**INSTRUKCJA**

**organizacji przetwarzania danych osobowych**

**w Zespole Szkół Ogólnokształcących nr 5**

**z oddziałami integracyjnymi i specjalnymi**

**w Sosnowcu**

Podstawa prawna:

1. *Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. 2018, poz. 1000)*
2. *Ustawa z dnia 26 czerwca 1974 r. Kodeks Pracy (Dz.U. 2018, poz. 917, 1000, 1076)*
3. *Rozporządzenie Ministra Pracy i Polityki Socjalnej z dnia 28 maja 1996 r. w sprawie zakresu prowadzenia przez pracodawców dokumentacji w sprawach związanych ze stosunkiem pracy oraz sposobu prowadzenia akt osobowych pracownika (Dz.U. 1996 nr 62, poz. 286 z późn. zm.)*
4. *Rozporządzenie Ministra Edukacji Narodowej z dnia 19 kwietnia 1999 r. w sprawie zakresu prowadzenia przez pracodawców dokumentacji w sprawach związanych ze stosunkiem pracy oraz sposobu prowadzenia akt osobowych pracownika (Dz.U. 1999, nr 41, poz. 414)*

**SPIS TREŚCI**

Rozdział 1. Postanowienia ogólne. Określenia i skróty użyte w Instrukcji i innych dokumentach związanych z ochrona danych osobowych .

Rozdział 2. Ogólne zasady przetwarzania danych osobowych.

Rozdział 3. Procedury tworzenia i zmian w przetwarzaniu danych osobowych w zbiorach.

Rozdział 4. Szkolenie osób w zakresie przetwarzania danych osobowych.

Rozdział 5. Dokumentacja przetwarzania danych osobowych.

Rozdział 6. Obowiązki osób odpowiedzialnych za ochronę danych osobowych.

Rozdział 7. Postanowienia końcowe.

Rozdział 8. Wykaz załączników.

**Rozdział 1**

**POSTANOWIENIA OGÓLNE**

* + **1**

1. Instrukcja organizacji przetwarzania danych osobowych w Zespole Szkół Ogólnokształcących nr 5 z oddziałami integracyjnymi i specjalnymi w Sosnowcu zwana dalej Instrukcją, określa ogólne zasady i cele przetwarzania danych oraz w skazuje działania podejmowane przez Administratora Danych Osobowych oraz osoby przez niego upoważnione w zakresie organizacji przetwarzania i ochrony danych osobowych w Szkole.
2. Instrukcja została opracowana na podstawie ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych w celu określenia zadań organizacyjnych i technicznych realizowanych w zakresie ochrony danych w Szkole.

**Określenia i skróty użyte w Instrukcji:**

* + **2**

1. Zespół Szkół Ogólnokształcących nr 5 w Sosnowcu z oddziałami integracyjnymi i specjalnymi - zwane dalej **Szkołą**.
2. Ustawa o ochronie danych osobowych z dnia 10 maja 2018, zwana dalej **Ustawą**.
3. **Administrator Danych Osobowych** (zwany dalej **Administrator Danych)** - podmiot, którydecyduje o środkach i celach przetwarzania danych osobowych, reprezentowany przez Dyrektor Szkoły.
4. **Administrator Bezpieczeństwa Informacji** (zwany dalej **Administrator Bezpieczeństwa**) -osoba wyznaczona przez dyrektora, odpowiedzialna za nadzorowanie stosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych, w tym w szczególności za przeciwdziałanie dostępowi osób trzecich do systemu, w którym przetwarzane są dane osobowe oraz za podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie ochrony danych osobowych.
5. **Administrator Systemu Informatycznego** (zwany dalej **Administrator Systemu)** - wyznaczeniprzez Administratora Danych pracownicy, odpowiedzialni za funkcjonowanie infrastruktury informatycznej, na którą składa się cały sprzęt informatyczny oraz systemy i aplikacje informatyczne, za ich przeglądy, konserwację oraz za stosowanie technicznych i organizacyjnych środków bezpieczeństwa w systemach informatycznych
6. **Osoba upoważniona** lub **użytkownik** systemu, osoba posiadająca upoważnienie przezAdministratora Danych i uprawniona do przetwarzania danych osobowych w zakresie wskazanym w upoważnieniu.
7. **Reprezentant** - rozumie sięprzez to osobęuprawnionądo składania oświadczeńwoli w imieniuadministratora danych.
8. **Osoba nieuprawniona** - rozumie sięprzez to osobęnie zatrudnionąprzy gromadzeniu lub przetwarzaniu danych (z wyłączeniem osoby uprawnionej do ich przeglądania i przetwarzania na mocy odrębnych przepisów), a tak że osobę, której dane osobowe nie podlegają przetwarzaniu we właściwych zbiorach danych.
9. **System informatyczny** - rozumie sięprzez to zespół współpracujących ze sobąurządzeń,programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
10. **Zabezpieczenie danych w systemie**, rozumie sięprzez to wdrożenie i eksploatacjęstosownychśrodków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem.
11. **Dane osobowe** - każda informacja dotyczącażyjącej osoby fizycznej, która pozwala nabezpośrednią lub pośrednią identyfikacje tej osoby.
12. **Dane sensytywne** - dane podlegające szczególnej ochronie, w rozumieniu art. 27 Ustawy.
13. **Integralność danych** - właściwośćzapewniająca,że dane nie zostały zmienione lub zniszczone wsposób nieautoryzowany.
14. **Poufność** - właściwośćzapewniająca,że informacja (np. dane osobowe) jest dostępna jedynieosobom upoważnionym.
15. **Rozliczalność** – właściwośćzapewniająca,że działania podmiotu mogąbyćprzypisane w sposóbjednoznaczny tylko temu podmiotowi
16. **Naruszenie ochrony danych osobowych** - zamierzone lub przypadkowe naruszenieśrodków technicznych i organizacyjnych zastosowanych w celu ochrony danych. W szczególności, gdy stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej mogą wskazywać na naruszanie ochrony danych osobowych.
17. **Przetwarzanie danych** - jakiekolwiek operacje wykonywane na danych osobowych, takie jakzbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych.
18. **Usuwanie danych** - rozumie sięprzez to zniszczenie danych osobowych lub takąichmodyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą.
19. **Zgoda osoby**, której dane dotyczą- rozumie sięprzez to oświadczenie woli, którego treściąjestzgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie; zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści; zgoda może być odwołana w każdym czasie.
    * **3**
20. Administrator Danych może upoważnić osoby zatrudnione w Szkole do wykonywania określonych czynności, znajdujących się w zakresie zadań Administratora Danych.

2. Kontrola prawidłowości wykonywania czynności, o których mowa w ust. 1 należy do Administratora Danych.

**Rozdział 2**

**OGÓLNE ZASADY PRZETWARZANIA DANYCH OSOBOWYCH**

* + **4**

1. Każdy uczeń i pracownik Szkoły ma prawo do ochrony danych osobowych, które go dotyczą.
2. Pełnoletni uczeń, rodzic (opiekun prawny) ucznia niepełnoletniego oraz pracownik szkoły w formie pisemnej wyrażają zgodę na przetwarzanie danych osobowych.
3. Dane osobowe są przetwarzane w Szkole w celu realizacji zadań określonych przepisami prawa.
4. Cel, o którym mowa w ust. 3, należy osiągać przez zachowanie szczególnej staranności w realizacji przedsięwzięć dotyczących ochrony interesów osób, których dane dotyczą oraz przestrzegania zasad bezpieczeństwa przetwarzania danych osobowych, uwzględniając:
   1. przepisy prawa,
   2. zasady udostępniania danych osobowych,
   3. dotrzymanie okresu przechowywania danych identyfikujących osobę,
   4. procedury ochrony danych osobowych.
      * **5**
5. Naczelną zasadą przetwarzania danych osobowych w Szkole jest zachowanie w tajemnicy przez osoby mające dostęp do danych wszelkich informacji dotyczących ich przetwarzania oraz sposobów zabezpieczania.
6. Możliwość wystąpienia zagrożeń danych przetwarzanych w systemach lub kartotekach, skorowidzach, księgach, wykazach i innych zbiorach ewidencyjnych na użytkowników i ich przełożonych obowiązek wykonywania czynności związanych z zapewnieniem danym właściwej ochrony.
7. Przesyłanie danych osobowych za pomocą urządzeń telekomunikacyjnych lub transmisji danych w sieci publicznej wymaga wykorzystania odpowiednich urządzeń i przedsięwzięć zabezpieczających poufność i integralność ich przekazu.
8. Przekazywanie danych osobowych w formie papierowej do organu prowadzącego i innych instytucji współpracujących ze Szkołą dokonywane jest wyłącznie przez osoby posiadające upoważnienia w zabezpieczonych kopertach z nadrukiem: Dane osobowe.
9. Kopiowanie danych osobowych oraz wykonywanie wydruków jest zabronione, chyba że konieczność ich sporządzania wynika z nałożonych na użytkownika obowiązków i dozwolona jest przepisami prawa.
10. Kopie zawierające dane osobowe można przekazywać tylko osobom upoważnionym lub podmiotom do tego uprawnionym.
11. Kopie, o których mowa w ust. 5, mogą być wykorzystywane tylko w celach, do jakich zostały sporządzone. Niepotrzebne kopie należy niszczyć w sposób uniemożliwiający ich odtworzenie

