INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH W SZKOLE PODSTAWOWEJ IM. MARII KONOPNICKIEJ W HARKABUZIE

Administrator Danych osobowych

.....

SPIS TREŚCI

I. POSTANOWIENIA OGÓLNE

Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. 2002 r. Nr 101, poz. 926, ze zm.) oraz rozporządzenie ministra spraw wewnętrznych i administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024) nakłada na administratora danych osobowych następujące obowiązki:

- zapewnienie bezpieczeństwa i poufności danych, w tym zabezpieczenie ich przed ujawnieniem,
- zabezpieczenie danych przed nieuprawnionym dostępem,
- zabezpieczenie danych przed udostępnieniem osobom nieupoważnionym (nieuprawnionym pozyskaniem),
- zabezpieczenie przed utratą danych,
- zabezpieczenie przed uszkodzeniem lub zniszczeniem danych oraz przed ich nielegalną modyfikacją.

Ochronie podlegają dane osobowe niezależnie od formy przechowywania, sprzęt komputerowy, systemy operacyjne i informatyczne oraz pomieszczenia, w których odbywa się proces przetwarzania.

Instrukcja określa ramowe zasady właściwego zarządzania systemem informatycznym służącym do przetwarzania danych osobowych oraz podstawowe warunki techniczne i organizacyjne, jakim powinny odpowiadać urządzenia i system informatyczny, odpowiednie do zagrożeń i kategorii danych objętych ochroną.

II. PRZEZNACZENIE, DEFINICJE

Instrukcja zarządzania systemie informatycznym, służącym do przetwarzania danych osobowych w **SZKOLE PODSTAWOWEJ IM. MARII KONOPNICKIEJ W HARKABUZIE** , zwaną dalej instrukcją- określa sposób zarządzania oraz zasady

administrowania systemem informatycznym służącym do przetwarzania danych osobowych.

Ilekroć w instrukcji jest mowa o:

1. Jednostce - rozumie się przez to **SZKOŁĘ PODSTAWOWĄ IM. MARII KONOPNICKIEJ W HARKABUZIE;**
2. Kierownictwie - rozumie się przez to **Dyrektora Jednostki**;
3. Danych osobowych - rozumie się przez to każdą informację dotyczącą osoby fizycznej, pozwalającą na określenie tożsamości tej osoby;
4. Zbiorze danych - rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępny według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony czy podzielony funkcjonalnie;
5. Przetwarzaniu danych - rozumie się przez to 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;
6. Usuwaniu danych - rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;
7. Administratorze bezpieczeństwa informacji (ABI) - rozumie się przez to osobę odpowiedzialną w danej jednostce organizacyjnej za bezpieczeństwo danych osobowych w systemie informatycznym, w tym w szczególności za przeciwdziałanie dostępowi osób niepowołanych do systemu, w którym przetwarzane są dane osobowe oraz za podejmowanie odpowiednich działań w wypadku naruszeń w systemie zabezpieczeń;
8. Administratorze sieci/systemu operacyjnego - rozumie się przez to osobę nadzorującą i odpowiadającą za poprawną pracę powierzonego mu sprzętu sieciowego oraz systemu operacyjnego w danej jednostce organizacyjnej, w tym w szczególności:
    - mającą prawo do zmiany uprawnień wszystkich użytkowników,
    - za pomocą platformy zarządzania dysponującą bezpośrednio wszystkimi zasobami podległej mu sieci,
    - pełniącą kontrolę nad dostępem użytkowników do systemów,

- podejmującą samodzielnie lub na polecenie administratora bezpieczeństwa informacji odpowiednie działania w wypadku naruszeń w systemie zabezpieczeń

9. Administratorze aplikacji - rozumie się przez to osobę odpowiedzialną w danej jednostce organizacyjnej za bezpieczeństwo przetwarzania danych w ramach aplikacji, w tym administrującą prawami dostępu w ramach eksploatowanych aplikacji;
10. Użytkownikach systemu - rozumie się osoby upoważnione do przetwarzania danych osobowych w systemie informatycznym;
11. Obszarze kontrolowanym - należy przez to rozumieć obszar znajdujący się pod ochroną, o ograniczonym dostępie osób nieautoryzowanych, w którym odbywa się przetwarzanie danych, w tym danych osobowych.

