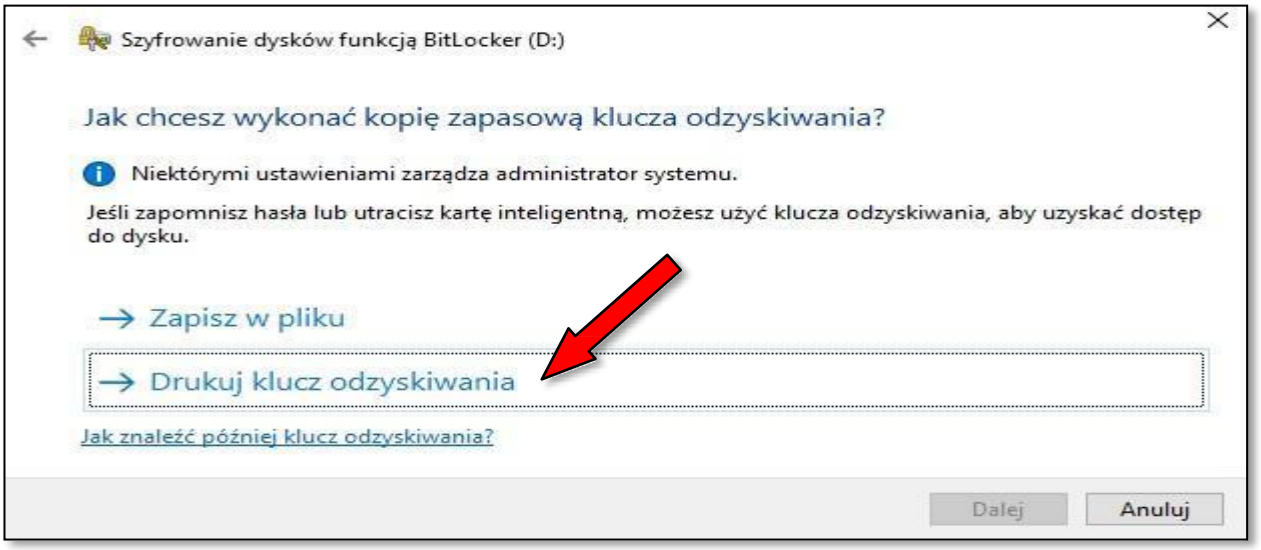
1. Włóż pendrive do jakiegokolwiek portu USB w komputerze z zainstalowanym systemem operacyjnym wymienionym w punkcie I-3.
2. Wejdź do „**Eksplorator plików**" oraz klikając prawym przyciskiem myszy na ikonkę pendrive'a który chcemy zaszyfrować rozwiń podręczne menu. Następnie kliknij „**Włącz funkcję BitLocker**":



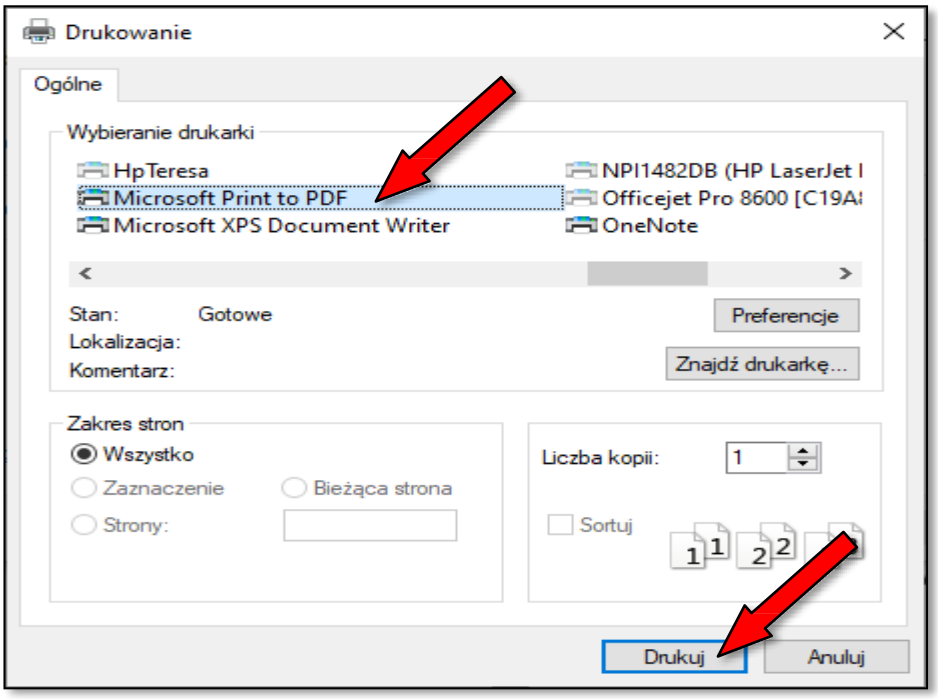
3. Zaznacz: „**Użyj hasła w celu odblokowania dysku**" oraz wpisz dwukrotnie hasło. Następnie kliknij „**Dalej**".



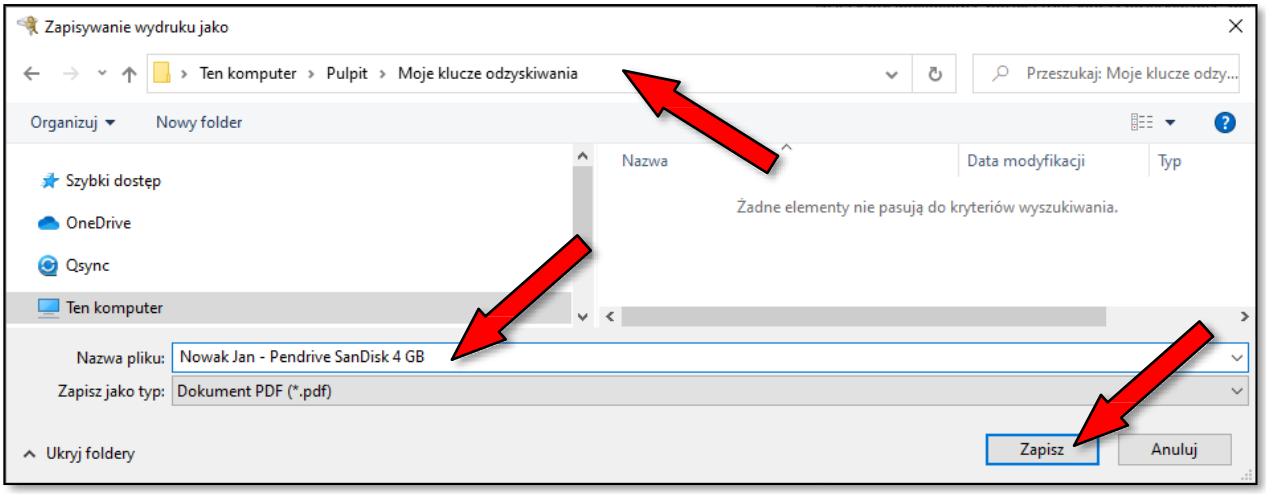
4. Teraz pojawi się okno, w którym wybierasz, gdzie zapisać klucz odzyskiwania (jest on potrzebny, gdy pracownik zapomni hasła, lub je zmieni bez wiedzy pracodawcy). Jeżeli wybierzesz opcję „**Zapisz w pliku**", to będzie potrzebny dodatkowy pendrive (na dysku twardym komputera, lub docelowo szyfrowanym pendrive nie można zapisać klucza). Zaleca się zaznaczyć/kliknąć: „**Drukuj klucz odzyskiwania**":



