

Zarządzenie nr 17/2019/2020

Dyrektora Szkoły Podstawowej im. K.I.Gałczyńskiego w Węgorzynie z dnia 16 kwietnia 2020 r.

w sprawie wprowadzenia Instrukcji stosowania w Szkole Podstawowej im. K. I. Gałczyńskiego w Węgorzynie środków zabezpieczających dane osobowe, w szczególności przesyłanych pocztą elektroniczną w postaci szyfrowania danych.

Na podstawie art. 68 ustawy z dnia 14 grudnia 2016 r. – Prawo Oświatowe (Dz. U. 2019 poz. 1148 z późn. zm.) i Statutu Szkoły Podstawowej im. K.I.Gałczyńskiego w Węgorzynie zarządza się co następuje:

§ 1

Wprowadza się Instrukcję stosowania w Szkole Podstawowej im. K. I. Gałczyńskiego w Węgorzynie środków zabezpieczających dane osobowe, w szczególności przesyłanych pocztą elektroniczną w postaci szyfrowania danych.

§ 2

Zarządzenie wchodzi w życie z dniem podpisania.

DYREKTOR
Szkoły Podstawowej
im. K.I. Gałczyńskiego w Węgorzynie
Ewa Adamów
mgr Ewa Adamów

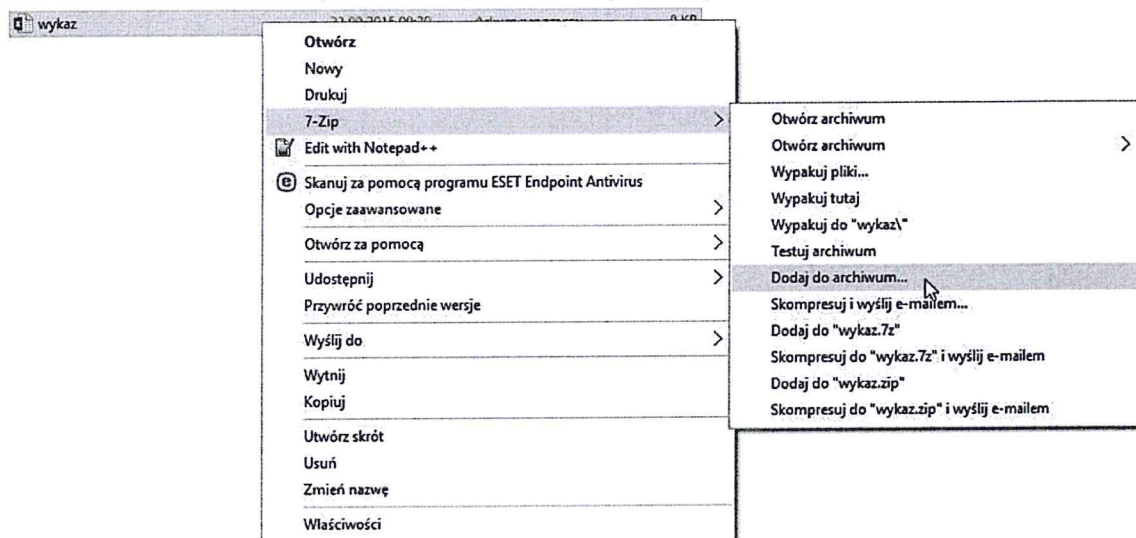
Instrukcja stosowania w Szkole Podstawowej im. K. I. Gałczyńskiego w Węgorzynie środków zabezpieczających dane osobowe, w szczególności przesyłanych pocztą elektroniczną w postaci szyfrowania danych.

