Załącznik nr 12
do Polityki bezpieczeństwa przetwarzania danych osobowych
w Liceum Ogólnokształcącym Nr II
im. Joachima Chreptowicza
w Ostrowcu Świętokrzyskim

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

§1

Definicje:

1) **Administrator Danych Osobowych**, **Administrator lub Szkoła** – Liceum Ogólnokształcące Nr II im. Joachima Chreptowicza w Ostrowcu Świętokrzyskim;
2) **Administrator Systemu Informatycznego (ASI)** – osoba, podmiot nadzorujący i odpowiadający za poprawną pracę powierzonego mu sprzętu sieciowego oraz systemu operacyjnego, oprogramowania instalowanego w danej jednostce organizacyjnej;
3) **dane osobowe** – wszelkie informacje 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) **odbiorcy danych** – każdy, komu udostępnia się dane osobowe, z wyłączeniem: osoby, której dane dotyczą; osoba upoważniona do przetwarzania danych; osoba, której powierzono przetwarzanie danych; organy państwowe lub organy samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem;
7) **osoba upoważniona do przetwarzania danych osobowych** – pracownik szkoły, który upoważniony został do przetwarzania danych osobowych przez ADO na piśmie;
8) **poufność danych** – właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom;

9) **przetwarzanie danych** – czynności takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, modyfikowanie, udostępnianie oraz usuwanie, a zwłaszcza te, które wykonują się w systemach informatycznych;
10) **raport** – przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzanych danych;
11) **serwisant** – firma lub pracownik firmy, zajmującej się instalacją, naprawą i konserwacją sprzętu komputerowego;
12) **sieć publiczna** – sieć telekomunikacyjna, wykorzystywana głównie do świadczenia publicznie dostępnych usług telekomunikacyjnych;
13) **system informatyczny** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
14) **teletransmisja** – przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej;
15) **uwierzytelnianie** – działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;
16) **użytkownik** – pracownik Szkoły, upoważniony do przetwarzania danych osobowych zgodnie z zakresem obowiązków, któremu nadano identyfikator i przyznano hasło;
17) **zbiór danych osobowych** – każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.

Rozdział 1

Cele wprowadzenia i zakres zastosowania Instrukcji Zarządzania Systemem Informatycznym

§2

1. Instrukcja Zarządzania Systemem Informatycznym, służącym do przetwarzania danych osobowych w Liceum Ogólnokształcącym Nr II im. Joachima Chreptowicza w Ostrowcu Świętokrzyskim, zwana dalej „Instrukcją", określa zasady, tryb postępowania i zalecenia Administratora Danych Osobowych, które muszą być stosowane przez osoby przez niego upoważnione do przetwarzania danych osobowych w systemach informatycznych.
2. Podstawowymi celami zabezpieczeń systemów informatycznych służących do przetwarzania danych osobowych jest zapewnienie jak najwyższego poziomu bezpieczeństwa przetwarzanych danych osobowych w systemach informatycznych.
3. Za priorytet uznano zagwarantowanie zgromadzonym danym osobowym, przez cały okres ich przetwarzania w systemach, charakteru poufnego wraz z zachowaniem ich integralności i rozliczalności.
4. Instrukcja jest dokumentem powiązanym z „Polityką bezpieczeństwa przetwarzania danych osobowych" w Liceum Ogólnokształcącym Nr II im. Joachima Chreptowicza w Ostrowcu Świętokrzyskim.
5. Niniejsza Instrukcja znajduje zastosowanie do systemów informatycznych, stosowanych w Szkole, w których są przetwarzane dane osobowe.