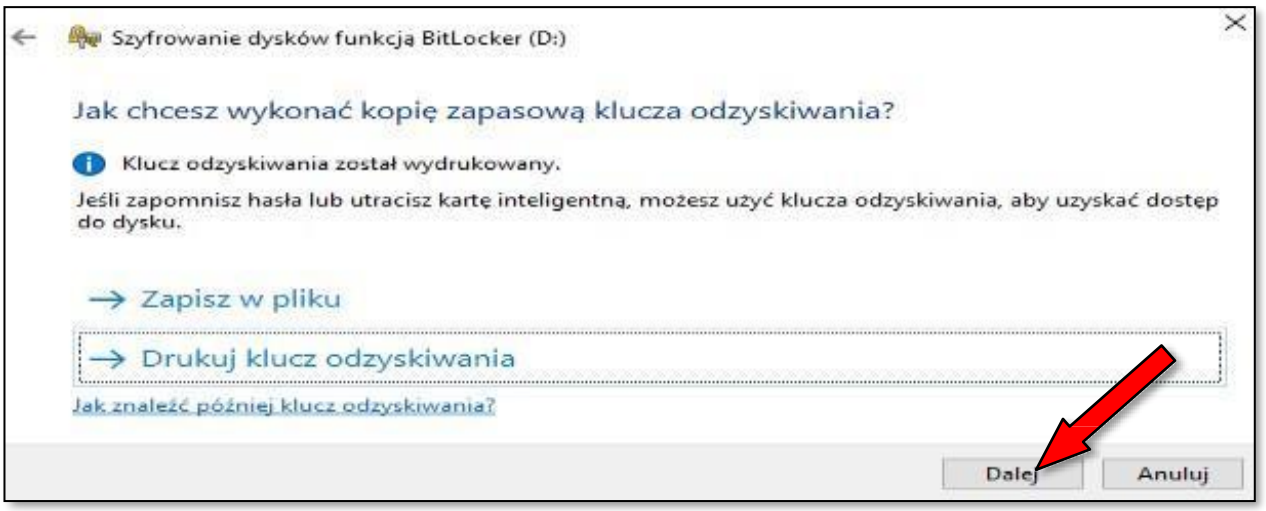
5. Następnie pojawi się okno „Drukowanie". W nim możesz wybrać, czy chcesz wydrukować zapasowy klucz odzyskiwania lub „wirtualnie" wydrukować do pliku PDF (czyli zapisać do PDF na dysku komputera). Większość systemów operacyjnych Windows ma takową funkcję pod postacią wirtualnej drukarki o nazwie: „Microsoft Print to PDF". Jeśli takiej nie masz, proponuje się zainstalować na komputerze darmową „drukarkę PDF" o nazwie PDF Creator (aby pobrać program, kliknij: link). Czyli zaznaczamy wirtualną drukarkę, w tym wypadku wbudowaną w system operacyjny Windows pod postacią „**Microsoft Print to PDF**" i klikasz „**Drukuj**".



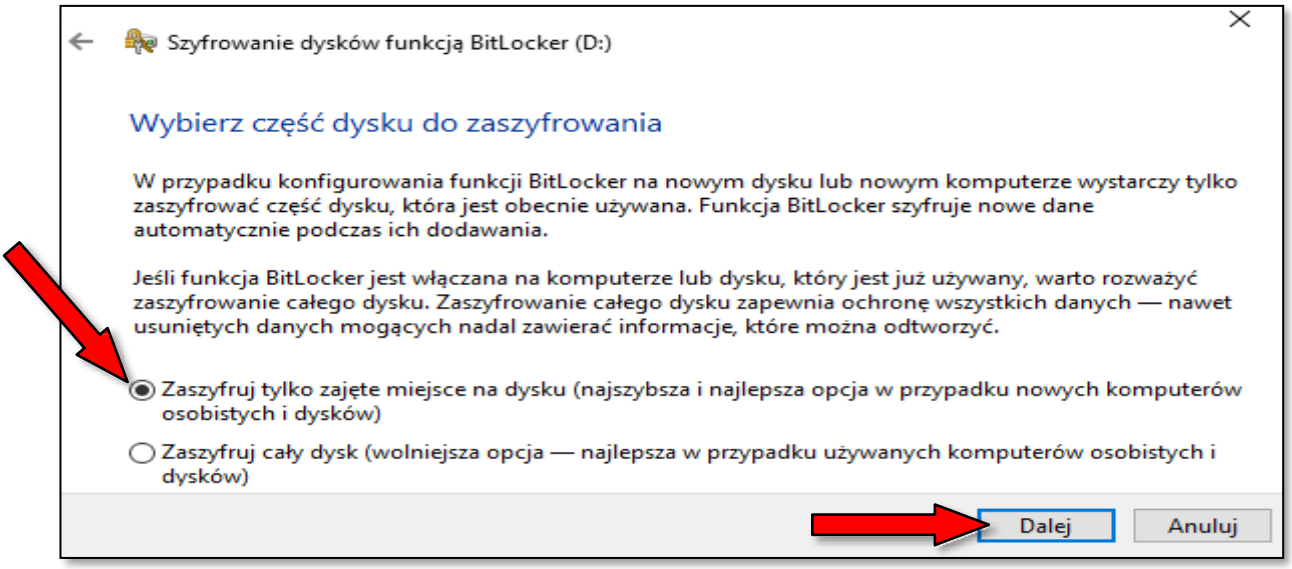
6. Teraz pojawi się okno, w którym powinieneś wybrać, gdzie chcesz zapisać wydruk klucza na komputerze (bądź innym urządzeniu zewnętrznym), nadajesz mu nazwę (najlepiej z nazwą użytkownika i urządzenia) oraz klikasz „**Zapisz**"