1. Przesyłanie danych osobowych z użyciem e-maila poza Szkołą może odbywać się tylko przez osoby do tego upoważnione.
2. W przypadku przesyłania informacji zawierających dane osobowe, w tym dane wrażliwe poza organizację należy wykorzystywać mechanizmy kryptograficzne (hasłowanie wysyłanych plików, podpis elektroniczny).
3. W przypadku zabezpieczenia plików hasłem, obowiązuje minimum 5 znaków. Ustalone hasło nadawca przekazuje adresatowi telefonicznie lub SMS-em.
4. Użytkownicy powinni zwracać szczególną uwagę na poprawność adresu odbiorcy dokumentu.
5. Zaleca się, aby użytkownik podczas przesyłania danych osobowych e-mailem zawarł w treści prośbę o potwierdzenie otrzymania i zapoznania się z informacją przez adresata.
6. Nie należy otwierać załączników (plików) w e-mailach nadesłanych przez nieznanego nadawcę lub podejrzanych załączników nadanych przez znanego nadawcę.
7. Nie należy otwierać stron internetowych wskazanych hiperlinkami w mailach, gdyż mogą to być hiperlinki do stron zainfekowanych lub niebezpiecznych.
8. Nie należy uruchamiać „makr” w przesyłanych dokumentach.
9. Należy zwrócić szczególną uwagę na adres e-mail nadawcy – fałszywy e-mail zazwyczaj posiada podejrzanego, nieoczekiwanego nadawcę.
10. Jeżeli z treści e-maila wynika, że została przesłana z firmy XXX zawierająca załączniki lub hiperłącza, upewnij się, czy faktycznie wiadomość pochodzi z firmy XXX.
11. Ewentualne faktury przesyłane drogą elektroniczną odbierane są tylko przez np. Pracownika ds. Administracji Szkoły.
12. Do zmiany haseł, blokowania dostępu do poczty e-mail Szkoły skrzynek uprawniony jest tylko i wyłącznie ASI.
13. Użytkownicy nie powinni rozsyłać za pośrednictwem maila informacji o zagrożeniach dla systemu informatycznego, „łańcuszków szczęścia”, itp.
14. Użytkownicy nie powinni rozsyłać, e-maili zawierających załączniki o dużym rozmiarze.
15. Użytkownicy powinni okresowo kasować niepotrzebne e-maile.
16. Podczas wysyłania maili do wielu adresatów jednocześnie, należy użyć metody „Ukryte do wiadomości – UDW”.
17. E-Mail jest przeznaczony wyłącznie do wykonywania obowiązków służbowych.

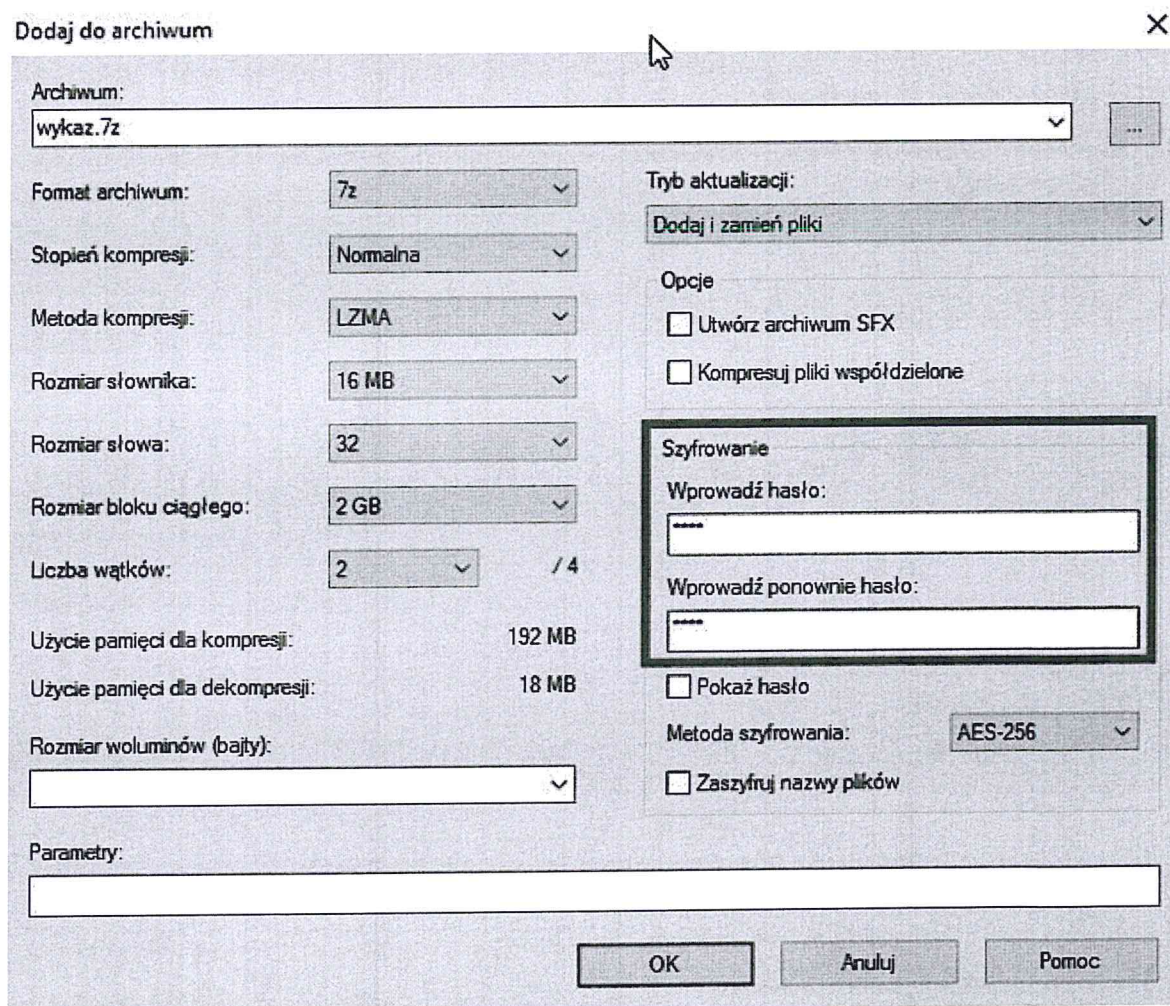
18. Przy korzystaniu z e-maila, Użytkownicy mają obowiązek przestrzegać prawa własności przemysłowej i prawa autorskiego.
19. Użytkownicy nie mają prawa korzystać z maila w celu rozpowszechniania treści o charakterze obraźliwym, niemoralnym lub niestosownym wobec powszechnie obowiązujących zasad postępowania.
20. Użytkownik bez zgody Pracodawcy nie ma prawa wysyłać wiadomości zawierających dane osobowe dotyczące Pracodawcy, jego pracowników, uczniów, rodziców, klientów, dostawców lub kontrahentów za pośrednictwem Internetu, w tym przy użyciu prywatnej elektronicznej skrzynki pocztowej.