**§ 6**

**Nadawanie upoważnień osobom do przetwarzania danych osobowych**

Przetwarzanie danych osobowych może być wykonywane wyłącznie przez osoby posiadające upoważnienie nadane przez Administratora Danych

1. Procedury nadawania w Szkole upoważnień dostępu do przetwarzania danych

osobowych obejmują:

* 1. wydanie przez Administratora Danych upoważnienia do przetwarzania danych osobowych pracownikom administracji przetwarzającym dane (załącznik nr 4)
  2. podpisanie przez osobę, do której obowiązków należy przetwarzanie danych osobowych, oświadczenia o zachowaniu w tajemnicy danych osobowych oraz zasad ich przetwarzania, sposobów ich zabezpieczania, obejmującej także okres po ustaniu stosunku pracy; oświadczenie takie podpisują wszyscy pracownicy dydaktyczni oraz pracownicy administracji przetwarzający dane osobowe (załącznik nr 4).

1. Zgoda na przetwarzanie danych osobowych uczniów pracownikom dydaktycznym zostaje udzielona automatycznie po podpisaniu oświadczenia o zachowaniu tajemnicy.
2. Zakres przetwarzanych przez nauczycieli danych obejmuje: dane osobowe uczniów oraz ich rodziców bądź opiekunów prawnych potrzebne w celu właściwego realizowania zadań dydaktycznych oraz opiekuńczo-wychowawczych, w tym dane niezbędne do prowadzenia dokumentacji szkolnej oraz dla celów egzaminów.
3. Kopie upoważnień oraz oświadczeń, o których mowa w ust. 2 przechowuje się w aktach osobowych pracownika. Każde upoważnienie jest rejestrowane w Rejestrze upoważnień przechowywanym w sekretariacie dyrektora.
4. Upoważnienia, o których mowa w ust. 2a są imienne i udzielane w formie pisemnej na czas określony lub czas nieokreślony – do odwołania udzielonego upoważnienia.

**§ 7**

Pomieszczenia lub ich część, w których przetwarzane są dane osobowe, tworzą obszary przetwarzania danych osobowych w Szkole. Przebywanie osób nieuprawnionych w tych obszarach jest ograniczone i odbywać się może tylko w obecności użytkowników.

**Rozdział 3**

**PROCEDURY TWORZENIA I DOKONYWANIA ZMIAN W PRZETWARZANIU DANYCH OSOBOWYCH W ZBIORACH**

**§ 8**

1. Tworzy się zbiory danych osobowych przez nadanie danym osobowym odpowiedniej struktury, dostępnej według określonych kryteriów, niezależnie od tego czy zestaw danych jest rozproszony lub podzielony funkcjonalnie.
2. Przetwarzanie danych osobowych może odbywać się metodą:
   1. papierową, w której dane osobowe przetwarza się klasycznie w postaci dokumentów;
   2. informatyczną, w której dane osobowe przetwarza się w systemie informatycznym;
   3. dualną, w której dane osobowe przetwarza się klasycznie i jednocześnie w systemie informatycznym;
   4. zbiorów rozproszonych, w której dane osobowe przetwarzane są w kilku obszarach przetwarzania.
3. Osoby upoważnione do przetwarzania danych tworzą zbiory danych osobowych lub wnioskują o ich wycofanie, zgodnie z potrzebami realizacji zadań służbowych, za zgodą Administratora Danych.

**Rozdział 4**

**SZKOLENIE OSÓB Z ZAKRESU PRZETWARZANIA DANYCH OSOBOWYCH**

**§ 9**

1. Każda osoba przed rozpoczęciem przetwarzania danych osobowych ma obowiązek zapoznania się z przepisami dotyczącymi bezpieczeństwa przetwarzania i ochrony danych osobowych.
2. Przełożony zobowiązany jest umożliwić podwładnym zapoznanie się z przepisami, o których mowa w ust. 1.
3. W przypadku wprowadzania w Szkole nowych przepisów dotyczących wdrażania procedur przetwarzania i ochrony danych osobowych Administrator Danych może zorganizować dodatkowe szkolenia dla określonych grup użytkowników.

**Rozdział 5**

**DOKUMENTACJA Z ZAKRESU PRZETWARZANIA DANYCH OSOBOWYCH**

**§ 10**

Główne dokumenty przetwarzania i ochrony danych osobowych w Szkole:

1. **Instrukcja organizacji przetwarzania** danych osobowych w Szkole
2. **Polityka bezpieczeństwa przetwarzania danych osobowych** w Szkole (załącznik nr 1),
3. **Instrukcja zarządzania systemem informatycznym** służącym do przetwarzania danychosobowych w Szkole (załącznik nr 2),
4. **Ewidencja osób** upoważnionych do przetwarzaniu danych osobowych w Szkole (załącznik nr 3 ).

**Rozdział 6**

**OBOWIĄZKI OSÓB ODPOWIEDZIALNYCH ZA OCHRONĘ DANYCH OSOBOWYCH**

**§ 11**

Administratorem Danych Osobowych w Szkole jest Dyrektor Szkoły.

**Obowiązki Administratora Danych Osobowych:**

1. Organizacja, koordynowanie i nadzór zadań z zakresu przetwarzania i ochrony danych zgodnie z przepisami Ustawy.
2. Dobór środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednio do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem Ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.
3. Ochrona interesów osób, których dane dotyczą, a w szczególności zapewnienie, aby dane te były:
   1. przetwarzane zgodnie z prawem,
   2. zbierane dla oznaczonych, zgodnych z prawem celów i niepoddawane dalszemu przetwarzaniu niezgodnemu z tymi celami,
   3. merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane,
   4. przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.
4. Wydawanie upoważnień pracownikom do wykonywania zadań związanych z przetwarzaniem danych osobowych.
5. Prowadzenie dokumentacji opisującej sposób przetwarzania danych oraz środki, o których mowa w ust. 3.
6. Wyznaczenie Administratora Bezpieczeństwa Informacji, nadzorującego przestrzeganie zasad ochrony, o których mowa w ust. 3.

**§ 12**

**Do zadań Administratora Bezpieczeństwa Informatycznego należy:**

1. Określenie zasad ochrony danych osobowych.
2. Wnioskowanie o ukaranie osób winnych naruszenia przepisów i zasad dotyczących ochrony danych osobowych.
3. Nadzór nad wdrożeniem stosownych środków organizacyjnych, technicznych i fizycznych w celu ochrony przetwarzanych danych osobowych.
4. Nadawanie, zmienianie oraz cofanie uprawnień do przetwarzania danych osobowych.

**§ 13**

**Do zadań Administratorów Systemu Informatycznego należy:**

1. Administrowanie systemami, w których przetwarzane są dane osobowe;
2. Nadawanie użytkownikom identyfikatorów i przyznawanie im uprawnień w systemie, wynikających z nadanego upoważnienia;
3. Instalowanie, aktualizowanie i konfigurowanie oprogramowania systemowego i aplikacyjnego oraz urządzeń, o ile czynności te nie są wykonywane przez upoważnionych przedstawicieli dostawcy systemu, na podstawie zawartej umowy;
4. Instalowanie i aktualizowanie oprogramowania antywirusowego;
5. Reagowanie i rejestrowanie przypadków naruszenia bądź zagrożenia bezpieczeństwa danych osobowych przetwarzanych w systemie;
6. Prowadzenie szkolenia w zakresie zabezpieczenia danych w systemach;
7. Tworzenie, rejestrowanie oraz przechowywanie kopii zapasowych baz danych, zawierających dane osobowe;
8. Przygotowywanie urządzeń, dysków i innych elektronicznych nośników informacji, zawierających dane osobowe, do likwidacji, przekazania innemu podmiotowi, konserwacji lub naprawy;
9. Kompletowanie i przechowywanie dokumentacji dotyczącej systemu, w którym przetwarzane są dane osobowe;
10. Powiadamianie Administratora Danych o miejscu przechowywania oraz metodzie i częstotliwości tworzenia kopii zapasowych zbiorów danych osobowych przetwarzanych w systemach;
11. Wykonywanie bieżącej konserwacji i przeglądu systemu;
12. Uaktualnianie kont i uprawnień użytkowników.