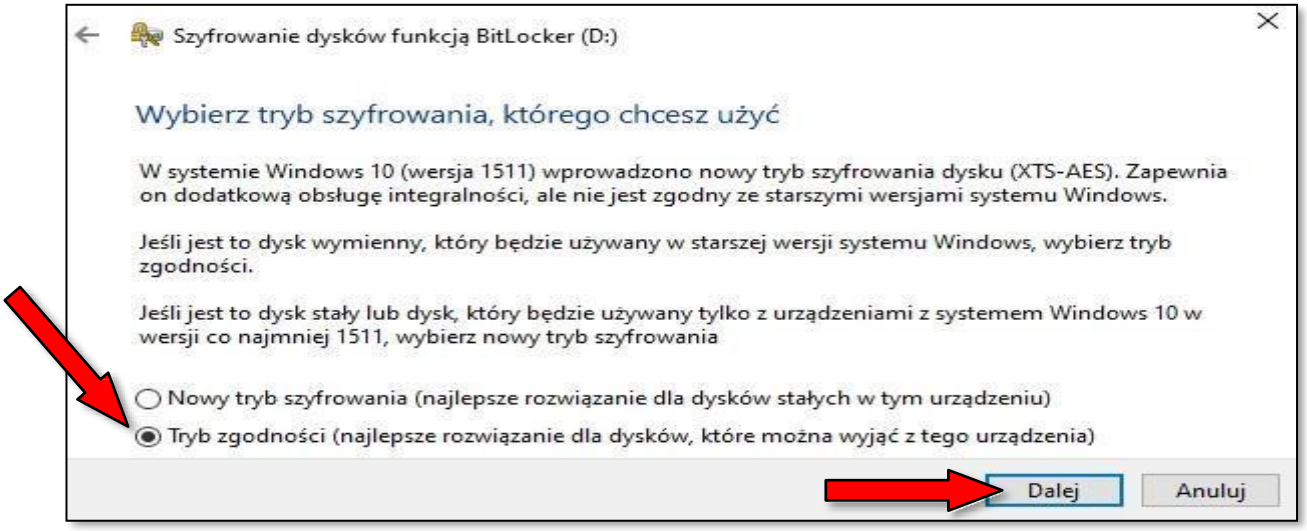
7. Ponownie pojawi się poniższe okno, w którym klikasz „**Dalej**":



8. Na tym etapie wybierasz zakres szyfrowania tj. czy cały dysk, czy zapisaną część. Wszystko zależy, ile masz czasu, jednakże opcja „Zaszyfruj tylko zajęte miejsce na dysku…" jest wystarczająca. Każdy nowy plik dodany do pamięci pendrive'a będzie automatycznie szyfrowany. Zaleca się zaznaczenie poniższej opcji oraz kliknięcie „**Dalej**":

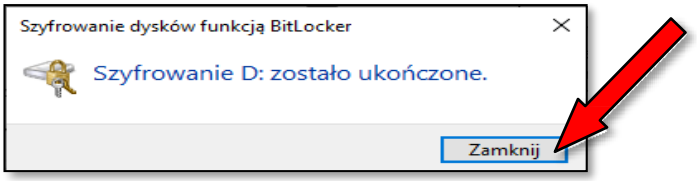


9. Teraz zaleca się zaznaczyć opcję: „**Tryb zgodności**" aby szyfrowany pendrive był kompatybilny ze starszymi wersjami systemu operacyjnego Windows, a następnie kliknąć „**Dalej**":



10. Kliknij „**Rozpocznij szyfrowanie**":

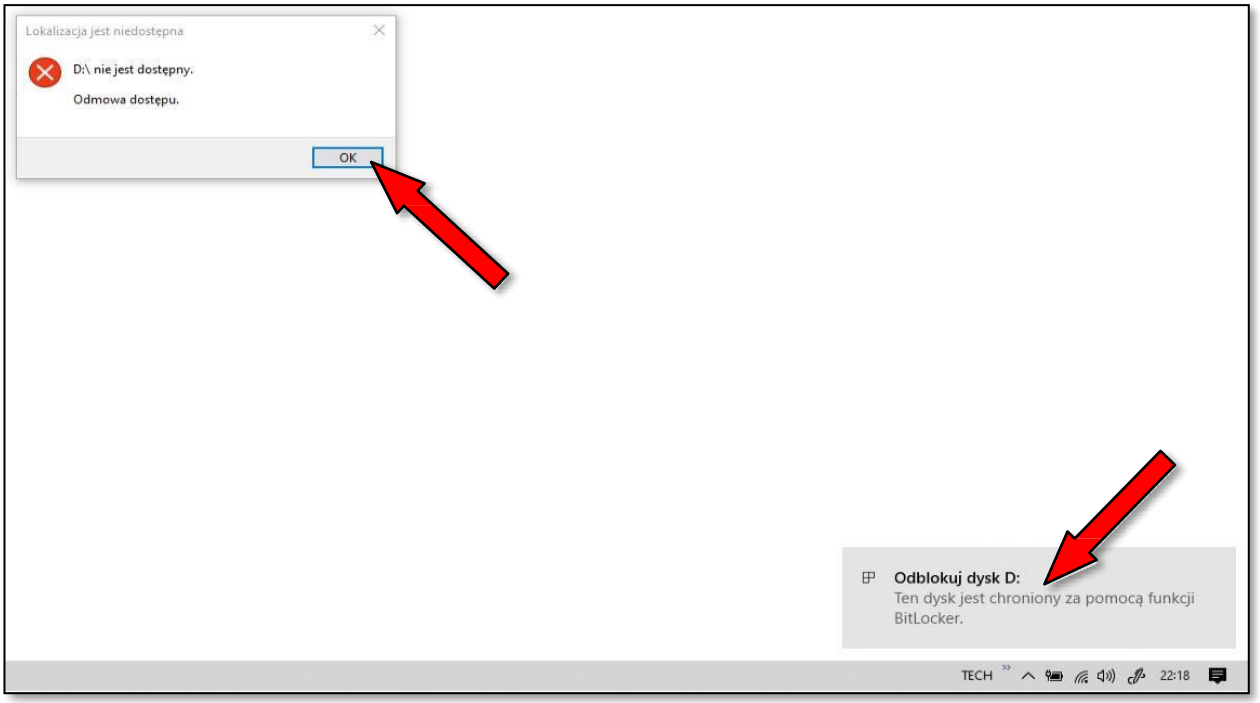
11. Poczekaj, aż szyfrowanie się dokończy i kliknij „**Zakończ**":



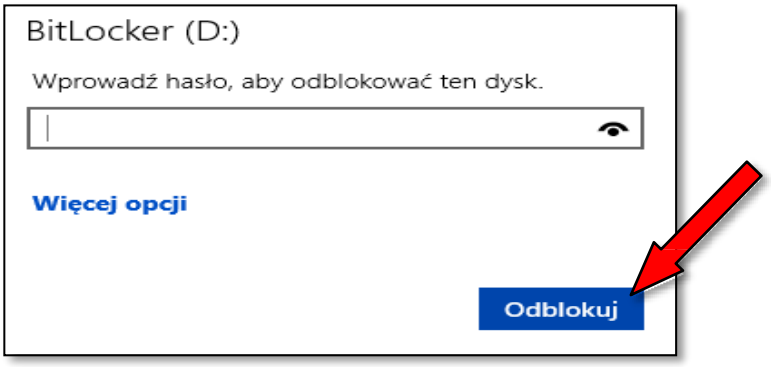
12. Teraz możesz odłączyć pendrive'a i ponownie włożyć do portu USB. System poprosi Cię o hasło.
13. Pamiętaj, aby trzymać „**klucze odzyskiwania**" w wydzielonym miejscu na komputerze lub innymurządzeniu..