Niniejsza Instrukcja zarządzania systemem informatycznym określa:

a) Określenie poziomu bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym;
b) Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym;
c) Stosowane metody i środki uwierzytelniania oraz procedury związane z ich zarządzaniem i użytkowaniem;
d) Sposób przydziału haseł dla użytkowników i częstotliwość ich zmiany oraz osoby odpowiedzialne za te czynności;
e) Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu;
f) Metoda i częstotliwość tworzenia kopii awaryjnych.
g) Metoda i częstotliwość sprawdzania obecności wirusów komputerowych oraz metoda ich usuwania;
h) Sposób, miejsce i okres przechowywania :
    - elektronicznych nośników informacji zawierających dane osobowe;
    - kopii zapasowych;
i) Sposób dokonywania przeglądów i konserwacji systemu i zbioru danych osobowych;

j) Sposób postępowania w zakresie komunikacji w sieci komputerowej;

k) Procedury wykonywania przeglądów i konserwacji systemu oraz nośników informacji służących do przetwarzania danych.

III. OKREŚLENIE POZIOMU BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH W SYSTEMIE INFORMATYCZNYM

1. Z analizy zagrożeń wynika, że w Jednostce miejscami najbardziej zagrożonymi są pomieszczenia budynku, w których znajdują się zbiory danych osobowych gromadzone w kartotekach oraz urządzeniach służących do przetwarzania tych danych, do których mogą mieć nieuprawniony dostęp osoby nieupoważnione spoza Jednostki.

2. W systemie informatycznym Jednostki przetwarzane są dane osobowe UCZNIÓW I RODZICÓW, DANE OSOBOWE NAUCZYCIELI I POZOSTAŁYCH PRACOWNIKÓW SZKOŁY.

IV. ZASADY PROWADZENIA EWIDENCJI PRACOWNIKÓW ZATRUDNIONYCHPRZY PRZETWARZANIU DANYCH OSOBOWYCH

1. Administrator bezpieczeństwa informacji prowadzi ewidencję wszystkich pracowników Jednostki zatrudnionych przy przetwarzaniu danych osobowych.

2. Powyższa ewidencja uwzględnia:

   - dane personalne pracownika (imię i nazwisko),
   - zakres uprawnienia (nr zbioru)
   - okres upoważnienia
   - program/identyfikator
   - stanowisko
   - podpis

3. Jakakolwiek zmiana informacji wyszczególnionej w ewidencji podlega natychmiastowemu odnotowaniu.

V. CHARAKTERYSTYKA SYSTEMU

1. Sieć informatyczna ma strukturę gwiazdy ze switchem centralnym, do którego podłączony jest serwer oraz komputery stacjonarne i przenośne, a także urządzenia peryferyjne i sieciowe.
2. Sygnał internetowy dostarczany jest przez usługodawcę internetowego i odpowiednio zabezpieczony.
3. System zabezpieczony jest oprogramowaniem antywirusowym zainstalowanym na każdym stanowisku oraz zasilaczami awaryjnymi utrzymującymi stałe zasilanie.

VI.OGÓLNE ZASADY PRACY W SYSTEMIE INFORMATYCZNYM

1. ABI odpowiada za korygowanie niniejszej instrukcji w przypadku uzasadnionych zmian w przepisach prawnych dotyczących przetwarzania danych osobowych w systemach informatycznych, jak również zmian organizacyjno-funkcjonalnych.
2. Przetwarzanie danych w systemie informatycznym może być realizowane wyłącznie poprzez dopuszczone przez ABI do eksploatacji licencjonowane oprogramowanie.
3. ABI prowadzi ewidencję oprogramowania.
4. Do eksploatacji dopuszcza się systemy informatyczne wyposażone w:
    a. mechanizmy kontroli dostępu umożliwiające autoryzację użytkownika, z pominięciem narzędzi do edycji tekstu,
    b. mechanizmy umożliwiające wykonanie kopii bezpieczeństwa oraz archiwizację danych, niezbędne do przywrócenia prawidłowego działania systemu po awarii,
    c. urządzenia niwelujące zakłócenia i podtrzymujące zasilanie,
    d. mechanizmy monitorowania w celu identyfikacji i zapobiegania zagrożeniom, w szczególności pozwalające na wykrycie prób

nieautoryzowanego dostępu do informacji lub przekroczenia przyznanych uprawnień w systemie,

e. mechanizmy zarządzania zmianami.

5. Użytkownikom zabrania się:
   a. korzystania ze stanowisk komputerowych podłączonych do sieci informatycznej poza godzinami i dniami pracy Szkoły bez pisemnej zgody ADO,
   b. udostępniania stanowisk roboczych osobom nieuprawnionym,
   c. wykorzystywania sieci komputerowej Szkoły w celach innych niż wyznaczone przez ADO,
   d. samowolnego instalowania i używania programów komputerowych,
   e. korzystania z nielicencjonowanego oprogramowania oraz wykonywania jakichkolwiek działań niezgodnych z ustawą o ochronie praw autorskich,
   f. umożliwiania dostępu do zasobów wewnętrznej sieci informatycznej Szkoły oraz sieci Internetowej osobom nieuprawnionym,
   g. używania komputera bez zainstalowanego oprogramowania antywirusowego.

VII. PROCEDURY NADAWANIA UPRAWNIEŃ DO PRZETWARZANIA DANYCH I REJESTROWANIA TYCH UPRAWNIEŃ W SYSTEMIE INFORMATYCZNYM ORAZ WSKAZANIE OSOBY ODPOWIEDZIALNEJ ZA TE CZYNNOŚCI

1. Użytkowników systemu informatycznego tworzy oraz usuwa ABI na podstawie zgody ADO.
2. Do przetwarzania danych osobowych zgromadzonych w systemie informatycznym jak również w rejestrach tradycyjnych wymagane jest upoważnienie.

3. Wprowadza się rejestr osób upoważnionych do przetwarzania danych osobowych, który stanowi załącznik nr 3 do niniejszej dokumentacji.
4. Uprawnienia do pracy w systemie informatycznym odbierane są czasowo, poprzez zablokowanie konta w przypadku:
    a. nieobecności pracownika w pracy trwającej dłużej niż 21 dni kalendarzowych,
    b. zawieszenia w pełnieniu obowiązków służbowych.
5. Uprawnienia do przetwarzania danych osobowych odbierane są trwale w przypadku ustania stosunku pracy.
6. Osoby, które zostały upoważnione do przetwarzania danych, są obowiązane zachować w tajemnicy te dane osobowe oraz sposoby ich zabezpieczenia nawet w przypadku ustania stosunku pracy.

VIII. STOSOWANIE METODY I ŚRODKI UWIERZYTELNIENIA ORAZ PROCEDURY ZWIĄZANE Z ICH ZARZĄDZANIEM I UŻYTKOWANIEM

1. System informatyczny przetwarzający dane osobowe wykorzystuje mechanizm identyfikatora i hasła jako narzędzi umożliwiających bezpieczne uwierzytelnienie.
2. Każdy użytkownik systemu informatycznego powinien posiadać odrębny identyfikator.
3. W przypadku zbieżności nadawanego identyfikatora z identyfikatorem wcześniej zarejestrowanego użytkownika ABI, nadaje inny identyfikator odstępując od ogólnej zasady.
4. W identyfikatorze pomija się polskie znaki diakrytyczne.
5. Hasło składa się z co najmniej ośmiu znaków, zawiera co najmniej jedną literę wielką.
6. Zmianę hasła należy dokonywać nie rzadziej niż co 30 dni.
7. Hasła użytkowników generuje ABI i przekazuję wraz z loginem w formie papierowej w zamkniętej kopercie.

8. Po zapoznaniu się z loginem i hasłem użytkownik zobowiązany jest do ich zniszczenia w odpowiednim urządzeniu niszczącym.
9. Hasło nie może być zapisywane i przechowywane.
10. Użytkownik nie może udostępniać identyfikatora oraz haseł osobom nieupoważnionym.

PROCEDURY ROZPOCZĘCIA, ZAWIESZENIA I ZAKOŃCZENIA PRACY.

1. Rozpoczęcie pracy użytkownika w systemie informatycznym obejmuje wprowadzenie identyfikatora i hasła w sposób minimalizujący ryzyko podejrzenia przez osoby nieupoważnione.
2. Użytkownik systemu jest odpowiedzialny za zabezpieczenie danych wyświetlanych przez system przed osobami nie mającymi uprawnień.
3. Zawieszenie pracy polega na opuszczeniu stanowiska pracy bez wylogowania się i jest dopuszczalne tylko w przypadku pozostania w pomieszczeniu. Użytkownik jest zobowiązany w takiej sytuacji do włączenia wygaszacza ekranu odblokowywanego hasłem.
4. Zabrania się opuszczania stanowiska pracy bez wcześniejszego wylogowania z systemu z zastrzeżeniem pkt 3.
5. Zakończenie pracy polega na wylogowaniu się z systemu i wyłączeniu komputera.
6. ABI monitoruje logowanie oraz wylogowanie się użytkowników oraz nadzoruje zakres przetwarzanych przez nich zbiorów danych.

IX. PROCEDURY TWORZENIA KOPII AWARYJNYCH ZBIORÓW DANYCH ORAZ PROGRAMÓW I NARZĘDZI PROGRAMOWYCH SŁUŻĄCYCH DO ICH PRZETWARZANIA

1. Dane osobowe zabezpiecza się poprzez wykonywanie kopii awaryjnych.

2. Ochronie poprzez wykonanie kopii podlegają także programy i narzędzia programowe służące przetwarzaniu danych. Kopie programów i narzędzi wykonywane są zaraz po instalacji oraz po każdej aktualizacji na zewnętrznych, elektronicznych nośnikach informacji.
3. Zabezpieczeniu poprzez wykonywanie kopii awaryjnych podlegają także dane konfiguracyjne systemu informatycznego przetwarzającego dane osobowe, w tym uprawnienia użytkowników systemu.
4. Za proces tworzenia kopii awaryjnych na serwerze odpowiada ABI.
5. W przypadku lokalnego przetwarzania danych osobowych na stacjach roboczych, użytkownicy systemu informatycznego zobowiązani są do wykonywania samodzielnie kopii bezpieczeństwa tych zbiorów.
6. Kopie awaryjne mogą być wykonywane tylko na nośnikach informatycznych dostarczonych przez ABI.
7. Kopie awaryjne mogą być sporządzane automatycznie lub manualnie z wykorzystaniem specjalistycznych urządzeń do wykonywania kopii lub standardowych narzędzi oferowanych przez stacje robocze.
8. Kopie awaryjne wykonuje się po znaczących zmianach w wprowadzonych danych w programie.
9. Kopie awaryjne przechowuje ABI, a w przypadku przetwarzania danych na stacjach roboczych poszczególni użytkownicy. Kopie usuwa się niezwłocznie po ustaniu ich użyteczności.
10. ABI zobowiązany jest do okresowego wykonywania testów odtworzeniowych kopii awaryjnych.
11. Wszelkie wydruki zawierające dane osobowe powinny być przechowywane w miejscu uniemożliwiającym ich odczyt przez osoby nieupoważnione, zaś po upływie czasu ich przydatności – niszczone w niszczarkach dokumentów.

X. SPOSÓB, MIEJSCE I OKRES PRZECHOWYWANIA ELEKTRONICZNYCH NOŚNIKÓW INFORMACJI

1. Nośniki danych oraz programów służących do przetwarzania danych osobowych, a także danych konfiguracyjnych systemu informatycznego, przechowuje ABI w odpowiednio zabezpieczonym pomieszczeniu.
2. Dane osobowe gromadzone są na stacjach roboczych oraz na nośnikach zewnętrznych.
3. Przenośne nośniki danych zabezpieczone są hasłem.
4. Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:
    a. **likwidacji** — pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie,
    b. **przekazania podmiotowi nieuprawnionemu do przetwarzania danych** — pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie,
    c. **naprawy** — pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem ABI.
5. Nośniki kopii awaryjnych, które zostały wycofane z użycia, podlegają zniszczeniu po usunięciu danych osobowych, w odpowiednim urządzeniu niszczącym przez ABI.

XI. SPOSÓB ZABEZPIECZENIA SYSTEMU PRZED DZIAŁALNOŚCIĄ OPROGRAMOWANIA, KTÓREGO CELEM JEST UZYSKANIE NIEUPRAWNIONEGO DOSTĘPU DO SYSTEMU INFORMATYCZNEGO

1. ABI zapewnia ochronę antywirusową oraz zarządza systemem wykrywającym i usuwającym wirusy i inne niebezpieczne kody. System antywirusowy jest skonfigurowany w następujący sposób:
    a. skanowanie dysków zawierających potencjalnie niebezpieczne dane następuje automatycznie po włączeniu komputera,

b. skanowanie wszystkich informacji przetwarzanych w systemie, a zwłaszcza poczty elektronicznej jest realizowane na bieżąco.

c. automatycznej aktualizacji wzorców wirusów.

2. W przypadkach wystąpienia infekcji użytkownik powinien niezwłocznie powiadomić o tym fakcie ABI.
3. W przypadku wystąpienia infekcji i braku możliwości automatycznego usunięcia wirusów przez system antywirusowy, ABI podejmuje działania zmierzające do usunięcia zagrożenia. W szczególności działania te mogą obejmować:

    a. usunięcie zainfekowanych plików, o ile jest to akceptowalne ze względu na prawidłowe funkcjonowanie systemu informatycznego,

    b. odtworzenie plików z kopii awaryjnych po uprzednim sprawdzeniu, czy dane zapisane na kopiach nie są zainfekowane,

    c. samodzielną ingerencję w zawartość pliku - w zależności od posiadanych narzędzi i oprogramowania.