**Rozdział 7**

**USTALENIA KOŃCOWE**

**§ 14**

1. sprawach nieuregulowanych niniejszą Instrukcją zastosowanie znajdują:
2. *Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. 2018, poz. 1000)*

**Rozdział 8**

**WYKAZ ZAŁĄCZNIKÓW**

**§ 15**

Instrukcja zawiera następujące załączniki:

|  |  |
| --- | --- |
| załącznik nr 1 | Polityka bezpieczeństwa przetwarzania danych osobowych |
| załącznik nr 2 | Instrukcja Zarządzania Systemem Informatycznym |
| załącznik nr 3 | Ewidencja osób upoważnionych do przetwarzania danych osobowych |
| załącznik nr 4 | Upoważnienie do przetwarzania danych osobowych uczniów lub/i pracowników Szkoły |
| załącznik nr 5 | Informacja dla rodziców/ prawnych opiekunów uczniów oraz ich oświadczenie |
| załącznik nr 6 | Informacja i oświadczenie pracowników szkoły |
| załącznik nr 7 | Wniosek o udzielenie upoważnienia dostępu do danych osobowych |
| załącznik nr 8 | Wniosek o udostępnienie danych ze zbioru danych osobowych |
| załącznik nr 9 | Zgoda na wykorzystanie wizerunku dziecka |
| załącznik nr 10 | Umowa powierzenia przetwarzania danych osobowych |
| załącznik nr 11 | Kontrola wewnętrzna ochrony danych osobowych w szkole |
| załącznik nr 12 | Raport z naruszenia bezpieczeństwa zasad ochrony danych osobowych |

***Załącznik nr 1***

**POLITYKA**

**BEZPIECZEŃSTWA**

**przetwarzania danych osobowych**

**w Zespole Szkół Ogólnokształcących**

**nr 5  
z oddziałami integracyjnymi i specjalnymi**

**w Sosnowcu**

**Rozdział 1**

**POSTANOWIENIA OGÓLNE**

* + - **1**

1. Polityka bezpieczeństwa w zakresie zarządzania systemem informatycznym służącym do przetwarzania danych osobowych określa reguły postępowania i praktyczne doświadczenia dotyczące zarządzania, ochrony i dystrybucji informacji podlegającej ochronie (danych osobowych) w Szkole.
2. Celem polityki bezpieczeństwa, jest wskazanie działań, jakie należy podejmować oraz ustanowienie zasad, jakie należy stosować, aby prawidłowo były realizowane obowiązki administratora danych osobowych w zakresie zabezpieczenia danych osobowych.
3. Polityka bezpieczeństwa w zakresie zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Szkole zawiera:
   1. identyfikację zasobów systemu informatycznego oraz programy zastosowane do przetwarzania tych danych,
   2. wykaz pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe,
   3. wykaz zbiorów danych osobowych,
   4. środki techniczne i organizacyjne służące zapewnieniu poufności, integralności i rozliczalności przetwarzanych danych.

**Rozdział 2**

**IDENTYFIKACJA ZASOBÓW SYSTEMU INFORMATYCZNEGO**

**ORAZ PROGRAMY ZASTOSOWANE DO PRZETWARZANIA TYCH DANYCH**

* + - * **2**

1. Struktura informatyczna Szkoły składa się z komputerów połączonych siecią zbudowaną w oparciu o łącza Miejskiego Centrum Zarządzania Siecią. Sieć Szkoły poprzez system firewall jest dołączona do sieci Internet.
2. W ramach tej infrastruktury funkcjonują systemy informatyczne:
   1. Dziennik elektroniczny VULCAN służący do rejestrowania i przetwarzania danych

związanych z procesem nauczania (oceny, frekwencja, informacje o uczniach i rodzicach oraz inne dane)

* 1. VULCAN:
     1. księgowość, faktury, rejestr VAT
     2. płace
     3. sekretariat
     4. arkusz organizacyjny
     5. plan lekcji
     6. zastępstwa
     7. egzamin gimnazjalny/ósmoklasisty

służący do rejestrowania i przetwarzania danych o uczniach i pracownikach pedagogicznych, wykorzystywany do tworzenia arkusza organizacyjnego szkoły, planów lekcji, dyżurów, wypisywania świadectw, prowadzenia ewidencji uczniów, przygotowania danych do egzaminu gimnazjalnego/ósmoklasisty,

* 1. VULCAN - służący do korespondencji z Wydziałem Edukacji i placówkami oświatowymi oraz do rejestrowania i przetwarzania danych do rekrutacji uczniów,
  2. e-PFRON on line - system obsługujący przesyłanie deklaracji i informacji do PFRON,
  3. SIO - program do obsługi systemu informacji oświatowej,
  4. PKO BP - system obsługujący przelewy bankowe.

1. Wymienione w ust. 2 systemy informatyczne zawierają dane podlegające ochronie ze względu na Ustawę oraz są strategicznie ważne dla ciągłości pracy Szkoły.
2. Do zbierania i wprowadzania danych do systemu wykorzystywane są stacjonarne i przenośne komputery.

**Rozdział 3**

**EWIDENCJA ZBIORÓW I BAZ DANYCH ORAZ WYKAZ POMIESZCZEŃ TWORZĄCYCH** **OBSZAR, W KTÓRYM PRZETWARZANE SĄ DANE OSOBOWE**

**§ 3**

1. Wykaz baz danych w wersji informatycznej

|  |  |  |
| --- | --- | --- |
| Lp. | Nazwa bazy | Zawartość poszczególnych pól informacyjnych |
|  | Ewidencja uczniów  i rodziców (opiekunów prawnych) | Imię, nazwisko, adres, imiona i nazwisko rodziców, nr tel. stacjonarnego lub komórkowego, e-mail, data urodzenia, rysopis (np. zdjęcie), nr PESEL |
|  | Kadry | Imię, nazwisko, adres, imiona i nazwisko rodziców, dane najbliższej rodziny, nr telefonu stacjonarnego lub komórkowego, data urodzenia, rysopis (np. zdjęcie), nr NIP, nr PESEL, seria i nr dowodu osobistego oraz stosunek do służby wojskowej, stanowisko i przydzielone zadania, dokumentacja kształcenia i zawodowa, nagrody, nr konta, stawka wynagrodzenia, |
|  | Arkusz organizacyjny szkoły | Imię, nazwisko, data urodzenia, nr PESEL, wykształcenie, stopień awansu zawodowego, staż pedagogiczny, pensum, dane płacowe, stanowisko i przydzielone zadania |
|  | Plan lekcji | Rozkład zajęć uczniów w poszczególnych klasach, rozkład zajęć nauczycieli, plan dyżurów Nauczycieli |
|  | Zastępstwa | Informacja o nieobecnościach i zastępstwach nauczycieli |
|  | Dziennik elektroniczny | Imię, nazwisko, adres, imiona i nazwisko rodziców, nr tel. stacjonarnego lub komórkowego, data urodzenia, nr PESEL informacje dotyczące ocen, frekwencji, plan lekcji, zastępstwa |
|  | Pomoc psychologiczno-pedagogiczna | Imię, nazwisko, adres, imiona i nazwisko rodziców , choroba/ dysfunkcja potwierdzona, orzeczeniem, zalecenia |
|  | Księgowość | Imię i nazwisko pracownika i członków rodziny zamieszkującej we wspólnym gospodarstwie domowym, data urodzenia, adres, telefon, nr NIP, nr PESEL, wykształcenie, płace , pożyczki, umowy, ewidencja zwolnień lekarskich |
|  | Ewidencja uczniów  przystępujących do egzaminu | Imię, nazwisko, adres, imiona i nazwisko rodziców, nr tel. stacjonarnego lub komórkowego, e-mail, data urodzenia, nr PESEL |
|  | Baza danych czytelników-  biblioteka | Imię, nazwisko, adres, nr tel. stacjonarnego lub komórkowego, e-mail |