ETAP III: UŻYTKOWANIE ZASZYFROWANEGO PENDRIVE'A

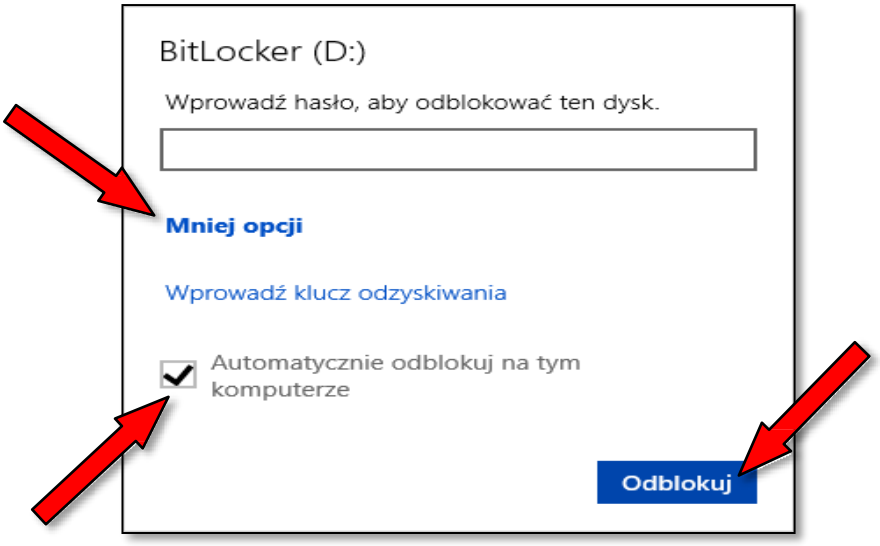
1. Za każdym razem, gdy podłączasz zaszyfrowany pendrive do komputera zostaniesz poproszony o wpisanie hasła. W Windowsie 10 będzie to taki komunikat o niedostępności danego pendrive'a/urządzenia oraz okienko „**Odblokuj dysk …**". Kliknij „**OK**" oraz „**Odblokuj dysk …"**



2. Teraz pojawi się okienko z możliwością podania Twojego hasła. Wpisz je i kliknij „**Odblokuj**":

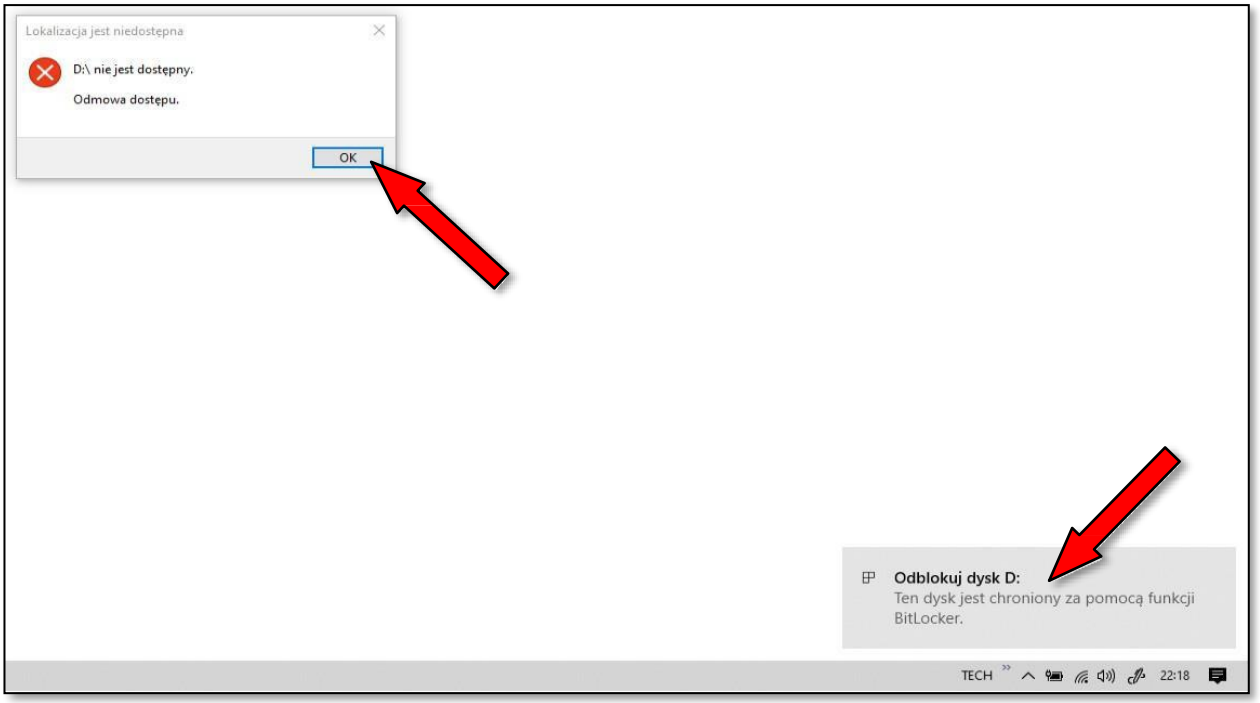


3. Jest jeszcze szerszy zakres dostępu do pendrive'a poprzez kliknięcie „**Więcej opcji**". W tym momencie masz możliwość wpisania „Klucza odzyskiwania", który powinien posiadać TYLKO Administrator organizacji (np. w przypadku zapomnienia/zmiany hasła przez użytkownika). Dodatkowo można zaznaczyć, aby na danym komputerze, pendrive został zapamiętany, aby w przyszłości nie trzeba było za każdym razem wpisywać hasła:

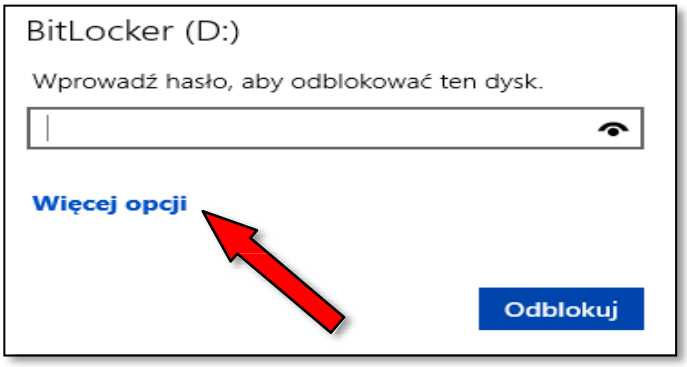


ETAP IV: ODZYSKIWANIE PENDRIVE'A POPRZEZ „KLUCZ ODZYSKIWANIA"

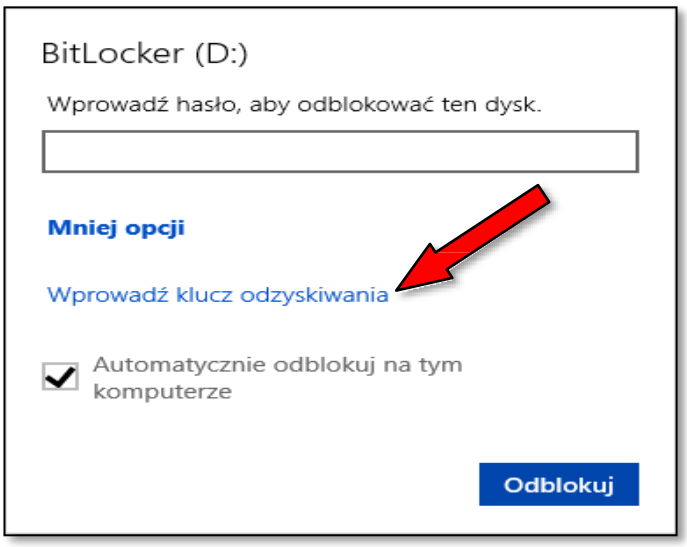
1. W przypadku, gdy użytkownik zapomni hasło, bądź je zmieni możesz uzyskać dostęp do pamięci pendrive'a. W tym celu podłącz zaszyfrowany pendrive do komputera. Następnie pojawi komunikat o niedostępności danego pendrive'a/urządzenia oraz okienko „**Odblokuj dysk …**". Kliknij „**OK**" oraz „**Odblokuj dysk …**":



