

Zarządzenie nr 12/2018
z dnia 3.09.2018 r.
Dyrektora
Szkoły Podstawowej im. Księdza Jana Siuzdaka
w Wołkowie

w sprawie wprowadzenia regulaminów i procedury dotyczących
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 takich danych oraz uchylenia dyrektywy 95/46/WE (4.5.2016 L 119/38 Dziennik Urzędowy Unii Europejskiej PL) , zarządzam co następuje:

§ 1

Wprowadza się następujące regulaminy i instrukcje dotyczące ochrony danych osobowych w Szkole Podstawowej im. Księdza Jana Siuzdaka w Wołkowie:

1. Regulamin użytkowania komputerów przenośnych w Szkole Podstawowej im. Księdza Jana Siuzdaka w Wołkowie – załącznik nr 1
2. Procedura wykorzystywania nośników danych cyfrowych w Szkole Podstawowej im. Księdza Jana Siuzdaka w Wołkowie – załącznik nr 2
3. Zasady bezpieczeństwa realizacji umowy wykonywania usług administracji i serwisowania IT w Szkole Podstawowej im. Księdza Jana Siuzdaka w Wołkowie – załącznik nr 3
4. Procedura czystego biurka stosowana w Szkole Podstawowej im. Księdza Jana Siuzdaka w Wołkowie – załącznik nr 4
5. Procedura czystego pulpitu w Szkole Podstawowej im. Księdza Jana Siuzdaka w Wołkowie – załącznik nr 5

§ 2

Regulaminy stanowią załączniki do zarządzenia.

§ 3

Zarządzenie wchodzi w życie 3 września 2018 r.

Dyrektor
Szkoły Podstawowej im. Księdza Jana
Siuzdaka w Wołkowie
mgr Witold Orłowski

**Regulamin użytkowania komputerów przenośnych
w Szkole Podstawowej im. Księdza Jana Siuzdaka w Wołkowie**

1. Każdy Użytkownik komputera przenośnego winien zapoznać się z Regulaminem użytkowania komputerów przenośnych oraz pisemnie zobowiązać się do jego przestrzegania.
2. W przypadku przechowywania na komputerze przenośnym danych osobowych lub stanowiących tajemnicę pracodawcy, użytkownik zobowiązany jest do ich przechowywania na dysku szyfrowanym, zabezpieczonym co najmniej 8 znakowym hasłem (duże, małe litery, znaki specjalne lub cyfry).
3. Na komputerach przenośnych przeznaczonych do zewnętrznych prezentacji multimedialnych nie powinny, o ile jest to możliwe, znajdować się dane osobowe lub stanowiące tajemnicę pracodawcy.
4. W przypadku kradzieży lub zgubienia komputera przenośnego, użytkownik powinien natychmiast powiadomić o tym osobę odpowiedzialną za ochronę danych (IOD), zaznaczając jednocześnie, jakiego rodzaju dane były na tym urządzeniu przechowywane.
5. Użytkownik zobowiązany jest do zabezpieczenia komputera przenośnego w czasie transportu, a w szczególności:
 - zaleca się przenoszenie go w specjalnym futerale, pokrowcu lub torbie,
 - zabrania się pozostawiania komputera przenośnego w samochodzie podczas postoju w miejscu publicznym bez nadzoru,
 - podczas jazdy samochodem zaleca się przechowywanie komputera przenośnego w bezpiecznym miejscu.
6. W przypadku, gdy komputer przenośny pozostawiony jest w miejscu dostępnym dla osób nieupoważnionych, użytkownik jest zobowiązany do stosowania kabla zabezpieczającego. W szczególności dotyczy to zabezpieczenia komputera na stanowisku pracy, podczas konferencji, prezentacji, szkoleń, targów itp.
7. W przypadku pozostawiania komputerów przenośnych w biurze zaleca się umieszczanie ich po zakończeniu pracy w zamykanych szafkach.
8. Użytkownik komputera przenośnego jest zobowiązany do regularnego tworzenia kopii bezpieczeństwa danych na serwerze lub na określonych nośnikach (pendrive, CD, DVD). Nośniki z takimi kopiami powinny być przechowywane w bezpiecznym miejscu, z uwzględnieniem ochrony przed dostępem osób niepowołanych.
9. Pracując na komputerze przenośnym w miejscach publicznych i środkach transportu, użytkownik zobowiązany jest chronić wyświetlane na monitorze informacje przed wglądem osób nieupoważnionych.

***Zapoznałem się z Regulaminem użytkowania komputerów przenośnych
i zobowiązuje się do przestrzegania zasad w nim zawartych.***

.....
/opracował/

.....
/podpis użytkownika/

**Procedura wykorzystywania
nośników danych cyfrowych
w Szkole Podstawowej im. Księdza Jana Siuzdaka w Wołkowie**

1. Każdy nośnik używany w środowisku informatycznym z wyłączeniem płyt CD i DVD, powinien posiadać unikalny numer seryjny pozwalający na powiązanie go z indywidualnym użytkownikiem.
2. Zabrania się używania nośników stanowiących własność użytkowników, a w szczególności dokonywania czynności polegających na kopiowaniu, przegrywaniu plików, montowaniu, demontowaniu urządzeń, wgrywaniu, przegrywaniu oprogramowania oraz danych w celu przeniesienia lub skopiowania informacji ze sprzętu informatycznego pracodawcy na nośniki stanowiące własność użytkowników.
3. Pamięć zewnętrzna powinna być przechowywana w sposób uniemożliwiający dostęp do niej osobom niepowołanym i powinna być chroniona przed utratą bądź zniszczeniem.
4. Pamięć należy sprawdzać oprogramowaniem antywirusowym na obecność wirusów lub innego szkodliwego oprogramowania.
5. Przed przekazaniem pamięci innemu użytkownikowi zawarte w niej dane należy zarchiwizować, a następnie usunąć za pomocą programu służącego do trwałego kasowania zawartości danych.
6. Zabrania się stosowania pamięci przenośnych do wykonywania kopii zapasowych danych przetwarzanych na twardych dyskach komputerów służbowych. Pamięć przenośna może być traktowana jedynie jako krótkotrwały nośnik danych wytwarzanych w systemie komputerowym, a po wykorzystaniu dane te powinny być z niej usunięte.
7. Użytkownik powinien używać oprogramowania szyfrującego dane przechowywane w pamięciach zewnętrznych.
8. Hasło zabezpieczające nośniki zewnętrzne powinno składać się z co najmniej 8 do 12 znaków zawierających małe i duże litery, cyfry oraz znaki specjalne.

.....
/opracował/

.....
/podpis pracownika/

**Zasady bezpieczeństwa realizacji umowy
wykonywania usług administracji i serwisowania IT
w Szkole Podstawowej im. Księdza Jana Siuzdaka w Wołkowie**

1. Zleceniobiorca zobowiązuje się dopuszczać do przetwarzania danych osobowych osoby realizujące Umowę poinformowane i przeszkolone z zasad bezpieczeństwa pracy z danymi osobowymi.
2. Każda osoba realizująca Umowę zobowiązana jest do przetwarzania danych osobowych do których uzyskała dostęp wyłącznie w zakresie i celu przewidzianym w Umowie.
3. Każda osoba realizująca Umowę zobowiązana jest do zapewnienia poufności danych osobowych przetwarzanych w związku z wykonywaniem Umowy a w szczególności do tego, że nie będzie przekazywać, ujawniać i udostępniać tych danych osobom nieuprawnionym.
4. Każda osoba realizująca Umowę zobowiązuje się do zachowania w tajemnicy sposobów zabezpieczenia danych osobowych o ile nie są one jawne.
5. Każda osoba realizująca Umowę zobowiązana jest do nie powodowania niezgodnych z Umową zmian danych lub utraty, uszkodzenia lub zniszczenia tych danych.
6. Każda osoba realizująca Umowę zobowiązuje się do niedokonywania jakiegokolwiek kopiowania i utrwalania danych osobowych poza systemami informatycznymi Zleceniodawcy.
7. W przypadku wykorzystania sieci publicznej, każda osoba realizująca Umowę zobowiązuje się do stosowania zabezpieczonego połączenia zdalnego SSL.
8. Każda osoba realizująca Umowę zobowiązuje się do pracy w systemach Zleceniodawcy z użyciem uwierzytelnienia.

.....
/ Zleceniodawca/

.....
/Zleceniobiorca/

**Procedura czystego biurka stosowana
w Szkole Podstawowej im. Księdza Jana Siuzdaka w Wołkowie**

1. Procedura czystego biurka obowiązuje wszystkich pracowników zatrudnionych w Szkole Podstawowej im. Księdza Jana Siuzdaka w Wołkowie i jest częścią Polityki Ochrony Danych Osobowych obowiązującej od 25.05.2018 r.
2. Za pracowników uważa się każdą osobę zatrudnioną na podstawie stosunku pracy, a także zleceniobiorców, stażystów, praktykantów, osoby współpracujące oraz samozatrudnione na rzecz administratora danych.
3. Każdy pracownik zobowiązany jest do przechowywania na biurku tylko tych dokumentów, które są mu niezbędne do pracy w danym momencie. Należy unikać przechowywania dokumentów niepotrzebnych do bieżących zadań.
4. Po zakończeniu pracy z dokumentami zawierającymi dane osobowe należy odłożyć je do szuflady lub szafy zamykanej na klucz.
5. Dokumenty niepotrzebne w dalszej pracy i niepodlegające archiwizacji należy niszczyć zgodnie z zaleceniami „Procedury niszczenia dokumentów”.
6. Ekran monitorów komputerów powinny być ustawione tak by uniemożliwiały widok osobom postronnym.
7. Na biurku nie powinny znajdować się napoje w pojemnikach grożących rozlaniem.
8. Po zakończeniu pracy na biurku powinny pozostać tylko telefon i przybory biurowe.

.....
/opracował/

.....
/podpis pracownika/

**Procedura czystego pulpitu
w Szkole Podstawowej im. Księdza Jana Siuzdaka w Wołkowie**

1. Celem działania jest ograniczenie ryzyka ujawnienia lub kradzieży informacji oraz danych osobowych przetwarzanych w czasie pracy. Procedura ujednocila tryb postępowania w czasie używania środowiska pracy, jakim jest monitor ekranowy.
2. Za przestrzeganie niniejszej procedury są odpowiedzialni wszyscy pracownicy, którzy używają komputerów wyposażonych w monitory ekranowe.
3. Pracownik ma obowiązek utrzymywać ład i porządek na stanowisku pracy.
4. Niedopuszczalne jest zapisywanie dokumentów bezpośrednio na pulpicie komputera i pozostawienie ich tam.
5. Dokumenty powinny być zapisywane w odpowiednich tematycznych folderach.
6. W przypadku zapisywania dokumentów zawierających dane osobowe foldery powinny być zabezpieczone hasłem.
7. W przypadku wykonywania kopii dokumentu za pomocą ksera, skanera, faksu, itp., należy sprawdzić czy wszystkie dokumenty zostały usunięte z urządzenia celem zminimalizowania przejęcia danego dokumentu przez osoby nieupoważnione.
8. Monitor ekranowy powinien być tak ustawiony, aby osoba nieupoważniona lub klient nie miał bezpośredniego wglądu na treść wyświetlaną na ekranie.
9. Podczas nawet chwilowego opuszczenia stanowiska pracy należy zablokować możliwość wglądu do przetwarzanych danych przez osoby postronne poprzez zablokowanie stacji używając klawiszy **Windows + L** lub wylogowanie użytkownika z aplikacji.
10. Na czas dłuższej nieobecności zalecane jest wyłączenie stanowiska komputerowego.
11. W razie problemów związanych z systemem informatycznym należy powiadomić przełożonego oraz skontaktować się z informatykiem.
12. Po zakończeniu pracy należy wyłączyć komputer oraz pozostałe urządzenia biurowe oraz upewnić się czy wszystkie dokumenty zostały zabezpieczone.

.....
/opracował/

.....
/podpis pracownika/