2. Wykaz baz danych w wersji tradycyjnej:

|  |  |  |
| --- | --- | --- |
| Lp. | Nazwa bazy | Zawartość poszczególnych pól informacyjnych |
|  | Dzienniki lekcyjne | Imię, nazwisko, adres, imiona i nazwisko rodziców, telefon, e-mail, frekwencja, oceny |
|  | Dzienniki nauczania indywidualnego | Imię, nazwisko, adres, telefon, frekwencja, oceny |
|  | Dzienniki zajęć pozalekcyjnych | Imię, nazwisko, frekwencja |
|  | Dziennik świetlicy szkolnej | Imię, nazwisko, klasa, adres zamieszkania, imiona i nazwiska rodziców/ prawnych opiekunów, data urodzenia, numery kontaktowe rodziców/ prawnych opiekunów, numery konta bankowego. |
|  | Księgi uczniów | Imię, nazwisko, adres, imiona i nazwisko rodziców, data urodzenia, nr PESEL, |
|  | Księgi absolwentów | Imię, nazwisko, adres, imiona i nazwisko rodziców, data urodzenia, nr PESEL, okres nauczania, dalsze losy edukacyjne |
|  | Rejestr wydanych świadectw | Imię, nazwisko, nr PESEL, data odbioru |
|  | Arkusze ocen | Imię, nazwisko, adres, imiona i nazwisko rodziców, wyniki nauczania, protokoły z egzaminów klasyfikacyjnych, poprawkowych i innych sprawdzianów |
|  | Teczki akt osobowych | Imię, nazwisko, adres, imiona i nazwisko rodziców, dane najbliższej rodziny, nr tel. stacjonarnego lub komórkowego, data urodzenia, rysopis (np. zdjęcie), nr NIP, nr PESEL, seria i nr dowodu osobistego oraz stosunek do służby wojskowej, stanowisko i przydzielone zadania, dokumentacja kształcenia i zawodowa, nagrody, nr konta, stawka wynagrodzenia |
|  | Teczki awansu zawodowego | Imię, nazwisko, stanowisko, wykształcenie, ścieżka awansu, dokumentacja awansu |
|  | Teczki nadzoru pedagogicznego (obserwacji zajęć) | Imię, nazwisko, stanowisko, ocena i zalecenia |
|  | Dokumentacja pedagoga/ psychologa | Imię, nazwisko, adres, imiona i nazwisko rodziców, telefon, orzeczenia, opis spotkań i porad |
|  | Teczki wychowawcy klasy | Imię, nazwisko, adres, imiona i nazwisko rodziców, telefon, e-mail, dokumentacja dotycząca osiągnięć, wykroczeń i innych w związku z nauką w szkole, lista uczniów posiadających orzeczenie lub opinie PPP, lista uczniów objętych PPP, deklaracja uczęszczania na religię i WDŻ |
|  | Dokumentacja komisji dyscyplinarnych | Imię, nazwisko, imiona i nazwisko rodziców, opis wykroczenia, warunki kontraktu |
|  | Dokumentacje komisji socjalnej | Imię, nazwisko, przyznana kwota, rodzaj ukończonego doskonalenia, |
|  | Dokumentacja wycieczek /wyjść szkolnych | Imię, nazwisko, adres, imiona i nazwisko rodziców, telefon, e-mail |
|  | Karty zdrowia uczniów | Imię, nazwisko, adres, nr PESEL, imiona i nazwisko rodziców, karta zdrowia, bilans zdrowia |
|  | Ewidencja i dokumentacja zwolnień lekarskich | Imię, nazwisko, adres, nr PESEL, jednostka chorobowa |

**Rozdział 4**

**WYKAZ POMIESZCZEŃ TWORZĄCYCH OBSZAR, W KTÓRYM PRZETWARZANE SĄ**

**DANE OSOBOWE**

**§ 4**

Ze względu na szczególne nagromadzenie danych osobowych w Szkole specjalnie chronione są następujące pomieszczenia:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Lp.** | **Miejsce przechowywania /**  **Zabezpieczenie** | **Rodzaj danych** | **Sposób**  **przetwarzania** | **Osoba**  **odpowiedzialna** |
|  | Składnica akt (gabinet wicedyrektorów, archiwum), klucze dostępne tylko w sekretariacie | Arkusze ocen i księgi arkuszy ocen  Rejestry archiwum (m.in. akta osobowe pracowników, listy płac, kartoteki płacowe pracowników) | Tradycyjny | Sekretarz |
|  | Biblioteka (p. 12), klucze  dostępne tylko na portierni | Ewidencja osób korzystających z  księgozbioru bibliotecznego | Elektroniczny | Bibliotekarze |
|  | Gabinet dyrektora (p. 16) ,  klucze dostępne na portierni i u sekretarki | Dokumentacja związana z nadzorem  pedagogicznym | Tradycyjny | Dyrektor |
| Arkusze organizacyjne | Tradycyjny i elektroniczny | Dyrektor |
|  | Gabinet pedagoga/psychologa  (p. 29a), klucze dostępne tylko  na portierni | Dokumentacja pomocy psychologiczno-  pedagogicznej (opinie, orzeczenia)  Dokumentacja związana z pomocą socjalną  dla uczniów    Dzienniki pedagoga  i psychologa | Tradycyjny | Pedagog  i psycholog |
|  | Gabinet wicedyrektora, klucze dostępne tylko na portierni | Dokumentacja związana z organizacją i przebiegiem egzaminów klasyfikacyjnych,  poprawkowych i innych.  Rejestr zastępstw nauczycieli.  Dokumentacja związana z organizacją  procesu dydaktycznego.  Dokumentacja związana z nadzorem  Pedagogicznym.  Wyniki klasyfikacji.  Arkusz organizacyjny.  Plan lekcji.  Dokumentacja zespołów przedmiotowych i zadaniowych  Dokumentacja związana z organizacją  Rekrutacji.  Listy obecności nauczycieli na radach  Pedagogicznych.  Dokumentacja dotycząca udziału  nauczycieli w szkoleniach.  Dokumentacja dotycząca dyscypliny pracy  Nauczycieli.  Dokumentacja dotycząca sukcesów  uczniów i nauczycieli.  Dokumentacja dotycząca współpracy z uczelniami i instytucjami  Dokumentacja wycieczek/ wyjść szkolnych.  Dokumentacja dotycząca losów  Absolwentów.  Arkusze ocen  Dzienniki zajęć dodatkowych i nauczania  Indywidualnego.  Rejestr wydanych świadectw.  Wyniki klasyfikacji.  Dokumentacja związana z organizacją  egzaminu maturalnego.  Wyniki pomiarów dydaktycznych . (egzamin maturalny, diagnozy).  Dokumentacja związana z organizacją  procesu dydaktycznego  Dokumentacja związana z nadzorem  Pedagogicznym.  Rozliczenia za godziny dodatkowe Nauczycieli. | Tradycyjny i elektroniczny | Wicedyrektor |
|  | Gabinet pielęgniarki, s. 21 | Karty zdrowia uczniów  Rejestr wizyt i porad | Tradycyjny | Pielęgniarka |
|  | Sekretariat, klucze  dostępne tylko na portierni | Ewidencja zwolnień lekarskich  Dowody i dokumenty księgowe  Listy płac  Deklaracje ubezpieczeniowe pracowników  Deklaracje i kartoteki ZUS pracowników  Dokumenty związane z Zakładowym  Funduszem Świadczeń Socjalnych  Oświadczenia podatkowe pracowników | Tradycyjny i elektroniczny | Pracownik  sekretariatu |
|  | Pokój nauczycielski  (p. 13), klucze ma każdy  nauczyciel oraz są dostępne  na portierni | Rejestr zastępstw  Nauczycieli  Dokumenty dotyczące organizacji pracy  szkoły (rozkład zajęć nauczycieli i klas, skład zespołów przedmiotowych i  zadaniowych…)  Rejestr uczniów zwalnianych z zajęć | Tradycyjny | Wicedyrektor  Nauczyciele |
|  | Sekretariat  (p. 15), klucze dostępne  tylko na portierni | Ewidencja zwolnień lekarskich  Ewidencja wypadków  Dokumenty osób starających się o  zatrudnienie w Szkole  Kartoteki wynagrodzeń  Rejestr delegacji służbowych  Ewidencja legitymacji nauczycieli  Teczki akt osobowych  Pracowników  Księga uchwał  Protokoły rady pedagogicznej  Listy obecności pracowników  Rejestr nagród pracowników  Aktualne listy uczniów w klasach (na  wypadek ewakuacji)  Ewidencja osób  upoważnionych do  przetwarzania danych osobowych  Ewidencja uczniów  Dokumenty rekrutacyjne uczniów  Teczki akt osobowych uczniów  Ewidencja wydanych legitymacji szkolnych  Ewidencja uczniów przystępujących do  egzaminów  Ewidencja podań i decyzji o zwolnieniu  ucznia z wychowania fizycznego  Zbiory oświadczeń rodziców lub prawnych  opiekunów uczniów  Ewidencja wydanych świadectw ukończenia szkoły  Rejestr dokumentów składowanych akt  Księga nagan |  | Pracownik  sekretariatu |
|  | Świetlice szkolne | Dziennik zajęć,.  Rejestr obecności  Ewidencja podań o przyjęcie na świetlice.  Ewidencja wydawania posiłków  Rejestr dzieci objętych pomocą społeczną. | Tradycyjny i elektroniczny | Kierownik świetlicy |

**Rozdział 5**

**ŚRODKI TECHNICZNE I ORGANIZACYJNE SŁUŻĄCE ZAPEWNIENIU POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZETWARZANIA DANYCH**

* + - **5**

1. Administrator Danych jest obowiązany czuwać nad tym, aby dane osobowe były przetwarzane zgodnie z prawem, aby były one zbierane dla oznaczonych, zgodnych z prawem celów, merytorycznie poprawne i adekwatne w stosunku do celów w jakich są przetwarzane.
2. Odpowiedzialność za wykonywanie wynikających z ustawy obowiązków ponoszą użytkownicy.
3. Osobami uprawnionymi do gromadzenia i przetwarzania danych osobowych są:
   * dyrektor i wicedyrektorzy szkoły,
   * kierownik świetlicy
   * pracownik sekretariatu szkoły,
   * nauczyciele,
   * pedagog, psycholog,
   * bibliotekarz,
   * pielęgniarka szkolna,
   * pracownik administrujący siecią informatyczną w szkole,
   * inne osoby upoważnione przez dyrektora szkoły.
4. Administrator Danych prowadzi listę osób zatrudnionych przy gromadzeniu i przetwarzaniu danych osobowych, stanowiącą załącznik nr 4 do niniejszej Instrukcji.
5. Osoby wymienione w punkcie 3 zbierają i przetwarzają dane osobowe wyłącznie do realizacji celów wymienionych w Rozdz. 2 § 5 Instrukcji.
6. Osoby te są obowiązane zachować uzyskane informacje w tajemnicy, co potwierdzają własnoręcznym podpisem wraz ze złożeniem stosownego oświadczenia na odpowiednim formularzu (załącznik nr 4).
7. Oświadczenie to zostaje włączone do akt osobowych pracownika.
8. Szczegółowe procedury związane z zarządzaniem systemem informatycznym służącym do przetwarzania danych osobowych zawarte są w Instrukcji Zarządzania Systemem Informatycznym (załącznik nr 2).

**§ 6**

**Bezpieczeństwo fizyczne**

1. Gwarancją zapewnienia bezpieczeństwa systemu informatycznego w placówce oraz przetwarzanych i przechowywanych danych jest zapewnienie bezpieczeństwa fizycznego. Warunkiem zapewnienia bezpieczeństwa fizycznego systemu jest kontrola dostępu do wszystkich stacji roboczych. W związku z tym szczególną ochroną obejmuje się pomieszczenia, w których znajdują się komputery oraz te, w których przechowywane są składowane dane.
2. Wyżej wymienione pomieszczenia powinny być zamknięte, a dostęp do nich powinny mieć tylko upoważnione osoby.
3. Klucze od pomieszczeń, w których wykonywane jest przetwarzanie danych osobowych, znajdują się w dyspozycji osób zatrudnionych przy przetwarzaniu danych i nie są udostępniane osobom postronnym ani innym pracownikom, za wyjątkiem personelu sprzątającego i usuwającego zaistniałe w tych pomieszczeniach awarie.
4. Przebywanie w tych pomieszczeniach osób nieuprawnionych do zapoznania się z danymi osobowymi jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu tych danych.
5. Obowiązkiem osoby użytkującej komputer przenośny zawierający dane osobowe jest zachowanie szczególnej ostrożności podczas jego transportu, przechowywania i użytkowania poza pomieszczeniami tworzącymi obszar, w którym przetwarzane są dane osobowe.

**§ 7**

**Konserwacja i naprawy sprzętu i oprogramowania**

1. Wszelkie naprawy i konserwacje sprzętu i oprogramowania mogą odbywać się tylko w obecności osób uprawnionych.
2. Urządzenia informatyczne służące do przetwarzania danych osobowych można przekazać do naprawy dopiero po uzyskaniu zgody dyrektora.
   * **8**

**Szkolenia**

1. Każdy użytkownik powinien mieć świadomość zagrożeń wpływających na bezpieczeństwo systemu informatycznego, z którego korzysta.
2. Nowy pracownik powinien być zapoznany z ogólnymi zasadami i przepisami dotyczącymi bezpieczeństwa systemów teleinformatycznych, a szczególnie wynikających z ustawy o ochronie danych osobowych.
   * **9**

**Informacje końcowe**

Szczegółowe ustalenia i procedury dotyczące zarządzania oprogramowaniem, uwierzytelniania użytkowników, tworzenia kopii zapasowych oraz profilaktyki antywirusowej zawarte są w Instrukcji Zarządzania Systemem Informatycznym w Szkole (załącznik nr 2).

***Załącznik nr 2***

**Instrukcja**

**Zarządzania Systemem Informatycznym służącym**

**do przetwarzania**

**danych osobowych**

**w Zespole Szkół Ogólnokształcących**

**nr 5  
z oddziałami integracyjnymi**

**i specjalnymi**

**w Sosnowcu**

***Podstawa prawna:***

1. *Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. 2018, poz. 1000)*

**Rozdział 1**

**WIADOMOŚCI WSTĘPNE**

**§ 1**

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Zespole Szkół Ogólnokształcących nr 5 w Sosnowcu określa:

1. Zarządzanie oprogramowaniem.
2. Uwierzytelnianie użytkowników (przydział loginów i haseł dla użytkowników oraz częstotliwość ich zmiany i osoby odpowiedzialne za te czynności).
3. Sposób rejestrowania i wyrejestrowywania użytkowników oraz osoby odpowiedzialne za te czynności.
4. Procedury rozpoczynania i kończenia pracy.
5. Metodę i częstotliwość tworzenia kopii awaryjnych.
6. Metodę i częstotliwość sprawdzania obecności wirusów komputerowych oraz metodę ich usuwania.
7. Sposób i czas przechowywania nośników informacji, w tym kopii informatycznych i wydruków.
8. Sposób dokonywania przeglądów i konserwacji systemu oraz zbioru danych osobowych .
9. Sposób postępowania w zakresie komunikacji w sieci komputerowej.

**Rozdział 2**

**ZARZĄDZANIE OPROGRAMOWANIEM**

**§ 2**

1. Najwyższe uprawnienia w systemie informatycznym posiada administrator systemu. W Zespole Szkół Ogólnokształcących nr 5 głównym Administratorem Systemu jest Dyrektor Szkoły.

2. Tylko Administrator Systemu jest osobą uprawnioną do instalowania i usuwania oprogramowania systemowego i narzędziowego.

3. Dopuszcza się instalowanie tylko legalnie pozyskanych programów i posiadających ważną licencję użytkowania.

**Rozdział 3**

**NADAWANIE UPRAWNIEŃ DO PRZETWARZANIA DANYCH**

**ORAZ ICH REJESTROWANIE W SYSTEMIE INFORMATYCZNYM**

* + **3**

1. Do obsługi systemu informatycznego służącego do przetwarzania danych osobowych może być dopuszczona wyłącznie osoba (użytkownik) posiadająca upoważnienie do przetwarzania danych osobowych, wydane przez Administratora Danych i zarejestrowana w tym systemie.
2. Rejestracja, o której mowa w ust. l polega na nadaniu identyfikatora i przydziale hasła oraz wprowadzeniu tych danych do bazy użytkowników systemu.
3. Upoważnienia do przetwarzania danych osobowych, o których mowa w ust. 1 przechowywane są w teczkach akt osobowych pracowników oraz prowadzona jest ich ewidencja.

