INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

ROZDZIAŁ I

Postanowienia ogólne

§ 1

Niniejsza Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, zwana dalej Instrukcją, przyjęta została w celu wykazania, że dane osobowe w systemach informatycznych Szkoły Podstawowej nr 39 im kpt.ż.w. Kazimierza Jurkiewicza w Gdyni przetwarzane są w sposób zgodny z przepisami prawa mającymi zastosowanie do takiej czynności, zgodnie z zasadą art. 5 ust. 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 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 (dalej RODO).

Definicje pojęć zawartych w instrukcji:

1. Administrator Danych Osobowych (ADO) - Szkoły Podstawowej nr 39 im.kpt. ż.w. Kazimierza Jurkiewicza w Gdyni reprezentowany przez dyrektora
2. Administrator Systemów Informatycznych – osoba wyznaczona przez ADO, odpowiedzialna za nadzór nad systemami informatycznymi wykorzystywanymi u Administratora.
3. Dane osobowe – wszelkie informacje, w tym o stanie zdrowia, dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.
4. Hasło – ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.
5. Identyfikator użytkownika – ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.
6. Przetwarzanie danych – jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych.
7. Sieć lokalna – połączenie systemów informatycznych, wyłącznie dla własnych potrzeb, przy wykorzystaniu urządzeń i sieci telekomunikacyjnych.

8. System informatyczny – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji, narzędzi programowych zastosowanych w celu przetwarzania danych.
9. Użytkownik – osoba upoważniona przez ADO do przetwarzania danych osobowych w Szkole Podstawowej nr 39 im.kpt. ż.w. Kazimierza Jurkiewicza w Gdyni
10. Zbiór danych – każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępny według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.
11. Zabezpieczenie danych w systemie informatycznym – wdrożenie i eksploatacja stosowanych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem.

ROZDZIAŁ II

Nadawanie i rejestrowanie uprawnień do przetwarzania danych
w systemie informatycznym.

§ 2

1. W systemach informatycznych dane osobowe może przetwarzać wyłącznie osoba posiadająca pisemne upoważnienie do przetwarzania danych osobowych w Szkole.
2. Pracownik otrzymuje uprawnienie do przetwarzania danych w systemie informatycznym na podstawie pisemnego upoważnienia nadanego przez ADO.
3. Po otrzymaniu upoważnienia dla każdego użytkownika systemu informatycznego ustala się odrębny identyfikator i hasło.
4. Zabrania się używania identyfikatora lub hasła innego pracownika.
5. Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, system zapewnia odnotowanie:

– daty pierwszego wprowadzenia danych do systemu,
– identyfikatora użytkownika wprowadzającego dane do systemu.
– informacji o odbiorcach, którym dane osobowe zostały udostępnione.

6. Usuwanie kont stosowane jest wyłącznie w uzasadnionych przypadkach, standardowo, przy ustaniu potrzeby utrzymywania konta danego użytkownika ulega ono dezaktywacji w celu zachowania historii jego aktywności.
7. Osoby dopuszczone do przetwarzania danych osobowych zobowiązane są do zachowania tajemnicy w zakresie tych danych oraz sposobów ich zabezpieczenia. Obowiązek ten

istnieje również po ustaniu stosunku pracy, co jest równoznaczne z cofnięciem uprawnień do przetwarzania danych osobowych.