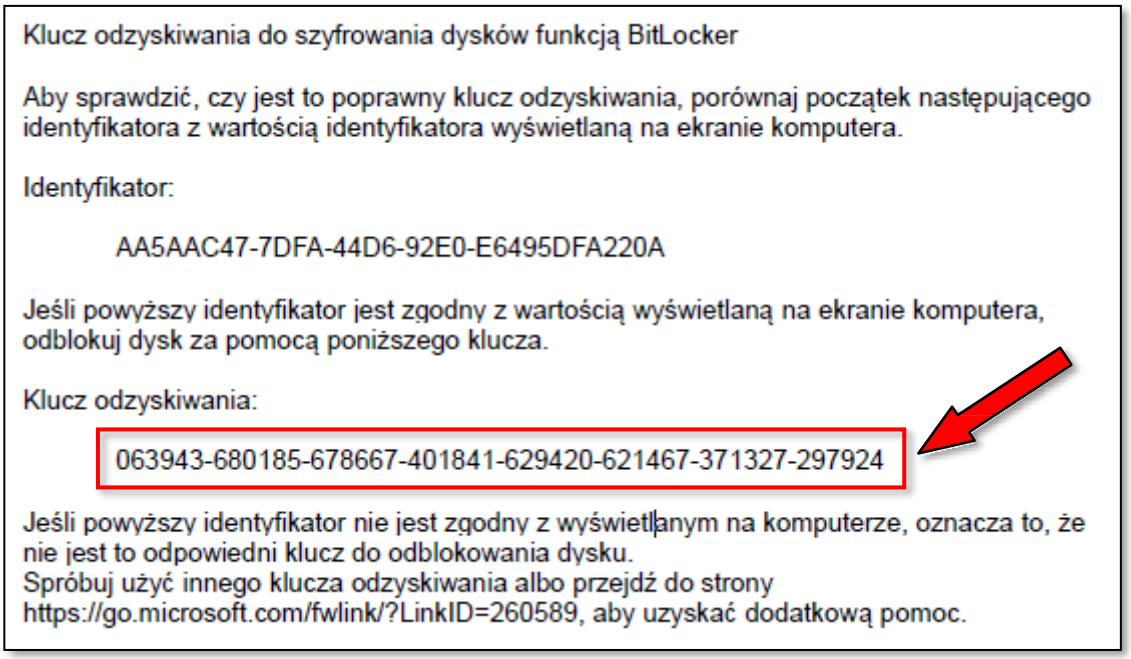
2. Teraz pojawi się okienko z możliwością podania hasła, które ktoś zapomniał, lub zmienił. Kliknij „**Więcej opcji**":



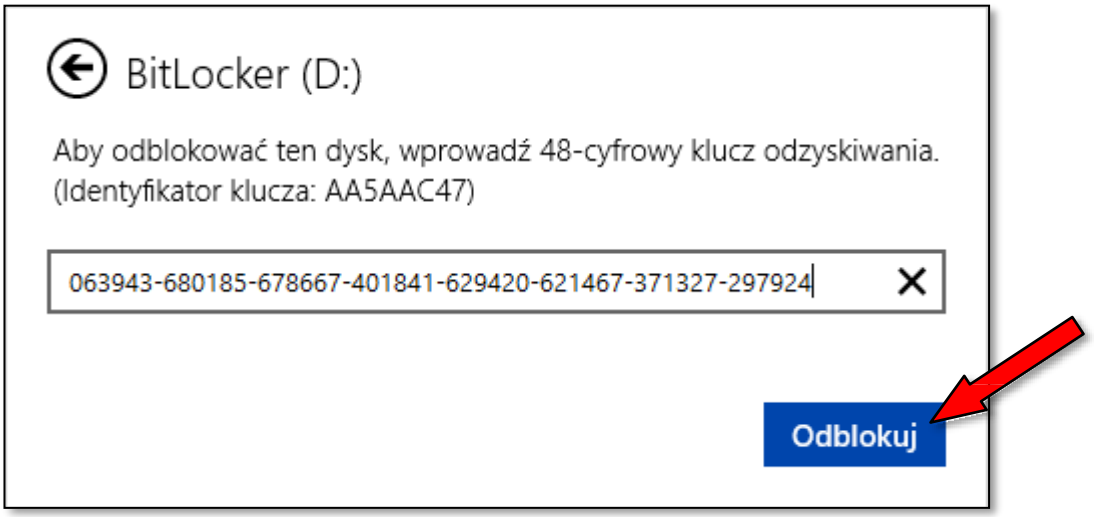
3. Następnie pojawi się okienko, w którym kliknij: „**Wprowadź klucz odzyskiwania**":



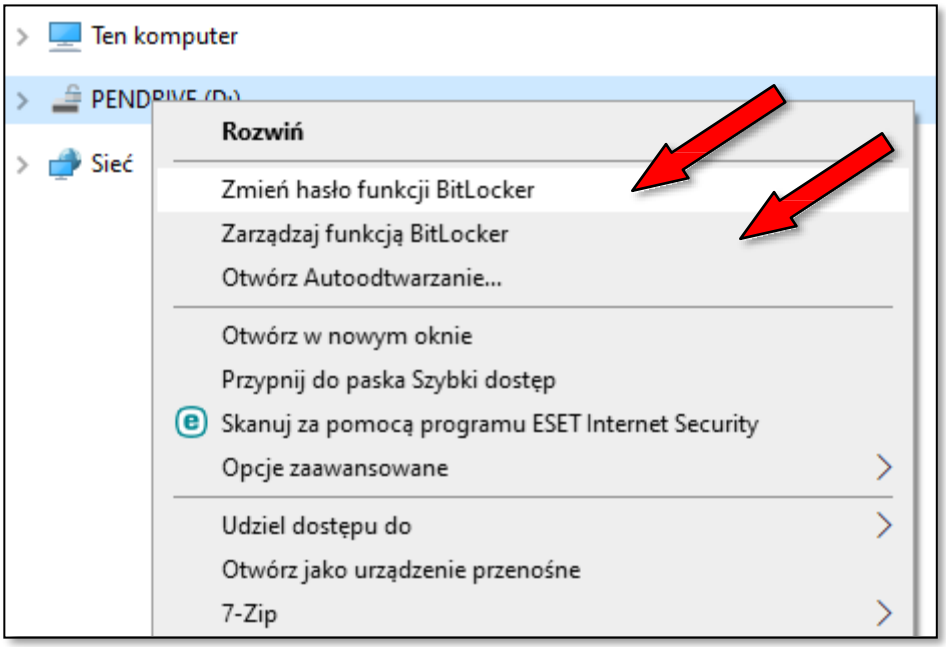
4. Teraz znajdź swój wcześniej zapisany w pliku PDF na komputerze lub innym urządzeniu klucz odzyskiwania, składający się z 48 znaków. Na potrzeby tegoż poradnika takowy plik z kluczem został wygenerowany i zawiera przykładową następującą treść:



5. Skopiuj ten klucz (zaznacz klucz → wciśnij kombinację znaków „**Ctrl+C**" oraz wklej do poniższego okna (kombinacja klawiszy „**Ctrl+V**", a następnie kliknij „**Odblokuj**"



6. Od tego momentu masz dostęp do danych na pednrive. Możesz wyłączyć szyfrowanie, bądź zmienić hasło, poprzez kliknięcie prawym przyciskiem myszy (rozwijając podręczne menu) na ikonce pendrive'a:



BEZPIECZNE KORZYSTANIE Z PRZEGLĄDARKI INTERNETOWEJ (Instrukcja użytkowania oprogramowania)

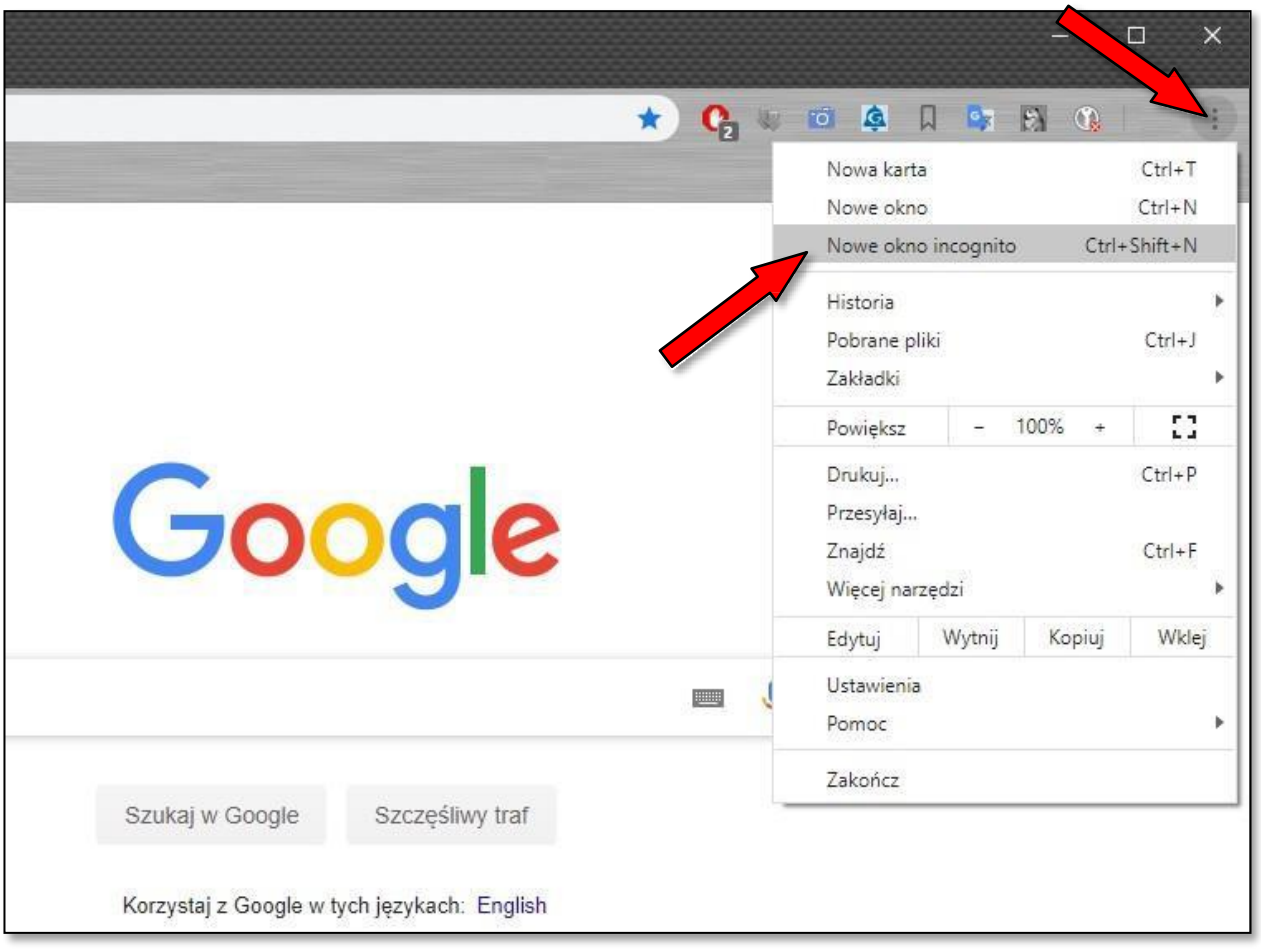
NAZWA OPROGRAMOWANIA:	*Przeglądarki internetowe:* *Chrome | Firefox | Opera | Safari | Internet Explorer | Microsoft Edge*
ZAKRES INSTRUKCJI:	*Wstęp i wykaz przeglądarek internetowych; Instrukcja bezpiecznego korzystania z wybranej przeglądarki internetowej*

ETAP I: WSTĘP I WYKAZ PRZEGLĄDAREK INTERNETOWYCH

1. W obecnych czasach jako administratorzy i użytkownicy sprzętu komputerowego używamy wielorakich przeglądarek internetowych. Niniejsza instrukcja ma na celu ograniczenie ryzyka w zakresie poufności danych podczas korzystania z dostępu do sieci www za pośrednictwem przeglądarki internetowej. Umożliwia:
   - **a)** brak zapisu „ciasteczek cookies”,
   - **b)** brak zapisu loginów i haseł,
   - **c)** brak zapisywania danych z auto-formularzy i wiele innych.
2. Wyróżniamy następujące a jednocześnie najczęściej używane przeglądarki internetowe:
   - **a)** Chrome,
   - **b)** Firefox,
   - **c)** Opera,
   - **d)** Safari,
   - **e)** Internet Explorer,
   - **f)** Microsoft Edge.