Rozdział 2

Nadawanie i wycofywanie uprawnień do przetwarzania danych w systemie informatycznym

Nadawanie uprawnień

§3

1. Dostęp do systemu informatycznego, służącego do przetwarzania danych osobowych, może uzyskać wyłącznie osoba upoważniona przez Administratora do przetwarzania danych osobowych.
2. Dostęp do systemu informatycznego, o którym mowa w ust. 1, zostaje udzielony poprzez nadanie uprawnień użytkownika.
3. Nadanie uprawnień użytkownika polega na przypisaniu do użytkownika indywidualnego identyfikatora i hasła oraz wprowadzeniu tych danych do bazy użytkowników systemu.
4. Za przydzielenie i wygenerowanie identyfikatora i hasła użytkownikowi, który będzie korzystał z systemu informatycznego, odpowiada ASI.
5. Nadanie, zmiana, zawieszenie lub wycofanie uprawnień użytkownika następuje na pisemne polecenie Administratora, którego wzór stanowi załącznik nr 18 do Polityki bezpieczeństwa przetwarzania danych osobowych.

Wycofywanie uprawnień

§4

1. Wycofania uprawnień użytkownika do przetwarzania danych osobowych w systemie informatycznym dokonuje Administrator lub upoważniona przez niego osoba.
2. Wycofanie uprawnień, o którym jest mowa w ust. 1, może mieć charakter czasowy lub trwały.
3. Wycofanie uprawnień następuje przez:
   1) zablokowanie konta użytkownika do czasu ustania przyczyny, uzasadniającej blokadę (wycofanie czasowe);
   2) usunięcie danych użytkownika z bazy użytkowników systemu (wycofanie trwałe).
4. Czasowe wycofanie uprawnień użytkownika następuje w razie:

1) nieobecności użytkownika w pracy, trwającej dłużej niż 90 dni kalendarzowych;
2) zawieszenia w pełnieniu obowiązków służbowych.

5. Przyczyną czasowego wycofania uprawnień użytkownika może być w szczególności:
   1) wypowiedzenie umowy o pracę;
   2) wszczęcie postępowania dyscyplinarnego.
6. Przyczyną trwałego wycofania uprawnień użytkownika jest rozwiązanie lub wygaśnięcie stosunku pracy lub innego stosunku prawnego, w ramach którego zatrudniony był użytkownik.

Rozdział 3

Metody i środki uwierzytelnienia

§5

1. Każdy użytkownik systemu informatycznego otrzymuje od Administratora lub osoby przez niego upoważnionej identyfikator i hasło wstępne (tymczasowe, wymagające zmiany przy pierwszym logowaniu).
2. Identyfikatory i hasła są sposobem zagwarantowania rozliczalności, poufności i integralności danych osobowych przetwarzanych w systemach informatycznych. Służą do weryfikowania tożsamości użytkownika, uzyskania dostępu do określonych zasobów, kont uprzywilejowanych lub uruchomienia określonej funkcjonalności.
3. Mając na uwadze zagwarantowanie wysokiego poziomu bezpieczeństwa przetwarzania danych osobowych oraz zagwarantowania użytkownikom pełnej rozliczalności wykonywanych przez nich operacji w systemach informatycznych, wszyscy użytkownicy przy uwierzytelnianiu do systemów informatycznych powinni stosować się do poniższych zasad:
   1) użytkownik systemu powinien posiadać unikalny identyfikator do swojego osobistego i wyłącznego użytku;
   2) hasła dostępu do systemów informatycznych powinny być tworzone przez użytkownika i stanowią tajemnicę służbową;
   3) użytkownik ponosi pełną odpowiedzialność za utworzenie hasła dostępu oraz jego przechowywanie;
   4) hasła nie mogą być ujawniane lub przekazywane komukolwiek, bez względu na okoliczności;
   5) użytkownik nie powinien przechowywać haseł w widocznych miejscach, nie powinien umieszczać haseł w żadnych automatycznych procesach logowania (skryptach, makrach lub pod klawiszami funkcyjnymi).

4. Hasło użytkownika powinno składać się z unikalnego zestawu znaków (litery, cyfry, znaki specjalne). Hasło nie może być identyczne z identyfikatorem użytkownika ani jego imieniem lub nazwiskiem.
5. Zabrania się użytkownikom systemu udostępniania swojego identyfikatora i hasła innym osobom oraz korzystania z identyfikatora lub hasła innego użytkownika.
6. Zmiana haseł w systemie następuje nie rzadziej niż co 90 dni.
7. Użytkownicy są odpowiedzialni za wszelkie działania w systemach informatycznych prowadzone z użyciem ich identyfikatora i hasła.
8. Administrator Systemu Informatycznego jest odpowiedzialny za okresowe sprawdzanie, usuwanie lub blokowanie zbędnych identyfikatorów użytkowników oraz kont w systemach.

Rozdział 4

Procedury bezpieczeństwa, związane z przetwarzaniem danych osobowych

Stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem

§ 6

1. Dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po podaniu identyfikatora i właściwego hasła.
2. Identyfikator jest w sposób jednoznaczny przypisany użytkownikowi. Użytkownik odpowiada za wszystkie czynności wykonane przy użyciu identyfikatora, którym się posługuje.
3. Nazwy i hasła użytkowników, posiadających uprawnienia do informatycznego przetwarzania danych osobowych, powinny być przechowywane w zamkniętej szafie, do której dostęp jest w pełni kontrolowany, przy czym dostęp do nich mają wyłącznie osoby uprawnione. Nazwy i hasła użytkowników powinny być przechowywane w opieczętowanej i opatrzonej pieczęcią szkoły i podpisem Administratora kopercie.

Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu

§ 7

1. Przed rozpoczęciem pracy, w trakcie rozpoczynania pracy z systemem informatycznym oraz w trakcie pracy każdy pracownik jest obowiązany do zwrócenia bacznej uwagi, czy nie wystąpiły symptomy, mogące świadczyć o naruszeniu ochrony danych osobowych. Na fakt naruszenia zabezpieczeń systemu mogą wskazywać:
   1) nietypowy stan stacji roboczej (np. brak zasilania, problemy z uruchomieniem);
   2) wszelkiego rodzaju różnice w funkcjonowaniu systemu (np. komunikaty informujące o błędach, brak dostępu do funkcji systemu, nieprawidłowości w wykonywanych operacjach);
   3) różnice w zawartości zbioru danych osobowych (np. brak lub nadmiar danych);
   4) inne nadzwyczajne sytuacje.
2. Rozpoczęcie pracy użytkownika w systemie informatycznym obejmuje wprowadzenie identyfikatora i hasła w sposób minimalizujący ryzyko podejrzenia przez osoby nieupoważnione oraz ogólne stwierdzenie poprawności działania systemu.
3. Maksymalna liczba prób wprowadzenia hasła przy logowaniu się do systemu wynosi trzy. Po przekroczeniu tej liczby prób logowania system blokuje dostęp do zbioru danych na poziomie danego użytkownika. Odblokowania konta może dokonać Administrator Systemu Informatycznego w porozumieniu z Administratorem Danych Osobowych. Użytkownik informuje Administratora Danych Osobowych o zablokowaniu dostępu do zbioru danych.
4. Zmianę użytkownika stacji roboczej każdorazowo musi poprzedzać wylogowanie się poprzedniego użytkownika. Niedopuszczalne jest, aby dwóch lub większa liczba użytkowników wykorzystywała wspólne konto użytkownika.
5. W przypadku, gdy przerwa w pracy na stacji roboczej trwa dłużej niż 30 minut, użytkownik obowiązany jest wylogować się z aplikacji i systemu stacji roboczej, na której pracuje, oraz sprawdzić, czy nie zostały pozostawione bez zamknięcia nośniki informacji, zawierające dane osobowe. W pomieszczeniach, w których przetwarzane są dane i w których jednocześnie mogą przebywać osoby postronne, monitory stanowisk dostępu do danych powinny być ustawione w taki sposób, żeby uniemożliwić tym osobom wgląd w dane. 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.

6. Zakończenie pracy użytkownika w systemie informatycznym obejmuje wylogowanie się użytkownika z aplikacji służącej do przetwarzania danych osobowych oraz wylogowanie z systemu operacyjnego.

Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych, służących do ich przetwarzania

§ 8

1. Dane osobowe, przetwarzane w systemie informatycznym, podlegają zabezpieczeniu poprzez tworzenie kopii zapasowych. Za proces tworzenia kopii zapasowych odpowiada Administrator Systemu Informatycznego lub osoba specjalnie w tym celu wyznaczona.
2. Kopie zapasowe informacji przechowywanych w systemie informatycznym, przetwarzającym dane osobowe, tworzone są w następujący sposób:
   1) kopia zapasowa aplikacji przetwarzającej dane osobowe – pełna kopia wykonywana jest po wprowadzeniu zmian do aplikacji, kopie umieszczone są na nośnikach wymiennych, kopia przechowywana jest w szafie pancernej, w sekretariacie szkoły.
   2) kopia zapasowa danych osobowych przetwarzanych przez aplikację (pełna kopia) wykonywana jest codziennie na dysku komputera wybranego przez Administratora Systemu Informatycznego;
   3) zbiorcze (tygodniowe) kopie przechowywane są przez okres dwóch tygodni, po tym terminie stare kopie są niszczone poprzez nadpisywanie ich przez bardziej aktualne.
3. W przypadku przechowywania kopii zapasowych przez okres dłuższy niż pół roku, wszystkie kopie zapasowe zbiorów danych osobowych, aplikacji przetwarzających dane osobowe oraz danych konfiguracyjnych systemu informatycznego, przetwarzającego dane osobowe, których to dotyczy, muszą być okresowo (co najmniej raz na pół roku) sprawdzane pod względem ich dalszej przydatności. Czynności te wykonuje Administrator Systemu Informatycznego lub osoba przez niego upoważniona.
4. Nośniki kopii zapasowych, które zostały wycofane z użycia, jeżeli jest to możliwe, należy pozbawić zapisanych danych za pomocą specjalnego oprogramowania do bezpiecznego usuwania zapisanych danych. W przeciwnym wypadku podlegają fizycznemu zniszczeniu z wykorzystaniem metod adekwatnych do typu nośnika, w sposób uniemożliwiający odczytanie zapisanych danych.

Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych

§ 9

1. Nośniki danych zarówno w postaci elektronicznej, jak i papierowej powinny być zabezpieczone przed dostępem osób nieuprawnionych, nieautoryzowaną modyfikacją i zniszczeniem. Dane osobowe mogą być zapisywane na nośnikach przenośnych w przypadku tworzenia kopii zapasowych lub gdy istnieje konieczność przeniesienia tych danych w postaci elektronicznej, a wykorzystanie do tego celu sieci informatycznej jest nieuzasadnione, niemożliwe lub zbyt niebezpieczne.
2. Nośniki danych osobowych oraz wydruki powinny być przechowywane w zamkniętych szafach i nie powinny być bez uzasadnionej przyczyny wynoszone poza ten obszar. Przekazywanie nośników danych osobowych i wydruków poza budynek szkoły powinno odbywać się za wiedzą Administratora Danych Osobowych.
3. W przypadku, gdy nośnik danych osobowych nie jest dłużej potrzebny, należy przeprowadzić zniszczenie nośnika lub usunięcie danych z nośnika zgodnie ze wskazówkami umieszczonymi w § 8 ust. 4. Jeżeli wydruk danych osobowych nie jest dłużej potrzebny, należy przeprowadzić zniszczenie wydruku przy użyciu niszczarki dokumentów.
4. W przypadku, gdy kopia zapasowa nie jest dłużej potrzebna, należy przeprowadzić jej zniszczenie lub usunięcie danych z nośnika, na którym się ona znajduje, zgodnie ze wskazówkami umieszczonymi w § 8 ust. 4.

Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego

§ 10

1. W związku z tym, że system informatyczny narażony jest na działanie oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do tego systemu, konieczne jest podjęcie odpowiednich środków ochronnych.
2. Można wyróżnić następujące rodzaje występujących zagrożeń związanych z nieuprawnionym dostępem bezpośrednio do bazy danych:
   1) uszkodzenie kodu aplikacji, umożliwiającej dostęp do bazy danych w taki sposób, że przetwarzane dane osobowe ulegną zafałszowaniu lub zniszczeniu;

2) przechwycenie danych podczas transmisji w przypadku rozproszonego przetwarzania danych z wykorzystaniem ogólnodostępnej sieci Internet;
3) przechwycenie danych z aplikacji, umożliwiającej dostęp do bazy danych na stacji roboczej wykorzystywanej do przetwarzania danych osobowych przez wyspecjalizowany program szpiegowski i nielegalne przesłanie tych danych poza miejsce przetwarzania danych;
4) uszkodzenie lub zafałszowanie danych osobowych przez wirus komputerowy, zakłócający pracę aplikacji, umożliwiającej dostęp do bazy danych na stacji roboczej wykorzystywanej do przetwarzania danych osobowych.

3. W celu przeciwdziałania wymienionym zagrożeniom system informatyczny musi posiadać następujące zabezpieczenia:
   1) autoryzację użytkowników przy zachowaniu odpowiedniego poziomu komplikacji haseł dostępu;
   2) stosowanie szyfrowanej transmisji danych przy zastosowaniu odpowiedniej długości klucza szyfrującego;
   3) stosowanie odpowiedniej ochrony antywirusowej na stacjach roboczych wykorzystywanych do przetwarzania danych osobowych.
4. Potencjalnymi źródłami przedostawania się programów szpiegowskich oraz wirusów komputerowych na stacje robocze są:
   1) załączniki do poczty elektronicznej;
   2) przeglądane strony internetowe;
   3) pliki i aplikacje, pochodzące z nośników wymiennych, uruchamiane i odczytywane na stacji roboczej.
5. W celu zapewnienia ochrony antywirusowej Administrator Systemu Informatycznego lub osoba specjalnie do tego celu wyznaczona jest odpowiedzialny za zarządzanie systemem wykrywającym i usuwającym wirusy. System antywirusowy powinien być skonfigurowany w następujący sposób:
   1) rezydentny monitor antywirusowy (uruchomiony w pamięci operacyjnej stacji roboczej) powinien być stale włączony;
   2) antywirusowy skaner ruchu internetowego powinien być stale włączony;
   3) monitor antywirusowy, zapewniający ochronę przed wirusami w dokumentach Microsoft Office, powinien być stale włączony;
   4) skaner poczty elektronicznej powinien być stale włączony.

6. Systemy antywirusowe, zainstalowane na stacjach roboczych, powinny być skonfigurowane w sposób następujący:
   1) zablokowanie możliwości ingerencji użytkownika w ustawienia oprogramowania antywirusowego;
   2) ustawienie automatycznej aktualizacji baz wirusów.
7. System antywirusowy powinien być aktualizowany na podstawie materiałów publikowanych przez producenta oprogramowania.
8. Użytkownicy systemu informatycznego zobowiązani są do następujących działań:
   1) skanowania zawartości dysków stacji roboczej, pracującej w systemie informatycznym pod względem potencjalnie niebezpiecznych kodów – przynajmniej 2 razy w tygodniu;
   2) skanowania zawartości nośników wymiennych odczytywanych na stacji roboczej, pracującej w systemie informatycznym, pod względem potencjalnie niebezpiecznych kodów – przy każdym odczycie;
   3) skanowanie informacji przesyłanych do systemu informatycznego pod kątem pojawienia się niebezpiecznych kodów – na bieżąco.
9. W przypadku wystąpienia infekcji i braku możliwości automatycznego usunięcia wirusów przez system antywirusowy, Administrator Systemu Informatycznego lub inny wyznaczony pracownik powinien podjąć działania, zmierzające do usunięcia zagrożenia. W szczególności działania te mogą obejmować:
   1) usunięcie zainfekowanych plików, o ile jest to akceptowalne ze względu na prawidłowe funkcjonowanie systemu informatycznego;
   2) odtworzenie plików z kopii zapasowych po uprzednim sprawdzeniu, czy dane zapisane na kopiach nie są zainfekowane;
   3) samodzielną ingerencję w zawartość pliku – w zależności od posiadanych kwalifikacji lub skonsultowanie się z zewnętrznymi ekspertami.
10. System informatyczny przetwarzający dane osobowe powinien posiadać mechanizmy pozwalające na zabezpieczenie ich przed utratą lub wystąpieniem zafałszowania w wyniku awarii zasilania lub zakłóceń w sieci zasilającej. W związku z tym system informatyczny powinien być wyposażony w system zasilania awaryjnego UPS lub listwy zabezpieczające stacje robocze przed skutkami przepięcia.

Wymogi dotyczące zmiany haseł

§ 11

1. Użytkownik jest zobowiązany zmieniać hasło, w którego posiadaniu się znajduje:
   1) okresowo, zgodnie z wymaganiami dla danego systemu informatycznego (przed upływem terminu ważności hasła);
   2) w przypadku ujawnienia lub podejrzenia ujawnienia hasła osobom nieupoważnionym.
2. W przypadku braku dostępu do konta chronionego hasłem, w którego posiadaniu się znajduje, użytkownik zobowiązany jest wystąpić o zmianę hasła do ASI, w sytuacji:
   1) zapomnienia/zgubienia hasła;
   2) wygaśnięcia ważności hasła;
   3) zablokowania konta spowodowanego nieprawidłowym wprowadzeniem hasła;
   4) braku uprawnień/interfejsu umożliwiających samodzielną zmianę hasła.
3. Zmiana haseł użytkowników powinna być wymuszana przez system co 90 dni. W przypadku braku wymuszenia przez system, użytkownik sam jest zobowiązany do zmiany hasła co 90 dni.

§ 12

1. System informatyczny przetwarzający dane osobowe musi posiadać mechanizm uwierzytelniający użytkownika, wykorzystujący identyfikator i hasło. Powinien także posiadać mechanizmy, pozwalające na określenie uprawnień użytkownika do korzystania z przetwarzanych informacji (np. prawo do odczytu danych, modyfikacji istniejących danych, tworzenia nowych danych, usuwania danych).

Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych

§ 13

1. Wszelkie prace związane z naprawami i konserwacją systemu informatycznego, przetwarzającego dane osobowe, muszą uwzględniać wymagany poziom zabezpieczenia tych danych przed dostępem do nich osób nieupoważnionych.
2. Prace serwisowe na terenie Szkoły, prowadzone w tym zakresie, mogą być wykonywane wyłącznie przez jej pracowników lub przez upoważnionych przedstawicieli wykonawców zewnętrznych w obecności pracowników Szkoły.

3. Przed rozpoczęciem prac serwisowych przez osoby spoza Szkoły konieczne jest potwierdzenie tożsamości serwisantów.
4. Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:
   1) likwidacji – pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie;
   2) przekazania podmiotowi nieuprawnionemu do przetwarzania danych – pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie;
   3) naprawy – pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez ADO.

Rozdział 5

Stosowane środki bezpieczeństwa

§ 14

1. W Szkole stosuje się następujące środki bezpieczeństwa:
   1) zabezpieczenie obszaru, w którym przetwarzane są dane osobowe, przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych;
   2) przebywanie osób nieuprawnionych jest dopuszczalne za zgodą ADO lub w obecności osoby upoważnionej do przetwarzania danych osobowych;
   3) stosowane są mechanizmy kontroli dostępu do danych;
   4) identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie jest przydzielany innej osobie;
   5) w przypadku, gdy do uwierzytelniania użytkowników używa się hasła, jego zmiana następuje nie rzadziej niż co 90 dni.
   6) dane osobowe przetwarzane w systemie informatycznym zabezpiecza się przez wykonywanie kopii zapasowych zbiorów danych oraz programów, służących do przetwarzania danych osobowych;
   7) kopie zapasowe przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem oraz usuwa się niezwłocznie po ustaniu ich użyteczności;

8) ADO monitoruje wdrożone zabezpieczenia systemu informatycznego;
9) 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 osoby upoważnionej przez ADO;
10) urządzenia i nośniki, zawierające dane osobowe, zabezpiecza się w sposób zapewniający poufność i integralność tych danych;
11) ADO stosuje środki kryptograficznej ochrony wobec danych wykorzystywanych do uwierzytelnienia, które są przesyłane w sieci publicznej.

Rozdział 7

Zalecenia w zakresie przetwarzania danych osobowych sposobem tradycyjnym

§ 15

1. Miejscem przetwarzania dokumentacji dotyczącej danych osobowych sposobem tradycyjnym są pomieszczenia w szkole: gabinet dyrektora, gabinet wicedyrektora, pokój głównego księgowego, sekretariat, gabinet pedagoga, gabinet psychologa, gabinet pielęgniarki szkolnej, biblioteka, pokój nauczycielski, pokój nauczycieli wychowania fizycznego, archiwum zakładowe, sale lekcyjne.
2. Osoby prowadzące dokumentację zobowiązane są do zachowania tajemnicy służbowej.
3. Dokumentacji, o której mowa w ust. 1, nie można wynosić poza teren Szkoły poza prawnie uzasadnionymi przypadkami.
4. Dokumentację, o której mowa w ust. 1, archiwizuje się zgodnie z Instrukcją kancelaryjną.
5. Osoby prowadzące dokumentację zobowiązane są do niezwłocznego poinformowania ADO o podejrzeniu dostępu do dokumentacji przez osoby nieupoważnione.

Rozdział 8

Zasady postępowania z komputerem przenośnym

§ 16

1. Osoba używająca komputera przenośnego, zawierającego dane osobowe, zobowiązana jest zachować szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem przetwarzania danych osobowych.
2. Osoba używająca komputera przenośnego, zawierającego dane osobowe, powinna w szczególności:
   1) zabezpieczyć dostęp do komputera na poziomie systemu operacyjnego za pomocą identyfikatora i hasła;
   2) nie zezwalać na używanie komputera osobom nieupoważnionym do dostępu do danych osobowych;
   3) nie wykorzystywać komputera przenośnego do przetwarzania danych osobowych w obszarach użyteczności publicznej;
   4) zachować szczególną ostrożność przy podłączaniu do sieci publicznych poza obszarem przetwarzania danych osobowych.
3. W przypadku podłączania komputera przenośnego do sieci publicznej poza siecią Szkoły należy stosować firewall zainstalowany bezpośrednio na tym komputerze oraz system antywirusowy.
4. Użytkownik powinien zachować wyjątkową ostrożność podczas korzystania z zasobów sieci publicznej.
5. Za wszelkie działania wykonywane na komputerze przenośnym odpowiada jego formalny użytkownik.

Rozdział 9

Postanowienia końcowe

§ 17

1. Osobą odpowiedzialną za przegląd przestrzegania Instrukcji, przegląd jej aktualności oraz aktualizację, a także nadawanie praw dostępu do systemu informatycznego jest Administrator Systemu Informatycznego lub inna osoba upoważniona przez Administratora Danych Osobowych.
2. W sprawach nieokreślonych niniejszą Instrukcją należy stosować instrukcje obsługi i zalecenia producentów aktualnie wykorzystywanych urządzeń i programów.
3. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest zapoznać się przed dopuszczeniem do przetwarzania danych z niniejszą instrukcją oraz złożyć stosowne oświadczenie, potwierdzające znajomość jej treści.
4. Niezastosowanie się do procedur określonych w niniejszej Instrukcji przez pracowników upoważnionych do przetwarzania danych osobowych może być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, skutkujące rozwiązaniem stosunku pracy bez wypowiedzenia na podstawie art. 52 Kodeksu pracy.