ROZDZIAŁ III

Zabezpieczenie danych w systemie informatycznym

§ 3

1. Ochronę przed awariami zasilania oraz zakłóceniami w sieci energetycznej serwera i stacji roboczych, na których przetwarzane są dane osobowe zapewniają zasilacze UPS.
2. W czasie pracy baterii zasilającej ASI dokonuje oceny sytuacji i podejmuje wszelkie niezbędne kroki w celu zachowania integralności danych oraz przywrócenia normalnego funkcjonowania systemu.
3. System informatyczny jest zabezpieczony przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu oraz przed działaniami inicjowanymi z sieci zewnętrznej.
4. Oprogramowanie wykorzystywane do przetwarzania danych posiada własny system kont (zabezpieczonych hasłami) i uprawnień. Zmiana hasła jest wymuszona automatycznie przez system.
5. Hasła do systemu stacji roboczych mają długość przynajmniej 8 znaków (duże i małe litery oraz cyfry lub znaki specjalne) i okres ważności nie dłużej niż 1 miesiąc. Hasło nie może być zapisywane lub przechowywane w miejscu dostępnym dla osób nieuprawnionych.
6. W przypadku utracenia hasła użytkownik ma obowiązek skontaktować się z ASI celem uzyskania nowego hasła.
7. System informatyczny, a w szczególności aplikacje służące do przetwarzania danych osobowych muszą posiadać mechanizmy pozwalające na odnotowanie faktu wykonania operacji na danych. W szczególności zapis ten powinien obejmować:
   - rozpoczęcie i zakończenie pracy przez użytkownika systemu,
   - operacje wykonywane na przetwarzanych danych,
   - nieudane próby dostępu do systemu informatycznego przetwarzającego dane osobowe oraz nieudane próby wykonania operacji na danych osobowych,
   - błędy w działaniu systemu informatycznego podczas pracy danego użytkownika.

8. System informatyczny powinien zapewnić zapis faktu przekazania danych osobowych z uwzględnieniem:

- identyfikatora osoby, której dane dotyczą,
- osoby przesyłającej dane,
- odbiorcy danych,
- zakresu przekazanych danych osobowych,
- daty operacji,
- sposobu przekazania danych.

9. Na każdym komputerze, na którym przetwarzane są dane osobowe, stosuje się aktywną ochronę antywirusową. Za dokonywanie skanowania systemu w poszukiwaniu złośliwego oprogramowania (w przypadku braku ochrony rezydentnej) i aktualizację bazy wirusów odpowiada ASI.
10. Aktualizacja bazy wirusów odbywa się poprzez automatyczne pobieranie bazy wirusów przez program antywirusowy. W przypadku wykrycia wirusa należy:
    - uruchomić program antywirusowy i skontrolować użytkowany system,
    - usunąć z systemy wykrytego wirusa.

Kiedy operacja nie powiedzie się należy:

- zakończyć pracę w systemie,
- odłączyć zainfekowany komputer od sieci,
- powiadomić o zaistniałej sytuacji ASI.

11. Osobom korzystającym z systemu informatycznego, w którym przetwarzane są dane osobowe zabrania się:
    - ujawniania loginu i hasła współpracownikom oraz osobom z zewnątrz,
    - pozostawiania haseł w miejscach widocznych dla innych osób,
    - udostępniania stanowisk pracy wraz z danymi osobowymi osobom nieuprawnionym,
    - udostępniania osobom nieuprawnionym programów komputerowych zainstalowanych w systemie,
    - używania oprogramowania w innym zakresie niż pozwala na to umowa licencyjna,
    - przenoszenia programów komputerowych, dysków twardych z jednego stanowiska na inne,
    - kopiowania danych na nośniki informacji, kopiowania na inne systemy celem wynoszenia ich poza szkołę,
    - samowolnego instalowania i używania jakichkolwiek programów komputerowych w tym również programów do użytku prywatnego; programy komputerowe instalowane są przez ASI.

- używania nośników danych udostępnionych przez osoby postronne,
- przesyłania dokumentów i danych z wykorzystaniem konta pocztowego prywatnego (nie służbowego),
- otwierania załączników i wiadomości poczty elektronicznej od nieznanych i „niezaufanych" nadawców,
- używania nośników danych niesprawdzonych, niewiadomego pochodzenia lub niezwiązanych z wykonywaną pracą.