4. Użytkownicy systemu mają również obowiązek skanowania każdego zewnętrznego elektronicznego nośnika informacji, który chcą wykorzystać.
5. ABI monitoruje stan systemu, ruch użytkowników w sieci oraz próby ingerencji z zewnątrz w system.

XII. INFORMACJE O ODBIORCACH, KTÓRYM DANE OSOBOWE ZOSTAŁY UDOSTĘPIONE, DACIE I ZAKRESIE TEGO UDOSTĘPNIENIA

1. Informacje o udostępnieniu danych osobowych przetwarza się i przechowuje w oparciu o Rzeczowy Wykaz Akt i Instrukcję kancelaryjną.
2. Za udostępnianie danych zgodnie z przepisami prawa odpowiedzialny jest ADO.
3. Nadzór nad właściwym udostępnianiem danych prowadzi ABI.

XIII.PRZESYŁANIE DANYCH POZA OBSZAR PRZETWARZANIA

1. Urządzenia i nośniki zawierające dane osobowe, przekazywane poza obszar przetwarzania zabezpiecza się w sposób zapewniający poufność i integralność tych danych, w szczególności poprzez hasło dostępu.
2. W wypadku przesyłania danych osobowych poza sieć przystosowaną do transferu danych osobowych należy zastosować szczególne środki bezpieczeństwa, które obejmują:
    a. zatwierdzenie przez ABI zakresu danych osobowych przeznaczonych do wysłania,
    b. zastosowanie mechanizmów szyfrowania danych osobowych,
    c. zastosowanie mechanizmów podpisu elektronicznego zabezpieczającego transmisje danych osobowych oraz rejestrację transmisji wysyłania danych osobowych.
3. Umożliwienie wysyłania danych osobowych tylko z wykorzystaniem określonej aplikacji i tylko przez określonych użytkowników.

XIV. PROCEDURY WYKONYWANIA PRZEGLĄDÓW I KONSERWACJI SYSTEMÓW ORAZ NOŚNIKÓW INFORMACJI SŁUŻĄCYCH DO PRZETWARZANIA DANYCH

1. Przeglądy i konserwacje systemu oraz nośników informacji służących do przetwarzania danych mogą być wykonywane jedynie przez osoby posiadające upoważnienie wydane przez ADO.
2. Wszelkie prace związane z naprawami i konserwacją systemu informatycznego przetwarzającego dane osobowe muszą uwzględniać zachowanie wymaganego poziomu zabezpieczenia tych danych przed dostępem do nich osób nieupoważnionych, w szczególności poprzez bezpośredni nadzór prowadzony przez ABI.

3. W przypadku uszkodzenia zestawu komputerowego, nośniki danych, na których są przechowywane dane osobowe powinny zostać zabezpieczone przez ABI.
4. W przypadku konieczności przeprowadzenia prac serwisowych poza Szkołą, dane osobowe znajdujące się w naprawianym urządzeniu muszą zostać w sposób trwały usunięte.
5. Jeżeli nie ma możliwości usunięcia danych z nośnika na czas naprawy komputera, należy zapewnić stały nadzór nad tym nośnikiem przez osobę upoważnioną do przetwarzania danych osobowych na nim zgromadzonych.
6. ABI wykonuje okresowy przegląd nośników danych osobowych eliminując te, które nie zapewniają odpowiedniego poziomu bezpieczeństwa oraz niezawodności.

XIV. POSTANOWIENIA KOŃCOWE

1. Każda osoba wpisana do ewidencji zobowiązana jest do odbycia stosownego przeszkolenia w zakresie ochrony danych osobowych oraz zapoznania się z :
    - treścią ustawy oraz rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych;
    - polityką bezpieczeństwa - regulaminem ochrony danych osobowych;
    - instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych;
    - uregulowaniami wewnętrznymi obowiązującymi w tym zakresie.
2. Wykonanie powyższych zobowiązań pracownik potwierdza własnoręcznym podpisem.
3. Wszelkie zagadnienia dotyczące ochrony danych osobowych nie ujęte w niniejszej „Instrukcji" należy rozpatrywać zgodnie z treścią

aktów prawnych wymienionych w regulaminie ochrony danych osobowych", z uwzględnieniem późniejszych zmian i uzupełnień.

4. Instrukcja niniejsza wchodzi w życie z dniem zatwierdzenia jej przez Dyrektora Jednostki (administratora danych osobowych).