# **Instrukcja przesyłania wiadomości e-mail z informacjami chronionymi w POSTACI ZAŁĄCZNIKÓW szyfrowanych z wykorzystaniem oprogramowania 7zip**

Rys 1



Rys. 2



Rys. 3



Wymagana zainstalowana aplikacja 7zip na komputerze użytkownika. W przypadku braku oprogramowania 7zip skontaktuj się z działem IT: Centrum Informatycznym UMW

* W celu przesłania załącznika zawierającego informacje chronione poza UMW za pomocą poczty e-mail należy przygotować pliki, które będą przesyłane umieszczając je w jednym folderze:
	+ Kliknij prawym klawiszem myszy na folderze (lub zaznaczonych plikach w folderze) zawierającym pliki do wysłania, a następnie z menu kontekstowego wybierz 7zip – Dodaj do archiwum (Rys. 1);
	+ W nowym oknie należy wybrać format archiwum (np. zip), a następnie w odpowiednie pola sekcji Szyfrowanie wpisać hasło zabezpieczające i wybrać metodę szyfrowania AES256, po czym kliknąć OK (Rys. 2).
* W przypadku braku programu 7zip w menu kontekstowym zgodnie z Rys.1, należy odnaleźć program 7zip na liście zainstalowanych programów w menu Start – Programy i uruchomić go. Po uruchomieniu programu należy odnaleźć i wskazać folder zawierający pliki do wysłania i kliknąć ikonę "+ Dodaj" (Rys. 3), a następnie postępować zgodnie z Rys.2.
* Utwórz wiadomość i przygotuj ją do wysłania wypełniając niezbędne pola i upewniając się, że wszelkie dane, ze szczególnym uwzględnieniem adresu e-mail adresata, zostały uzupełnione poprawnie.
* Dodaj zaszyfrowane dane w postaci załącznika do wiadomości e-mail.

Zasady tworzenia haseł:

* hasło powinno się składać z minimum 8 znaków,
* hasło musi spełniać warunek złożoności polegający na występowaniu w nim: wielkiej i małej litery, oraz cyfry i znaku specjalnego (np. !@#),
* kolejne używane hasła muszą być różne,
* zabrania się udostępniania haseł innym osobom niż wskazane do dostępu do zabezpieczonych plików.
* Zabrania się tworzenia haseł na podstawie:
	+ cech i numerów osobistych (np. dat urodzenia, imion itp.),
	+ sekwencji klawiszy klawiatury (np. qwerty, 12qwaszx),
	+ identyfikatora użytkownika,
	+ zabrania się tworzenia haseł łatwych do odgadnięcia.

Zasady przekazywania haseł odbiory wiadomości:

* Hasło powinno zostać przekazane innym kanałem komunikacji:
	+ wiadomość SMS;
	+ telefonicznie;
	+ osobiście;
	+ przesłanie wiadomości na inny adres e-mail odbiorcy niż wskazany w wiadomości z informacjami chronionymi.
* W przypadku braku dostępności powyższych kanałów komunikacji w sytuacjach wyjątkowych hasło do odszyfrowania plików może zostać przesłane na ten sam adres co wskazany w wiadomości z informacjami chronionymi, ale w osobnej wiadomości e-mail.