ROZDZIAŁ IV

Zasady bezpieczeństwa podczas pracy w systemie informatycznym

§ 4

1. W celu rozpoczęcia pracy w systemie informatycznym użytkownik:
- uruchamia stację roboczą i loguje się do systemu operacyjnego przy pomocy identyfikatora i hasła,
- loguje się do programów i systemów wymagających dodatkowego wprowadzenia unikalnego identyfikatora i hasła,
- podczas tymczasowego zaprzestania pracy, aby uniemożliwić osobom postronnym korzystanie z systemu informatycznego należy wylogować się z systemu lub uruchomić wygaszasz ekranu chroniony hasłem,
- w sytuacji gdy wgląd w wyświetlane na monitorze dane może mieć nieuprawniona osoba należy tymczasowo zmienić widok wyświetlany na monitorze lub obrócić monitor (przymknąć ekran laptopa) w sposób uniemożliwiający wgląd w wyświetlaną treść,
- użytkownik wyrejestrowuje się z systemu informatycznego przed wyłączeniem stacji komputerowej poprzez zamknięcie programu przetwarzającego dane oraz wylogowanie się z systemu operacyjnego.
2. Zawieszenie korzystania z systemu informatycznego może nastąpić losowo wskutek awarii lub planowo (np. w celu konserwacji sprzętu). Planowe zawieszenie prac jest poprzedzone poinformowaniem pracowników Szkoły przez ASI o planowanym zawieszeniu.
3. Pracownik korzystający z systemu informatycznego zobowiązany jest do powiadomienia ASI w razie:

- podejrzenia naruszenia bezpieczeństwa systemu,
- braku możliwości zalogowania się użytkownika na jego konto,
- stwierdzenia fizycznej ingerencji w przetwarzana dane,
- stwierdzenia użytkowania narzędzia programowego lub sprzętowego.

4. Na fakt naruszenia zabezpieczeń systemu mogą wskazywać:

- nietypowy stan stacji roboczej (np. brak zasilania, problemy z uruchomieniem),
- wszelkiego rodzaju różnice w funkcjonowaniu systemu (np. komunikaty informujące o błędach, brak dostępu do funkcji systemu, nieprawidłowości w wykonywanych operacjach),
- różnice w zawartości zbioru danych osobowych (np. brak lub nadmiar danych),
- inne nadzwyczajne sytuacje.

RODZIAŁ V

Tworzenie kopii zapasowych

§ 5

Dane systemów kopiowane są w trybie rocznym (kopie zapisów e-dziennika). Odpowiedzialnym za wykonanie kopii danych jest szkolny administrator Librusa. Kopie zbiorów umieszczonych na serwerze wykonywane są automatycznie oprogramowaniem wytworzonym we własnym zakresie. Kopie danych przechowywane są w sejfie w gabinecie dyrektora szkoły i zabezpieczane przez ASI. Okresową weryfikację kopii bezpieczeństwa pod kątem ich przydatności do odtworzenia danych przeprowadza ASI. Nośniki danych, na których zapisywane są kopie bezpieczeństwa niszczy się trwale w sposób mechaniczny.

ROZDZIAŁ VI

Udostępnienie danych

§ 6

Dane osobowe przetwarzane w systemach informatycznych mogą być udostępnione osobom i podmiotom z mocy przepisów prawa.

ROZDZIAŁ VII

Przeglądy i konserwacje systemów

§ 7

Wszelkie prace związane z naprawami i konserwacją systemu informatycznego przetwarzającego dane osobowe mogą być wykonywane wyłącznie przez pracowników Szkoły lub przez upoważnionych przedstawicieli wykonawców. Prace konserwacyjne powinny

uwzględniać wymagany poziom zabezpieczenia danych przed dostępem osób nieupoważnionych.

Czynności serwisowe powinny być wykonywane w obecności osoby upoważnionej do przetwarzania danych osobowych, a przed ich wykonaniem należy zabezpieczyć dane i programy przed zniszczeniem lub zmianą.

ROZDZIAŁ VIII

Niszczenie wydruków

§ 8

Wszelkie wydruki z systemów informatycznych zawierające dane osobowe przechowywane są w miejscu uniemożliwiającym ich odczyt przez osoby nieuprawnione, w zamkniętych szafach lub pomieszczeniach i po upływie ich przydatności są niszczone przy użyciu niszczarek.