Instrukcja szyfrowania pliku/katalogu programem 7-zip

1. Należy kliknąć prawym przyciskiem myszy na plik lub katalog i wybrać opcję 7-zip -> Dodaj do archiwum. Przykład na poniższym rysunku:



2. Następnie w okienku „Dodaj do archiwum” w polu „Wprowadź hasło:” wpisujemy hasło, którym chcemy zaszyfrować plik lub katalog. W polu „Wprowadź ponownie hasło:” ponownie wpisujemy hasło w celu weryfikacji poprawności wpisanego hasła. Przykład na poniższym rysunku:

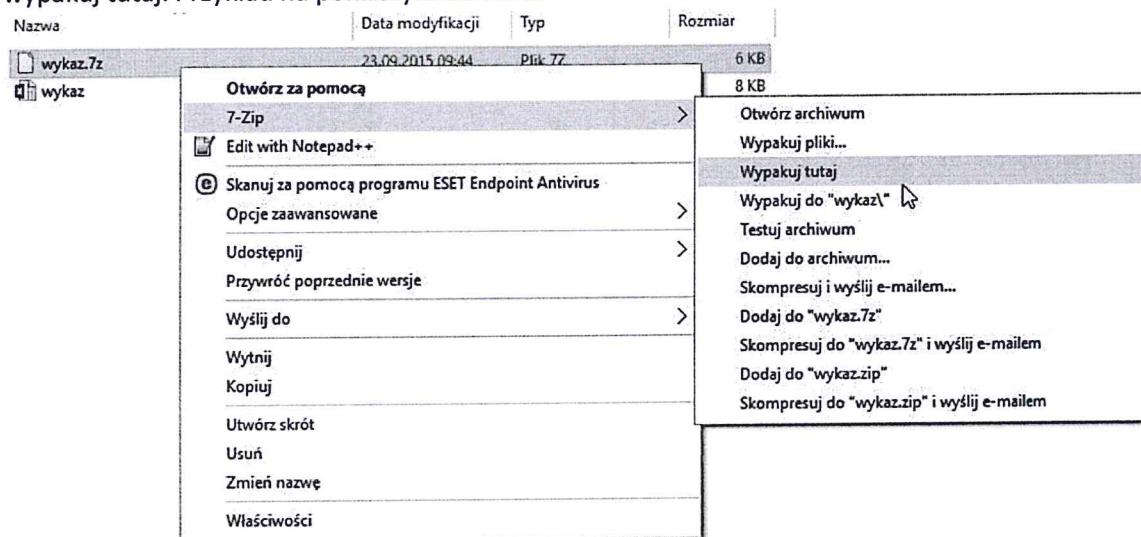


3. W wyniku szyfrowania otrzymujemy plik o rozszerzeniu .7z, który można bezpiecznie przestać e-mailem jak normalny załącznik.

Nazwa	Data modyfikacji	Typ	Rozmiar
wykaz.7z	23.09.2015 09:44	Plik 7Z	6 KB
wykaz	23.09.2015 09:29	Arkusz programu ...	8 KB

Instrukcja odszyfrowania pliku/katalogu programem 7-zip

1. Zaszzyfrowany załącznik w wiadomości e-mail należy zapisać na komputerze.
2. Na zaszzyfrowanym pliku należy kliknąć prawym przyciskiem myszy i wybrać opcję 7 zip -> wypakuj tutaj. Przykład na poniższym obrazku:



3. Następnie w okienku wpisujemy hasło do archiwum. Przykład na poniższym obrazku:

