Szkoła Podstawowa z Oddziałami Integracyjnymi nr 343
im. Matki Teresy z Kalkuty w Warszawie
ul. Kopcińskiego 7, 02-777 Warszawa
tel./fax: 22 643 84 54, e-mail: sp343@edu.um.warszawa.pl

SP343.021.112.2020.D

ZARZĄDZENIE NR 56 / 2020
DYREKTORA SZKOŁY PODSTAWOWEJ Z ODDZIAŁAMI INTEGRACYJNYMI NR 343 IM. MATKI TERESY Z KALKUTY W WARSZAWIE
z dnia 12 października 2020 roku

w sprawie zasad bezpiecznego korzystania z technologii informacyjno – komunikacyjnych w zakresie ochrony danych osobowych

Na podstawie Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu tych danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych osobowych) zarządza się, co następuje:

§ 1

Wprowadza się *Zasady bezpiecznego korzystania z technologii informacyjno – komunikacyjnych w zakresie ochrony danych osobowych podczas nauki zdalnej,* obowiązujących w Szkole Podstawowej z Oddziałami Integracyjnymi nr 343 im. Matki Teresy z Kalkuty w Warszawie, stanowiące załącznik nr 1 do niniejszego zarządzenia.

§ 2

Zarządzenie wchodzi w życie z dniem ogłoszenia.

DYREKTOR SZKOŁY
mgr Jolanta Kubalska

załącznik nr 1
do zarządzenia nr 56/2020
dyrektora SP 343

Zasady bezpiecznego korzystania z technologii informacyjno - komunikacyjnych (w zakresie ochrony danych osobowych) podczas nauki zdalnej obowiązujące w Szkole Podstawowej z Oddziałami Integracyjnymi nr 343 im. Matki Teresy z Kalkuty w Warszawie

1. Za bezpieczeństwo danych osobowych, których Administratorem jest Szkoła Podstawowa z Oddziałami Integracyjnymi nr 343 w Warszawie, odpowiedzialni są wszyscy pracownicy.
2. Pracownicy odpowiadają w szczególności za:
   1) przestrzeganie zasad bezpieczeństwa wynikających z *Polityki Bezpieczeństwa* w SP 343 oraz *Instrukcji zarządzania systemem informatycznym (IZSI)* służącym do przetwarzania danych osobowych;
   2) zgłaszanie incydentów i naruszeń, a także wykonywanie zaleceń IOD.

3. Zakres obowiązywania zasad bezpieczeństwa:
   1) niniejsze *Zasady* obowiązują wszystkich pracowników;
   2) każdy pracownik ma obowiązek zapoznania się z treścią niniejszego dokumentu;
   3) zasady dotyczą wyposażenia, systemów, urządzeń przetwarzających informacje w formie elektronicznej, papierowej lub jakiejkolwiek innej.
4. Użyte pojęcia w niniejszym dokumencie są wspólne z pojęciami określonymi w *Polityce Bezpieczeństwa Informacji* obowiązującej w SP 343.
5. W sytuacji wprowadzenia w SP 343 nauki w formie zdalnej lub hybrydowej częściowo zawieszeniu ulegają zapisy *Polityki Bezpieczeństwa Informacji* w SP 343 oraz *Instrukcji zarządzania systemem informatycznym (IZSI),* w zakresie zakazu wynoszenia dokumentów poza teren szkoły oraz zakazu korzystania z prywatnych urządzeń i sieci na potrzeby logowania się do systemów szkolnych.
6. Każda upoważniona przez ADO osoba, jest zobowiązana zachować szczególną ostrożność przy przetwarzaniu wszelkich danych chronionych.

7. Podstawowe zasady ochrony danych osobowych podczas pracy zdalnej:
   1) nie należy udostępniać osobom nieupoważnionym dokumentów z danymi osobowymi;
   2) nośniki informacji (w formie papierowej i elektronicznej) z danymi podlegającymi ochronie nie mogą zostać pozostawione w miejscach ogólnodostępnych i niezabezpieczonych;
   3) w przypadku pracy w pomieszczeniach, do których dostęp mają także osoby nieupoważnione (np. członek rodziny), pracownicy zobowiązani są stosować zasadę czystego biurka i ekranu - wszystkie dokumenty i materiały powinny być po zakończeniu pracy chowane w przeznaczonych do tego szufladach, szafkach itp. W przypadku braku dostatecznej ilości dostępnego miejsca dokumenty i materiały powinny być pozostawione na biurku uporządkowane;
   4) miejsca (np. szafy) przeznaczone do przechowywania danych chronionych muszą być zamykane na klucz. Klucze do tych miejsc posiadają tylko upoważnieni pracownicy. Miejsca z danymi są otwarte tylko na czas potrzebny na dostęp do danych, a następnie zostają zamknięte;
   5) dane chronione w formie papierowej mogą znajdować się w miejscach ogólnodostępnych (np. na biurkach) tylko w trakcie dokonywania czynności służbowych, a następnie muszą być przechowywane w miejscach przeznaczonych do tego celu (np. zamykana szafa);
   6) wydruki robocze zawierające informacje chronione, błędne lub zdezaktualizowane muszą być niezwłocznie bezpowrotnie niszczone przy użyciu niszczarki do papieru lub w inny sposób, zapewniający skuteczne ich usunięcie lub anonimizowanie.
8. Zasady bezpieczeństwa teleinformatycznego:
   1) obowiązuje bezwzględny wymóg instalacji oprogramowania antywirusowego na każdym stanowisku roboczym, zarówno na komputerach stacjonarnych, jak i przenośnych wykorzystywanych do przetwarzania danych;
   2) dostęp do komputerów, na których są przetwarzane dane, powinni mieć tylko upoważnieni pracownicy. Jeżeli nie jest to możliwe (urządzenia prywatne), pracownicy zostają zobowiązani do zachowania szczególnej ostrożności. Zaleca się stworzenie na komputerze oddzielnego konta użytkownika, do którego hasło będzie posiadać jedynie upoważniony pracownik, a dane powinny być zaszyfrowane;
   3) monitory komputerów, na których przetwarzane są dane, należy ustawić tak, aby osoby nieupoważnione nie miały wglądu w dane;

4) po zakończeniu pracy komputery przenośne zawierające dane osobowe powinny być zabezpieczone w zamykanych na klucz szafach;
5) nie należy udostępniać osobom nieupoważnionym komputerów służbowych, których zasady użytkowania i konserwacji są opisane w *IZSI;*
6) w przypadku potrzeby przeniesienia danych osobowych pomiędzy komputerami należy dokonać tego z zachowaniem szczególnej ostrożności. Nośniki użyte do tego należy wyczyścić (skasować nieodwracalnie), aby nie zostały na nich dane osobowe. W przypadku braku możliwości wyczyszczenia takiego nośnika (np. płyta CD), należy go zniszczyć fizycznie;
7) niezabezpieczonych danych osobowych nie należy przesyłać drogą elektroniczną;
8) sieć komputerowa powinna być zabezpieczona przed wszelkim dostępem z zewnątrz. Nie zaleca się łączenia z publicznymi sieciami teleinformatycznymi;
9) zabrania się używania urządzeń lub oprogramowania mogących naruszyć bezpieczeństwo innych systemów lub urządzeń;
10) zakazane jest przesyłanie informacji podlegających ochronie na prywatne adresy poczty elektronicznej oraz prowadzenie korespondencji służbowej z wykorzystaniem prywatnego adresu e-mail użytkowania. W SP 343 obowiązują służbowe adresy email, które zostały wygenerowane w ramach udziału w projekcie eduwarszawa.pl. Adresy są dostępne u wicedyrektora;
11) w przypadku wykonania kopii bazy danych lub przenoszenia danych na nośnikach zewnętrznych (np. typu pendrive), pracownik zobowiązany jest do zabezpieczenia ww. rzeczy przed dostępem osób trzecich (m.in. niepozostawianie nośników w miejscach ogólnodostępnych);
12) pracownicy zobowiązani są do systematycznej zmiany haseł dostępu do systemów informatycznych. W uzasadnionych sytuacjach dyrektor szkoły może polecić dokonanie zmiany hasła przez użytkownika np. po każdym incydencie lub podejrzeniu naruszenia bezpieczeństwa:
    a) hasło powinno składać się z unikalnego zestawu co najmniej 5 znaków. Nie może być identyczne z identyfikatorem użytkownika ani jego imieniem lub nazwiskiem;
    b) użytkownik powinien stosować hasło, które jest łatwe do zapamiętania, ale trudne do odgadnięcia, nie jest oparte na prostych skojarzeniach dotyczących właściciela konta (np. nr telefonu, imię, data urodzenia);
    c) należy unikać ponownego lub cyklicznego używania starych haseł;

d) zabrania się udostępniania swojego identyfikatora i hasła innym osobom oraz korzystania z identyfikatorów i haseł innych użytkowników;

e) pracownicy są odpowiedzialni za zachowanie swoich haseł w poufności;

f) użytkownik nie powinien przechowywać haseł w widocznym miejscu, nie powinien umieszczać haseł w żadnych automatycznych procesach logowania (skryptach, makrach lub pod klawiszami funkcyjnymi);

g) użytkownik wprowadza swoje hasło w sposób uniemożliwiający innym osobom jego poznanie;

h) w sytuacji, gdy zaistnieje podejrzenie, że hasło mogła poznać osoba nieupoważniona, użytkownik natychmiast dokonuje zmiany hasła;

i) hasła użytkownika utrzymuje się w tajemnicy również po upływie ich ważności;

9. Przed przystąpieniem do pracy użytkownicy informacji zobowiązani są dokonać sprawdzenia stanu urządzeń informatycznych oraz oględzin swojego stanowiska pracy, w tym zwrócić szczególną uwagę, czy nie zaszły okoliczności wskazujące na wystąpienie bądź podejrzenie wystąpienia incydentu bezpieczeństwa.

10. W przypadku stwierdzenia wystąpienia incydentu bezpieczeństwa lub możliwości jego wystąpienia, użytkownicy informacji zobowiązani są do bezzwłocznego powiadomienia o tym fakcie dyrektora szkoły, który postępuje zgodnie z zasadami opisanymi w *Polityce bezpieczeństwa Informacji.*

11. Zawieszenie pracy w przypadku czasowego opuszczenia stanowiska pracy:

1) zablokowanie sesji na stacji roboczej;

2) odblokowanie sesji po podaniu hasła.

12. W przypadku bezczynności na stacji roboczej przez czas przekraczający 2 minuty, zaleca się automatyczne włączenie wygaszacza ekranu, który powinien być zaopatrzony w hasło umożliwiające ponowne podjęcie pracy na stacji roboczej.

13. Krótkotrwała przerwa w pracy, podczas której użytkownik nie opuszcza stanowiska roboczego, nie wymaga zamykania aplikacji, wylogowania.

14. Zakończenie pracy:

1) zakończenie pracy programu zgodnie z instrukcją obsługi;

2) wylogowanie z systemu;

3) wyłączenie stacji roboczej i monitora;