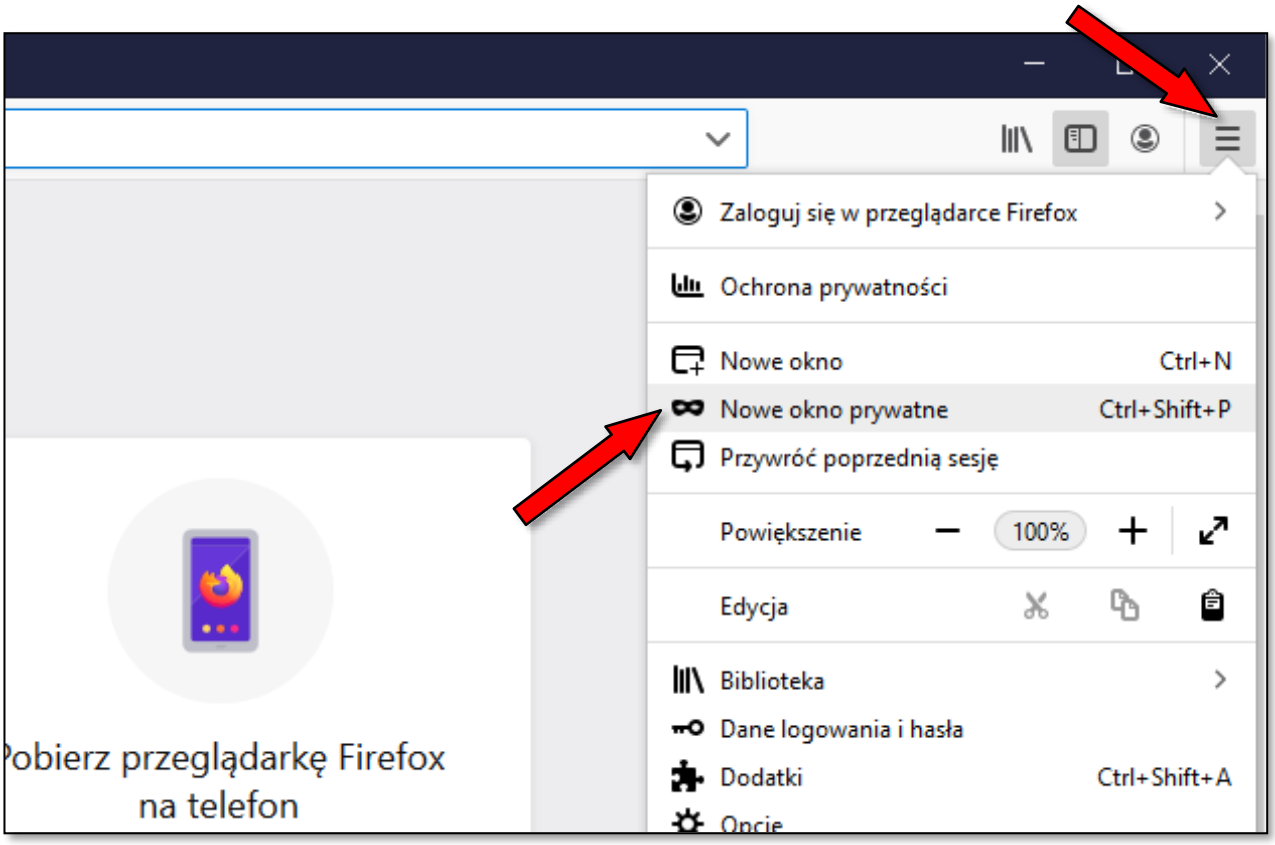
ETAP II-A: INSTRUKCJA BEZPIECZNEGO KORZYSTANIA PRZEGLĄDARKI CHROME

1. Po uruchomieniu przeglądarki Chrome kliknij w prawym górnym rogu przycisk z trzema kropkami (menu przeglądarki) a następnie kliknij „**Nowe okno incognito**”:



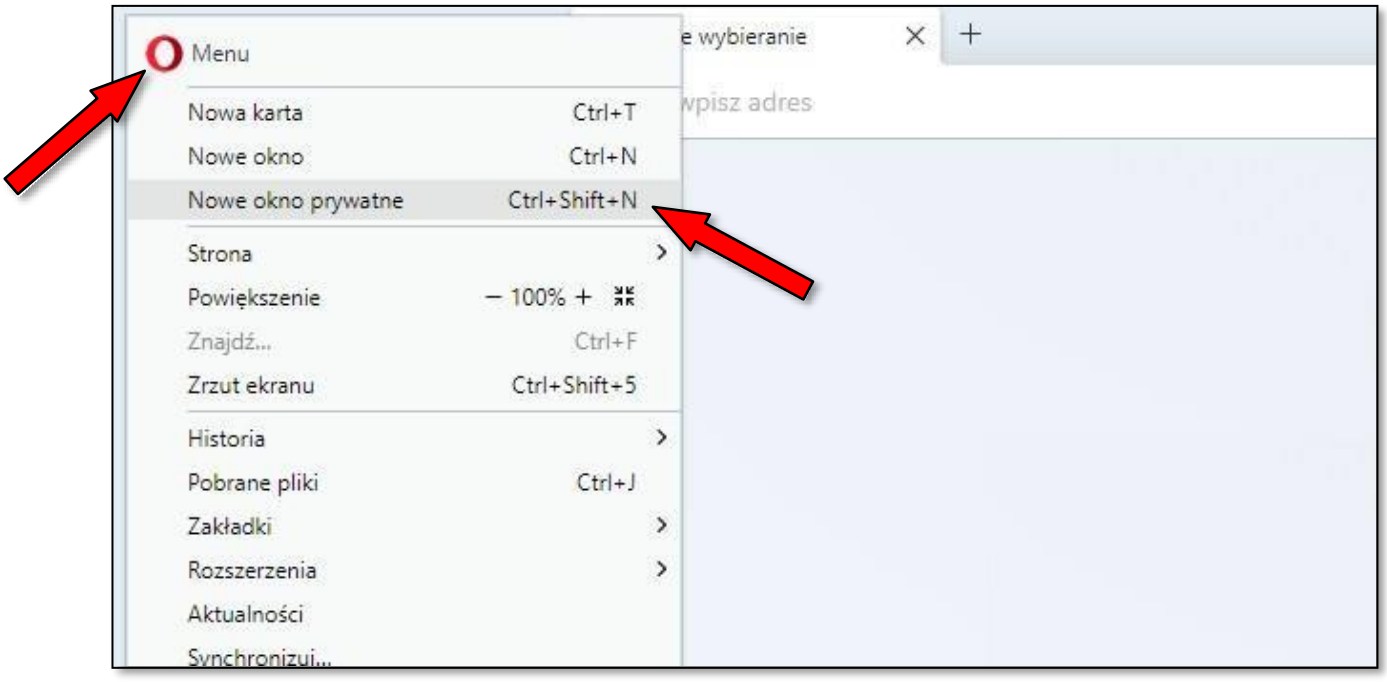
ETAP II-B: INSTRUKCJA BEZPIECZNEGO KORZYSTANIA PRZEGLĄDARKI FIREFOX

1. Po uruchomieniu przeglądarki Firefox kliknij w prawym górnym rogu przycisk z trzema kreskami (menu przeglądarki) a następnie kliknij „**Nowe okno prywatne**”:



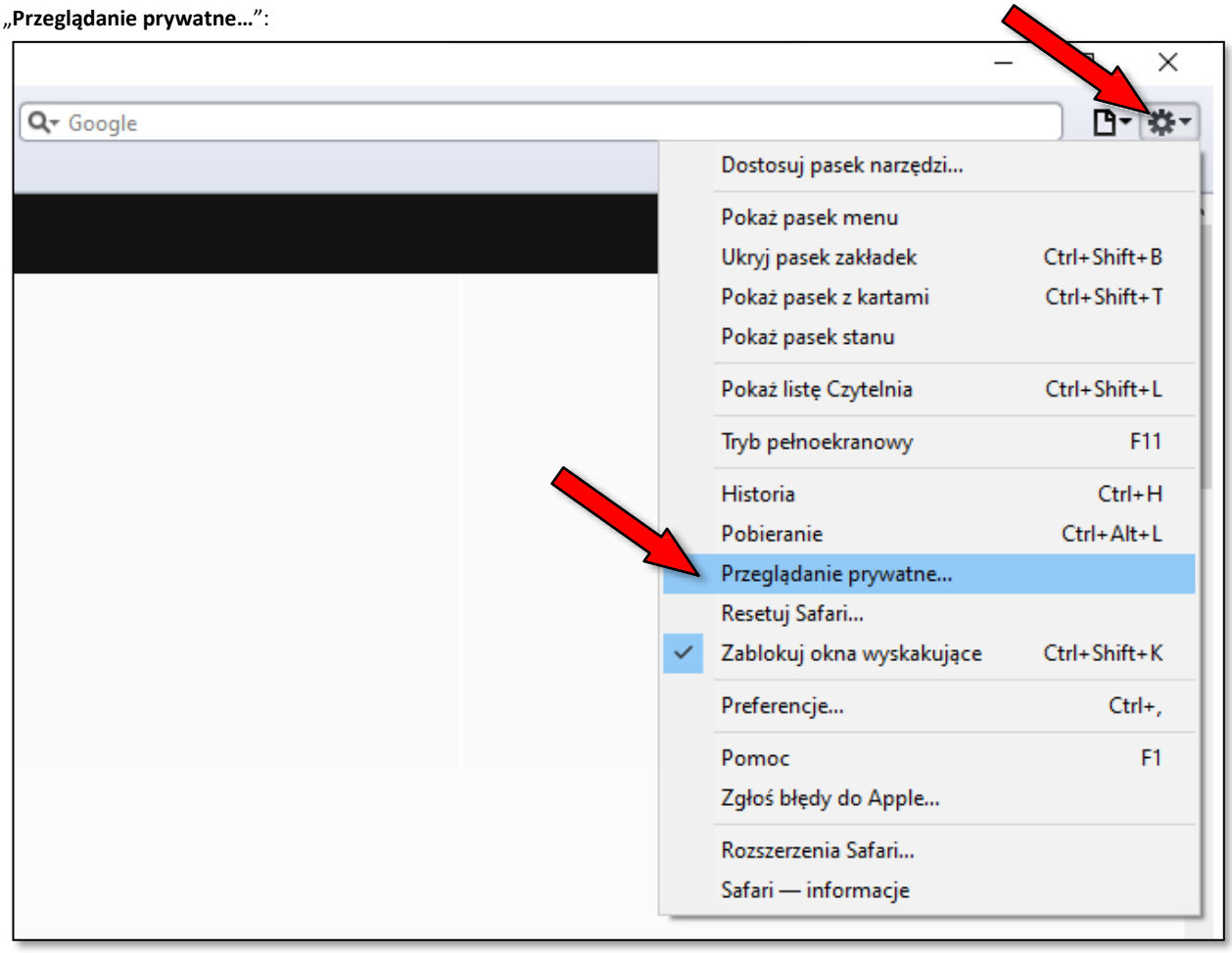
ETAP II-C: INSTRUKCJA BEZPIECZNEGO KORZYSTANIA PRZEGLĄDARKI OPERA

1. Po uruchomieniu przeglądarki Opera kliknij w lewym górnym rogu przycisk z z literą „**O**” (menu przeglądarki) a następnie kliknij „**Nowe okno prywatne**”:



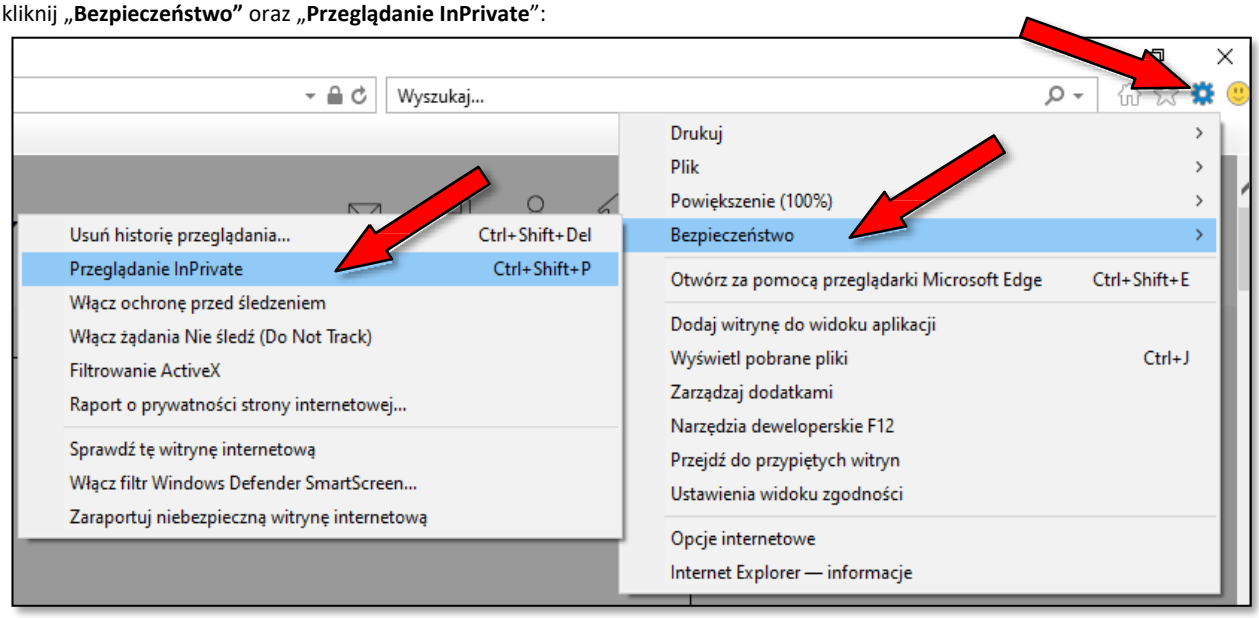
ETAP II-D: INSTRUKCJA BEZPIECZNEGO KORZYSTANIA PRZEGLĄDARKI SAFARI

1. Po uruchomieniu przeglądarki Safari kliknij w prawym górnym rogu przycisk „**zębatki**” (menu przeglądarki) a następnie kliknij „**Przeglądanie prywatne…**”:



ETAP II-E: INSTRUKCJA BEZPIECZNEGO KORZYSTANIA Z PRZEGLĄDARKI INTERNET EXPLORER

1. Po uruchomieniu przeglądarki Internet Explorer kliknij w prawym górnym rogu przycisk „**zębatki**” (menu przeglądarki), następnie kliknij „**Bezpieczeństwo”** oraz „**Przeglądanie InPrivate**”:



ETAP II-F: INSTRUKCJA BEZPIECZNEGO KORZYSTANIA Z PRZEGLĄDARKI MICROSOFT EDGE

1. Po uruchomieniu przeglądarki Microsoft Edge kliknij w prawym górnym rogu przycisk z trzema kropkami (menu przeglądarki), a następnie kliknij „**Nowe okno InPrivate**”: