INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM, SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH W SZKOLE PODSTAWOWEJ IM. PROF. JANA CZEKANOWSKIEGO W CMOLASIE

Załącznik nr 2 Zarządzenia Nr 51 2017/2018
Dyrektora
Szkoły Podstawowej im. prof. Jana Czekanowskiego w Cmolasie
z dnia 25-05-2018 r.
w sprawie wprowadzenia wewnętrznych uregulowań
dotyczących ochrony danych osobowych

Instrukcja określa zasady zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Szkole Podstawowej im. prof. Jana Czekanowskiego w Cmolasie zwanej w dalszej części „szkołą", zgodnie ze strategią określoną w „Polityce Bezpieczeństwa Danych Osobowych".

Dokument stanowi specyfikację podstawowych środków technicznych ochrony danych oraz elementów zarządzania systemem informatycznym. W przypadku wystąpienia potrzeb wprowadzenia nowych lub modyfikacji istniejących uregulowań proceduralnych danego obszaru, wnioski o ich opracowanie powinni składać pracownicy których procedury dotyczą do inspektora ochrony danych osobowych - IOD. Zasady zawarte w niniejszym dokumencie oraz określone w odrębnych dokumentach powinny być udostępniane pracownikom na poszczególnych stanowiskach tylko w niezbędnym zakresie. Za wdrożenie procedur odpowiedzialny jest Dyrektor Szkoły.

Obowiązki wynikające z dokumentów dotyczących zarządzania systemem informatycznym oraz zasady ochrony danych osobowych należy określać w indywidualnych zakresach czynności pracowników -odpowiednio do zadań wykonywanych na zajmowanym stanowisku.

System informatyczny i jego zasoby.

Nazwy zbioru danych osobowych

Zbiór nr 1 - Ewidencja osób zatrudnionych przy przetwarzaniu danych osobowych

Zbiór nr 2 - Kontrola wewnętrzna - wyniki, opracowania, raporty, notatki

Zbiór nr 3 - Akta osobowe pracowników

Zbiór nr 4 - Dokumentacja dotycząca polityki kadrowej: opiniowanie awansów, wyróżnień, odznaczeń - nagrody i kary, itp.

Zbiór nr 5 - Notatki służbowe oraz postępowanie dyscyplinarne w stosunku do nauczycieli i pracowników administracyjno-obsługowych

Zbiór nr 6 - Podania i wnioski osób z zewnątrz

Zbiór nr 7 - Ewidencja zwolnień lekarskich pracowników

Zbiór nr 8 - Skierowania do specjalistów

Zbiór nr 9 - Dokumentacja związana ze zdrowiem pracowników; legitymacje ubezpieczeniowe, pracownicze książeczki zdrowia

Zbiór nr 10 - Zastępstwa za nieobecnych nauczycieli

Zbiór nr 11 - Ewidencja urlopów nauczycieli, pracowników obsługi i administracji

Zbiór nr 12 - Kartoteki wydawanej pracownikom odzieży ochronnej i środków ochrony indywidualnej

Zbiór nr 13 - Rejestr delegacji służbowych

Zbiór nr 14 - Ewidencja osób korzystających ze świadczeń funduszu socjalnego wraz z dokumentacją

Zbiór nr 15 - Listy płac pracowników - system informatyczny

Zbiór nr 16 - Kartoteki zarobkowe pracowników

Zbiór nr 17 - Deklaracje ubezpieczeniowe pracowników

Zbiór nr 18 - Deklaracje i kartoteki ZUS pracowników

Zbiór nr 19 - Deklaracje podatkowe pracowników

Zbiór nr 20 - Księga uczniów (realizacja obowiązku szkolnego)

Zbiór nr 21 - Arkusze ocen

Zbiór nr 22 - Karty zgłoszeń uczniów

Zbiór nr 23 - Dzienniki zajęć obowiązkowych i dodatkowych

Zbiór nr 24 - Zaświadczenia z PPP i in.

Zbiór nr 25 - Deklaracje uczęszczania na zajęcia nieobowiązkowe

Zbiór nr 26 - Ewidencja decyzji - zwolnienia uczniów z zajęć

Zbiór nr 27 - Rejestr zaświadczeń wydawanych pracownikom

Zbiór nr 28 - Rejestr wypadków uczniów

Zbiór nr 29 - Rejestr wypadków pracowników

Zbiór nr 30 - Księga druków ścisłego zarachowania

Zbiór nr 31 - Zbiór upoważnień

Zbiór nr 32 - Dowody wpłat

Zbiór nr 33 - Umowy zawierane z osobami fizycznymi

Zbiór nr 34 - Protokoły rady pedagogicznej; uchwały rady pedagogicznej

Zbiór nr 35 - Protokoły narad pracowników administracyjno-obsługowych

Zbiór nr 36 - Składnica akt (akta osobowe pracowników, listy płac, kartoteki zarobkowe, księgi arkuszy ocen, dzienniki lekcyjne, protokoły)

Zbiór nr 37 Biblioteka - rejestry, kartoteki czytelników.

Wobec faktu przetwarzania jednego zbioru danych osobowych w architekturze rozproszonej, wyodrębniony został jeden system informatyczny.

System informatyczny stanowią środki przetwarzania informacji wraz ze związanymi z nim ludźmi oraz zasobami technicznymi i finansowymi, czyli urządzeniami komputerowymi i niekomputerowymi do przetwarzania danych osobowych i informacji z nimi związanych.

Przetwarzanie informacji, w tym danych osobowych obejmuje operacje polegające na ich zbieraniu, utrwalaniu, zmianie, przechowywaniu, opracowywaniu, udostępnianiu i usuwaniu.

<u>Środki techniczne</u>

Sieć komputerowa.

Infrastruktura sieciowa składa się z okablowania strukturalnego w budynku z wydzieloną instalacją zasilającą urządzenia komputerowe.

Elementy aktywne sieci to przełączniki.

Sprzęt komputerowy.

W systemie informatycznym szkoły wykorzystywany jest sprzęt komputerowy określony w szczegółowej specyfikacji technicznej prowadzonej przez administratora systemu.

Inne środki przetwarzania.

- Drukarki
- Skanery

- Niszczarki dokumentów
- Urządzenia niekomputerowe inne (dokumenty papierowe, skoroszyty, meblowe wyposażenie pokoi).

Określenie miejsca przetwarzania danych w systemie informatycznym.

Miejscem przetwarzania danych osobowych są pomieszczenia pracy komórek organizacyjnych szkoły Osoby nieuprawnione mogą przebywać w pomieszczeniach w których przetwarza się dane osobowe tylko w obecności uprawnionych pracowników szkoły.

Aplikacje i rejestry.

W skład systemu informatycznego wchodzą aplikacje użytkowe ujęte w szczegółowej specyfikacji technicznej prowadzonej przez administratora systemu oraz kartoteki, decyzje i rejestry prowadzone ręcznie lub komputerowo przy użyciu aplikacji biurowych (pakiet MS Office) w komórkach organizacyjnych szkoły.

Identyfikatory, hasła, prawo dostępu

Przydział identyfikatorów dla użytkowników.

Użytkownik otrzymuje identyfikator, który identyfikuje go w systemie informatycznym. Bez jego posiadania użytkownik nie może pracować w systemie. Administrator Systemów Informatycznych przydziela identyfikatory dla użytkowników a Inspektor Ochrony Danych prowadzi ewidencję osób zatrudnionych przy przetwarzaniu danych osobowych.

Przydział haseł dla użytkowników.

Pierwsze hasło dla użytkownika jest zakładane przez Administratora Systemu Informatycznego podczas wprowadzania jego identyfikatora do systemu. Następnie użytkownik powinien zmienić hasło wg określonych zasad:

- hasło jest obowiązkowe dla każdego użytkownika posiadającego identyfikator w systemie,
- hasło jest zakładane jednocześnie z utworzeniem identyfikatora dla użytkownika,
- po założeniu hasła przez administratora systemu, użytkownik ma obowiązek zarejestrować się do systemu i zmienić hasło,
- hasło jest ciągiem znaków, które nie powinny być łatwe do zidentyfikowania (nie należy używać jako hasła np. imienia, daty urodzenia własnej, dzieci ani współmałżonka)
- hasło objęte jest tajemnicą- użytkownik nie może go ujawnić,
- przy wpisywaniu hasła nie jest ono wyświetlane na ekranie,
- w przypadku ujawnienia hasła musi ono zostać niezwłocznie zmienione,
- hasło musi być zmieniane przynajmniej raz na kwartał,
- użytkownik odpowiada za systematyczną zmianę haseł,
- hasła użytkowników muszą być zapisywane w systemie w postaci zaszyfrowanej.

Kartoteki, decyzje, rejestry itp. tworzone za pomocą aplikacji biurowych (pakiet MS Office) są chronione przy użyciu haseł systemowych i haseł zakładanych przez użytkownika dla poszczególnych dokumentów wg instrukcji dostępnej w pakiecie MS Office.

Zarządzanie hasłami użytkowników.

Hasła użytkowników należą do nich samych. Są one objęte tajemnicą i nikt poza właścicielami haseł nie
może ich znać. Hasło musi być zmieniane przez użytkownika nie rzadziej niż raz na 30 dni.

Odpowiedzialność za okresowe zmiany hasła ciąży na użytkowniku - właścicielu hasła. W przypadku
potrzeby zabezpieczenia dostępu do systemu Dyrektor Szkoły decyduje o deponowaniu hasła.

Postępowanie z hasłami systemowymi.

Hasła systemowe są to hasła specjalnych użytkowników w systemie operacyjnym serwera. Dają one bardzo szerokie uprawnienia i pozwalają na wykonanie każdego działania w systemie - z tego względu podlegają szczególnej ochronie.

Przydzielanie użytkownikowi praw dostępu do systemu informatycznego.

Nadawanie praw dostępu do systemu informatycznego jest dokonywane przez Administratora Systemu Informatycznego za zgodą Dyrektora Szkoły. Nadane uprawnienia pozwalają na wykonanie określonego zakresu prac.

Wejście do systemu / wyjście z systemu.

Rejestrowanie i wyrejestrowanie użytkowników.

Rejestrowanie użytkownika odbywa się obowiązkowo gdy rozpoczyna on pracę w systemie. Polega na wprowadzeniu identyfikatora, objętego tajemnicą! znanego tylko użytkownikowi hasła, na podstawie których system stwierdza tożsamość użytkownika. Po poprawnym zarejestrowaniu użytkownik może wykonywać wszystkie czynności, na jakie pozwalaj ą przydzielone mu prawa dostępu.

Rozpoczęcie i zakończenie pracy.

Rozpoczęcie pracy w systemie informatycznym wymaga wykonania następujących czynności:

- włączenia komputera,
- po załadowaniu systemu operacyjnego uruchomienia oprogramowania komunikacyjnego,
- rejestracji w systemie informatycznym,
- po pozytywnym przejściu procedury uwierzytelnienia - uzyskanie dostępu do systemu.
    - Po zakończeniu pracy w systemie należy:
- wyrejestrować się z systemu,
- zakończyć działanie oprogramowania komunikacyjnego,
- zakończyć pracę systemu operacyjnego,
- wyłączyć komputer.

Kopie i nośniki

Sposób i częstotliwość tworzenia awaryjnych kopii baz danych.

Awaryjne kopie baz danych należy tworzyć w celu zabezpieczenia zbiorów danych osobowych przed niezamierzoną ich utratą oraz możliwością ich odtworzenia. Awaryjne kopie baz danych muszą być aktualizowane przez użytkowników.

Sposób tworzenia kopii baz danych jest zróżnicowany w zależności od rodzaju aplikacji użytkowej.

Sposób i czas przechowywania nośników z kopiami danych osobowych.

Nośniki z kopiami zbiorów danych osobowych muszą być opisane i przechowywane jak dokumenty stanowiące tajemnicę służbową w zamykanych szafach metalowych lub drewnianych.

Przechowywanie wydruków

W przypadku wykonywania wydruków ze zbioru danych osobowych wykonawca jest zobowiązany do zachowania wszelkich niezbędnych działań w celu niedopuszczenia do ich nieuprawnionego ujawnienia lub utraty. Wydruki muszą być odpowiednio zabezpieczone.

Sieć komputerowa

Postępowanie w zakresie komunikacji w lokalnej sieci komputerowej.

Przetwarzanie danych osobowych w szkole jest możliwe przy wykorzystaniu sieci wewnętrznej i zewnętrznej, po zastosowaniu procedur dopuszczających poszczególnych wykonawców do dostępu do zbioru danych lub ich części, umożliwiających identyfikację osób, czas pracy na zbiorach danych osobowych oraz wykonywane czynności przez użytkownika.

Zasady korzystania z komputerów przenośnych

Za bezpieczeństwo komputera przenośnego odpowiedzialny jest jego użytkownik. Osoba użytkująca przenośny komputer, na którym przetwarzane są dane należące do systemu informatycznego zobowiązana jest zachować szczególną ostrożność podczas transportu i przechowywania go poza strefą przetwarzania danych i nie powinna zezwalać na korzystanie z niego osobom nieupoważnionym. Komputer taki powinien być zabezpieczony hasłem dostępu.

Zasady korzystania z monitorów komputerowych

Ustawienie monitorów w pomieszczeniach, w których przebywają osoby postronne.

W pomieszczeniach, w których odbywa się przetwarzanie danych osobowych a jednocześnie mają do tych pomieszczeń dostęp osoby postronne, monitory urządzeń komputerowych muszą być ustawione w taki sposób, by informacje na nich wyświetlane nie były widoczne dla osób postronnych.

Stosowanie automatycznego wygaszania ekranu.

Dla urządzeń komputerowych mających odpowiednie możliwości techniczne, ekrany monitorów muszą być automatycznie wygaszane w przypadku dłuższej nieaktywności użytkownika. Wygaszacz powinien być chroniony hasłem.

Zasady instalacji oprogramowania

Instalacja nowego oprogramowania i jego aktualizacja na serwerze.

Dopuszcza się instalację nowego oprogramowania do przetwarzania danych osobowych lub aktualizacji
istniejących pod warunkiem spełnienia określonych wymagań. Instalacji oprogramowania lub aktualizacji dokonuje Administrator Systemów Informatycznych lub sam użytkownik**.**

Instalacja oprogramowania na komputerach.

Na wszystkich komputerach szkoły dopuszcza się instalację tylko legalnego, licencjonowanego oprogramowania. Zabrania się instalowania oprogramowania bez zgody Administratora Systemów Informatycznych.

Zasady dokonywania napraw

Dokonywanie napraw, przeglądów i konserwacji systemu przez pracowników serwisu.

Działania pracowników serwisu muszą odbywać się w obecności Administratora Systemów Informatycznych lub osoby przez niego upoważnionej.

Postępowanie z uszkodzonymi nośnikami magnetycznymi zawierającymi dane osobowe.
Uszkodzone nośniki magnetyczne lub inne zawierające dane osobowe nie mogą być użytkowane. Muszą być odpowiednio zabezpieczone przed nieuprawnionym udostępnieniem a następnie zniszczone lub naprawione pod nadzorem osoby upoważnionej przez Administratora Danych Osobowych.

Profilaktyka antywirusowa
Każdy użytkownik komputera w szkole zobowiązany jest do używania w pracy CD i innych nośników danych zakupionych przez szkołę (nie prywatnych) i przechowywania na nich tylko i wyłącznie danych związanych z charakterem pracy.
Ochrona antywirusowa komputerów tj. skanowanie, reakcja na odnalezienie oprogramowania złośliwego, aktualizacja bazy wirusów etc. realizowana jest automatycznie przez program antywirusowy. Ustawieniami programów antywirusowych zarządza administrator sieci.

Urządzenia podtrzymujące zasilanie
Wszystkie komputery na których przetwarzane są dane osobowe. muszą być wyposażone w zasilacze awaryjne. Zasilacze te muszą być wyposażone w mechanizm umożliwiający bezpieczne wyłączenie komputera, poprzedzone prawidłowym zakończeniem rozpoczętych operacji i zamknięciem baz danych.

Ochrona obiektu
Zabezpieczenie fizyczne pomieszczeń, w których odbywa się przetwarzanie danych.
Pomieszczenia, w których znajdują się urządzenia komputerowe i niekomputerowe umożliwiające dostęp do systemu informatycznego służącego do przetwarzania danych osobowych muszą być wyposażone w zamknięcia oraz w miarę możliwości w urządzenia alarmowe. Sposób zabezpieczeń musi uwzględniać zasady ochrony fizycznej przewidziane dla informacji stanowiących tajemnicę służbową, w powiązaniu z którymi dane osobowe występują.
Zabezpieczenie elementów lokalnej sieci komputerowej.
Dostęp do infrastruktury technicznej związanej z siecią komputerową i jej zasilaniem nie może być możliwy dla osób postronnych. Rozdzielnie elektryczne i skrzynki z bezpiecznikami muszą posiadać skuteczne zamknięcia uniemożliwiające otwarcie przez osoby postronne. Klucze do nich powinny być w dyspozycji osoby odpowiedzialnej za instalacje energetyczne w budynku.
Instalacje alarmowe przeciwwłamaniowe i przeciwpożarowe.
Instalacja alarmowa uzupełnia system zabezpieczeń fizycznych, umożliwiając lepszą ochronę przed kradzieżą sprzętu i danych oraz jego zniszczeniem.
Sygnalizatory instalacji alarmowych należy połączyć w sposób umożliwiający reagowanie odpowiednich
służb.
Izolowanie lokalnej sieci komputerowej od sieci zewnętrznej.
Połączenie lokalnej sieci komputerowej szkoły z Internetem musi być chronione za pomocą urządzeń i oprogramowania typu „zapora ogniowa". Instalowanie odpowiedniego oprogramowania musi być przeprowadzone przez administratora systemów informatycznych.