\

1. Dla każdego użytkownika systemu informatycznego, który przetwarza dane osobowe, Administrator Systemu ustala niepowtarzalny identyfikator i hasło początkowe.

**Rozdział 4**

**METODY I ŚRODKI UWIERZYTELNIENIA ORAZ PROCEDURY**

**ZWIĄZANE Z ICH ZARZĄDZANIEM I UŻYTKOWANIEM**

**§ 4**

**Nadawanie identyfikatorów i haseł użytkownikom**

1. Dane osobowe przetwarzane są z użyciem dedykowanych serwerów, komputerów stacjonarnych.
2. Hasło użytkownika powinno mieć minimum 8 znaków i być zmieniane

w przypadku:

* + Systemu Vulcan - co 30 dni,
  + komputerów w gabinetach - w miarę potrzeb.

1. Hasło oprócz znaków małych i dużych liter winno zawierać znaki alfanumeryczne i specjalne.
2. Hasło powinno być tak zbudowane, aby nie można było go kojarzyć z użytkownikiem komputera – przykładowo dane osobiste: nazwisko, inicjały, imiona, data urodzin własna, dziecka lub małżonka, imię domowego zwierzaka itp.
3. Hasło użytkownika, umożliwiające dostęp do systemu informatycznego, należy utrzymywać w tajemnicy, również po upływie jego ważności.
4. Hasło nie może znajdować się w miejscu widocznym oraz nie mogą mieć do niego dostępu osoby nieuprawnione. Użytkownikowi nie wolno udostępnić swojego loginu i hasła, jak również dopuszczać osoby nieuprawnione do stanowiska roboczego po uwierzytelnieniu w systemie.
5. Raz przypisany login nie może być przydzielony innemu użytkownikowi lub po przerwie w pracy (przerwa w zatrudnieniu) temu samemu pracownikowi.
6. W przypadku, gdy istnieje podejrzenie, że hasło mogła poznać osoba nieuprawniona, użytkownik zobowiązany jest do natychmiastowej zmiany hasła.
7. Nowo przyjęty pracownik po przydzieleniu loginu i „hasła jedno razowego” zobowiązany jest do jego zmiany przy pierwszym logowaniu się do systemu.
8. Hasła administratorów przechowywane są w bezpiecznym miejscu w szkole.
9. Zakazane jest korzystanie z identyfikatorów oraz haseł nie przydzielonych użytkownikowi.

**Wyrejestrowanie użytkownika**

* + **5**

1. Wyrejestrowania użytkownika z systemu informatycznego dokonuje Administrator Systemu na wniosek dyrektora placówki.
2. Przyczyną wyrejestrowania użytkownika z systemu informatycznego jest rozwiązanie lub wygaśnięcie stosunku pracy użytkownika.

**Rozdział 5**

**PROCEDURY ROZPOCZĘCIA, ZAWIESZENIA I ZAKOŃCZENIA PRACY**

**§ 6**

Dane osobowe, których administratorem jest Szkoła mogą być przetwarzane sposobem tradycyjnym lub z użyciem systemu informatycznego tylko na potrzeby realizowania zadań statutowych i organizacyjnych szkoły.

1. Rozpoczęcie pracy użytkownika w systemie odbywa się poprzez:
   * przygotowanie stanowiska pracy,
   * włączenie stacji roboczej,
   * wprowadzenie swojego identyfikatora i hasła.
     + **7**
2. Zakończenie pracy w systemie odbywa się poprzez:
   * zamknięcie aplikacji,
   * odłączenie się od zasobów systemowych,
   * zamknięcie systemu operacyjnego,
   * wyłączenie stacji roboczej.
3. Niedopuszczalne jest zakończenie pracy w systemie bez wykonania wylogowania się z aplikacji i zamknięcia systemu.
4. Użytkownik ma obowiązek wylogowania się w przypadku zakończenia pracy. Stanowisko komputerowe nie może pozostać z włączonym i dostępnym systemem bez nadzoru pracującego na nim pracownika.
   * + **8**

**Działania podejmowane w celu uniemożliwienia osobom nieuprawnionym dostęp do danych osobowych**

1. Monitory stanowisk komputerowych, na których przetwarzane są dane osobowe, w pobliżu których przebywają osoby nieuprawnione, należy ustawić w taki sposób, aby uniemożliwić osobom postronnym wgląd w monitor komputera.
2. Przebywanie osób nieuprawnionych w pomieszczeniach znajdujących się na obszarze, w którym są przetwarzane dane osobowe, jest dopuszczalne tylko w obecności osoby upoważnionej do ich przetwarzania.
3. Wydruki zawierające dane osobowe należy przechowywać w miejscu uniemożliwiającym do nich dostęp osobom postronnym.
4. Wydruki niepotrzebne należy zniszczyć w niszczarce dokumentów.
5. Pomieszczenia, w których przetwarzane są dane osobowe, na czas nieobecności osób zatrudnionych, należy zamykać, w sposób uniemożliwiający dostęp do nich osobom trzecim.
6. Zabrania się użytkownikom pracującym w systemie:
   * udostępniania stacji roboczej osobom niezarejestrowanym w systemie,
   * udostępniania stacji roboczej do konserwacji lub naprawy bez porozumienia z Administratorem Bezpieczeństwa,
   * używania nielicencjonowanego oprogramowania.

**§ 9**

**Formy naruszenia ochrony danych osobowych przez osoby zatrudnione przy przetwarzaniu** **danych** **oraz sposoby postępowania**

|  |  |
| --- | --- |
| **FORMY NARUSZEŃ** | **SPOSOBY POSTĘPOWANIA** |
| **W ZAKRESIE WIEDZY** | |
| Ujawnienie sposobu działania aplikacji i systemu oraz  zabezpieczeń osobom nieupoważnionym. | 1. Przerwać czynność prowadzącą do ujawnienia informacji. 2. Sporządzić raport z opisem, jaka informacja została ujawniona. 3. Powiadomić Administratora Bezpieczeństwa Informacji. |
| Ujawnienie danych dotyczących infrastruktury informatycznej. |
| Dopuszczanie do sytuacji lub stwarzanie warunków,  w których osoba nieupoważniona pozyskuje wyżej wymienione  informacje. |
| **W ZAKRESIE SPRZĘTU I OPROGRAMOWANIA** | |
| Opuszczenie stanowiska pracy z aktywną aplikacją  umożliwiającą dostęp do bazy danych osobowych. | 1. Zakończyć działanie aplikacji. 2. Sporządzić raport. |
| Dopuszczenie innej osoby do korzystania z aplikacji  umożliwiającej dostęp do bazy danych osobowych. | 1. Wezwać osobę bezprawnie korzystającą z aplikacji do 2. opuszczenia stanowiska przy komputerze. 3. Sporządzić raport. |
| Pozostawienie w niezabezpieczonym i widocznym miejscu hasła dostępu do bazy danych osobowych lub sieci. | 1. Zabezpieczyć informację z hasłami w sposób uniemożliwiający 2. odczytanie. 3. Powiadomić Administratora Bezpieczeństwa Informacji. 4. Sporządzić raport. |
| Dopuszczenie do użytkowania sprzętu komputerowego i oprogramowania z dostępem do bazy danych osobowych osobom nieupoważnionym. | 1. Wezwać osobę nieupoważnioną do opuszczenia stanowiska. 2. Ustalić czynności, których dokonały osoby nieupoważnione. 3. Przerwać działanie programów. 4. Powiadomić Administratora Bezpieczeństwa Informacji. 5. Sporządzić raport |
| Samodzielne instalowanie oprogramowania oraz ściąganie oprogramowania z Internetu na stacje robocze oraz na serwer. | 1. Pouczyć osobę, która zainstalowała oprogramowanie o 2. bezprawności jej działania. 3. Wezwać służby informatyczne. 4. Sporządzić raport. |
| Modyfikowanie parametrów systemu i aplikacji. | 1. Wezwać osobę modyfikującą, aby tego zaniechała. 2. Sporządzić raport. |
| Odczytywanie nośników informacji przed sprawdzeniem ich  działania poprzez program antywirusowy. | 1. Pouczyć osobę o szkodliwości takiego działania. 2. Wezwać służby informatyczne. 3. Sporządzić raport. |
| **W ZAKRESIE DOKUMENTÓW I OBRAZÓW, KTÓRE ZAWIERAJĄ DANE OSOBOWE** | |
| Pozostawienie dokumentów w otwartych pomieszczeniach bez nadzoru. | 1. Zabezpieczyć dokumenty. 2. Sporządzić raport. |
| Przechowywanie dokumentów niezabezpieczonych przed  osobami nieupoważnionymi. | 1. Powiadomić Administratora Bezpieczeństwa Informacji. 2. Poprawić zabezpieczenia. 3. Sporządzić raport. |
| Wyrzucanie dokumentów niewłaściwie zniszczonych, co  umożliwia ich odczytanie. | 1. Zabezpieczyć dokumenty. 2. Powiadomić przełożonych. 3. Sporządzić raport. |
| Dopuszczanie do kopiowania dokumentów bez kontroli nad ich kopią. | 1. Zaprzestać kopiowania. 2. Odzyskać kopię. 3. Powiadomić Administratora Bezpieczeństwa Informacji. 4. Sporządzić raport. |
| **W ZAKRESIE POMIESZCZEŃ I INFRASTRUKTURY SŁUŻĄCYCH**  **DO PRZETWARZANIA DANYCH OSOBOWYCH** | |
| Opuszczanie i pozostawianie bez nadzoru niezamkniętego  pomieszczenia z dostępem do danych osobowych. | Zabezpieczyć pomieszczenie.  Powiadomić Administratora Bezpieczeństwa Informacji.  Sporządzić raport. |
| Dopuszczanie do kontaktu ze sprzętem komputerowym osobom  nieznanym. | Wezwać osoby opuszczenia pomieszczeń.  Ustalić tożsamość osób.  Powiadomić Administratora Bezpieczeństwa Informacji.  Sporządzić raport. |
| Dopuszczanie do podłączania urządzeń do sieci komputerowej,  demontażu gniazd i torów kablowych przez osoby nienależne do  służb informatycznych i telekomunikacyjnych. | Wezwać osoby do zaprzestania bezprawnych działań.  Ustalić tożsamość osób.  Powiadomić służby informatyczne i Administratora  Bezpieczeństwa Informacji.  Sporządzić raport. |
| **W ZAKRESIE POMIESZCZEŃ, W KTÓRYCH ZNAJDUJĄ SIĘ KOMPUTERY CENTRALNE**  **I URZĄDZENIA SIECI** | |
| Dopuszczanie do podłączania urządzeń do sieci komputerowej,  demontażu gniazd i torów kablowych przez osoby nienależne do  służb informatycznych i telekomunikacyjnych. | Wezwać osoby do zaprzestania bezprawnych działań.  Ustalić tożsamość osób.  Powiadomić służby informatyczne i Administratora  Bezpieczeństwa Informacji.  Sporządzić raport. |
| Dopuszczanie osób spoza służb informatycznych i  telekomunikacyjnych do przebywania w pomieszczeniach  komputerów centralnych lub węzłów sieci komputerowej. | Wezwać osoby do zaprzestania bezprawnych działań.  Ustalić tożsamość osób.  Wezwać do opuszczenia chronionych pomieszczeń.  Powiadomić służby informatyczne i Administratora  Bezpieczeństwa Informacji.  Sporządzić raport. |

**§ 10**

**Procedury w przypadku naruszenia ochrony danych osobowych**

1. Każdy przypadek naruszenia ochrony danych osobowych, a w szczególności:
   * naruszenia bezpieczeństwa systemu informatycznego,
   * stwierdzenia objawów (stanu urządzeń, sposobu działania programu lub jakości komunikacji w sieci), które mogą wskazywać na naruszenie bezpieczeństwa podlega zgłoszeniu Administratorowi Bezpieczeństwa.
2. Administratorowi Bezpieczeństwa zgłasza się w szczególności przypadki:
   * użytkowania stacji roboczej przez osobę nie będącą użytkownikiem systemu,
   * usiłowania logowania się do systemu (sieci) przez osobę nieuprawnioną,
   * usuwania, dodawania lub modyfikowania bez wiedzy i zgody użytkownika jego dokumentów,
   * przebywania osób nieuprawnionych w obszarze, w którym przetwarzane są dane osobowe, w trakcie nieobecności osoby zatrudnionej przy przetwarzaniu tych danych i bez zgody Administratora Danych, pozostawiania bez nadzoru otwartych pomieszczeń, w których przetwarzane są dane osobowe,
   * udostępniania osobom nieuprawnionym stacji roboczej lub komputera przenośnego, służących do przetwarzania danych osobowych,
   * niezabezpieczenia hasłem dostępu do komputera służącego do przetwarzania danych osobowych,
   * przechowywania kopii awaryjnych w tych samych pomieszczeniach, w których przechowywane są zbiory danych osobowych eksploatowane na bieżąco,
   * przechowywania nośników informacji oraz wydruków z danymi osobowymi, nieprzeznaczonymi do udostępniania, w warunkach umożliwiających do nich dostęp osobom nieuprawnionym.
3. Obowiązek dokonania zgłoszenia spoczywa na każdym pracowniku, który powziął wiadomość o naruszeniu ochrony danych osobowych.
4. W przypadku naruszenia integralności bezpieczeństwa sieciowego, obowiązkiem Administratora Bezpieczeństwa jest natychmiastowe wstrzymanie udostępniania zasobów dla użytkowników i odłączenie serwera od sieci.
5. Przywrócenie udostępniania zasobów użytkownikom może nastąpić dopiero po ustaleniu i usunięciu przyczyny naruszenia integralności bezpieczeństwa sieciowego.

**Rozdział 6**

**PROCEDURY TWORZENIA KOPII ZAPASOWYCH ZBIORÓW DANYCH** **ORAZ PROGRAMÓW I NARZĘDZI SŁUŻĄCYCH DO ICH PRZETWARZANIA**

* + - **11**

1. Zbiory danych w systemie informatycznym są zabezpieczane przed utratą lub uszkodzeniem za pomocą:
   * urządzeń zabezpieczających przed awarią zasilania lub zakłóceniami w sieci zasilającej,
   * sporządzania kopii zapasowych zbiorów danych (kopie pełne ).
2. Za tworzenie kopii bezpieczeństwa systemu informatycznego odpowiedzialny jest Administrator Bezpieczeństwa Informacji.
3. Kopie awaryjne tworzy się z następującą częstotliwością:
   * kopie systemu kadrowo-płacowego i finansowo-księgowego - codziennie,
   * kopie pozostałe - nie rzadziej niż raz na miesiąc.
4. Każdą kopię tworzy się na oddzielnym nośniku informatycznym.
5. W przypadku aktualizacji lub dokonywania zmian w systemie należy obowiązkowo wykonać kopię zapasową systemu.
6. W przypadku awarii systemu kopie zapasowe zbiorów danych należy okresowo sprawdzać pod kątem ich przydatności do odtworzenia. Za przeprowadzanie tej procedury odpowiedzialny jest Administrator Systemu.
7. Zabrania się przechowywania kopii awaryjnych w pomieszczeniach przeznaczonych do przechowywania zbiorów danych pozostających w bieżącym użytkowaniu.
8. Administrator Systemu przegląda okresowo kopie awaryjne i ocenia ich przydatność   
   do odtworzenia zasobów systemu w przypadku jego awarii .
9. Nośniki danych po ustaniu ich użyteczności należy pozbawić danych lub zniszczyć w sposób uniemożliwiający odczyt danych.

**Rozdział 7**

**SPOSÓB, MIEJSCE I OKRES PRZECHOWYWANIA ELEKTRONICZNYCH NOŚNIKÓW INFORMACJI ZAWIERAJĄCYCH DANE OSOBOWE**

**ORAZ KOPII ZAPASOWYCH**

* + **12**

1. Okresowe kopie zapasowe wykonywane są na zewnętrznych elektronicznych nośnikach informacji. Kopie zapasowe przechowuje się w kasie pancernej w pomieszczeniu ustalonym przez dyrektora szkoły, w sposób uniemożliwiający nieuprawnione przejęcie, modyfikacje, uszkodzenie lub zniszczenie.
2. Dostęp do nośników z kopiami zapasowymi systemu oraz kopiami danych osobowych ma wyłącznie Administrator Bezpieczeństwa.
3. Kopie miesięczne przechowuje się przez okres 6 miesięcy. Wykonywane co 2 miesiące kopie systemu kadrowego przechowuje się przez 50 lat. Kopie zapasowe należy bezzwłocznie usuwać po ustaniu ich użyteczności.
4. Usunięcie danych z systemu powinno zostać zrealizowane przy pomocy oprogramowania przeznaczonego do bezpiecznego usuwania danych z nośnika informacji.
5. W przypadku kopii zapasowych sporządzanych indywidualnie przez użytkownika –   
   –odpowiedzialny za ich zniszczenie jest użytkownik.
6. Przez zniszczenie nośników informacji rozumie się ich trwałe i nieodwracalne zniszczenie do stanu niedającego możliwości ich rekonstrukcji i odzyskania danych.

**Rozdział 8**

**SPOSÓB ZABEZPIECZENIA SYSTEMU INFORMATYCZNEGO PRZED** **OPROGRAMOWANIA, KTÓREGO CELEM JEST UZYSKANIE NIEUPRAWNIONEGO** **DOSTĘPU DO SYSTEMU INFORMATYCZNEGO**

* + **13**

1. W związku z istnieniem zagrożenia dla zbiorów danych osobowych ze strony złośliwego oprogramowania, którego celem jest m.in. uzyskanie nieuprawnionego dostępu do systemu informatycznego, konieczna jest ochrona sieci komputerowej i stanowisk komputerowych.
2. Wirusy komputerowe mogą rozpowszechniać się w systemach Szkoły poprzez Internet oraz zewnętrzne elektroniczne nośniki informacji.
3. Do obowiązków Administratora Systemu należy aktualizacja oprogramowania służącego **DZIAŁANIEM** do sprawdzania w systemie obecności wirusów komputerowych.
4. Przeciwdziałanie zagrożeniom ze strony złośliwego oprogramowania realizowane jest następująco:
   * Komputery i systemy są wyposażone w oprogramowanie antywirusowe oraz posiadają oprogramowanie i mechanizmy zabezpieczające przed nieautoryzowanym dostępem z sieci (firewall).
   * Bezpieczeństwo na styku z siecią Internet zapewniają systemy firewall. Zabrania się dokonywania połączeń modemowych z sieci lokalnej do sieci Internet z pominięciem oprogramowania firewall.
   * Jeżeli komputer przenośny podczas pracy w terenie został podłączony do sieci Internet, to przed podłączeniem do sieci lokalnej cały jego dysk twardy musi być sprawdzony zaktualizowanym programem antywirusowym.
   * Zainstalowany program antywirusowy powinien być tak skonfigurowany, by co najmniej raz dziennie dokonywał aktualizacji bazy wirusów oraz co najmniej raz w tygodniu dokonywane było automatycznie sprawdzenie komputera pod kątem obecności wirusów komputerowych.
   * Dane zawarte na nośnikach zewnętrznych (np. płyta CD, pendrive…) muszą być sprawdzone przez program antywirusowy przed wprowadzeniem do systemu. W przypadku jakichkolwiek wątpliwości odnośnie zagrożenia wirusowego należy sprawdzić zawartość całego dysku twardego programem antywirusowym. W przypadku dalszych niejasności należy kontaktować się z Administratorem Systemu.
5. Zabrania się użytkownikom komputerów wyłączania, blokowania czy odinstalowania programów zabezpieczających komputer (skaner antywirusowy, firewall) przed oprogramowaniem złośliwym oraz nieautoryzowanym dostępem.
6. W przypadku, gdy użytkownik stanowiska komputerowego zauważy komunikat oprogramowania zabezpieczającego wskazujący na zaistnienie zagrożenia lub rozpoznanie tego typu zagrożenia, zobowiązany jest zaprzestać jakichkolwiek czynności w systemie i niezwłocznie skontaktować się z Administratorem Systemu.
7. Przy korzystaniu z poczty elektronicznej użytkownicy są zobowiązani do zachowania szczególnej ostrożności, zwłaszcza w przypadku załączników. Zabrania się otwierania załączników i wiadomości poczty elektronicznej od nieznanych nadawców.
8. Zabrania się wszelkich prac z wykorzystaniem oprogramowania, na które użytkownik nie ma ważnej licencji (zakaz nie dotyczy programów, na użytkowanie których licencja nie jest wymagana) lub niewiadomego pochodzenia.
9. Przy wprowadzaniu do systemu nowych programów lub danych zawsze należy kierować się zasadą ograniczonego zaufania.

**Rozdział 9**

**CIĄGŁO ŚĆ PRACY URZĄDZEŃ INFORMATYCZNYCH**

* + **14**

1. System i urządzenia informatyczne służące do przetwarzania danych osobowych, zasilane energią elektryczną, zabezpiecza się przed utratą danych osobowych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.
2. Minimalne zabezpieczenie systemu i urządzeń informatycznych, o których mowa w ust. 1, polega na wyposażeniu serwera oraz stacji roboczych w zasilacze awaryjne (UPS).

**Rozdział 10**

**UDOSTĘPNIANIE DANYCH OSOBOWYCH I SPOSÓB ODNOTOWANIA INFORMACJI** **O** **UDOSTĘPNIONYCH DANYCH**

* + - **15**

1. Udostępnienie danych instytucjom może odbywać się wyłącznie zgodnie z przepisami prawa (OKE, CKE, Urząd Gminy i inne).
2. Osoba, której dane osobowe są przetwarzane ma prawo do wglądu tylko do swoich danych.
3. Przy każdym udostępnianiu danych osobowych osobie nieupoważnionej (wnioski załącznik nr 7 i 8), w rejestrze odnotowywane jest komu dane zostały udostępnione, data udostępnienia oraz zakres (rejestr w sekretariacie dyrektora).

**Rozdział 11**

**WYKONYWANIE PRZEGLĄDÓW I KONSERWACJI SYSTEMU ORAZ NOŚNIKÓW INFORMACJI SŁU ŻĄCYCH DO PRZETWARZANIA DANYCH**

* + - **16**

1. Przeglądy i konserwacje systemu oraz zbiorów danych wykonu je na bieżąco Administrator Bezpieczeństwa Informacji.
2. Administrator Bezpieczeństwa Informacji okresowo sprawdza możliwość odtworzenia danych z kopii zapasowej.
3. Umowy dotyczące instalacji i konserwacji sprzętu zawierane są z podmiotami, które gwarantują wykonanie prawidłowo usług.
4. Naprawy sprzętu zlecane są podmiotom, które gwarantują wykonanie prawidłowo usług. Naprawa sprzętu, na którym mogą znajdować się dane osobowe, odbywa się pod nadzorem Administratora Bezpieczeństwa Informacji w miejscu jego użytkowania.
5. W przypadku konieczności naprawy w serwisie, sprzęt komputerowy przed oddaniem do serwisu powinien być odpowiednio przygotowany. Dane należy zarchiwizować na nośniki informacji, a dyski twarde bezwzględnie wymontować na czas naprawy lub trwale usunąć z nich dane.
6. Zmiana konfiguracji sprzętu komputerowego, na którym znajduj ą się dane osobowe lub zmiana jego lokalizacji może być dokonana tylko za wiedzą i zgodą Administratora Bezpieczeństwa Informacji.
7. Urządzenia informatyczne służące do przetwarzania danych osobowych można przekazać:
   * do naprawy,
   * do użytkowania podmiotowi nieuprawnionemu do otrzymania tych danych,
   * do likwidacji

dopiero po uprzednim uzyskaniu zgody dyrektora.

1. Urządzenia, o których mowa w ust. 7, przed ich przekazaniem pozbawia się zapisu danych osobowych.
2. Jeżeli nie jest możliwe pozbawienie urządzenia przekazywanego do likwidacji zapisu danych osobowych, urządzenie - przed przekazaniem - uszkadza się w sposób uniemożliwiający odczytanie tych danych.

**Rozdział 12**

**ZASADY BEZPIECZEŃSTWA UŻYTKOWNIKA SYSTEMU INFORMATYCZNEGO**

**§ 17**

**Osobom korzystającym z systemu informatycznego, w którym przetwarzane są dane osobowe w Szkole zabrania się**:

1. Ujawniania loginu i hasła współpracownikom i osobom z zewnątrz.
2. Pozostawiania haseł w miejscach widocznych dla innych osób.
3. Udostępniania stanowisk pracy wraz z danymi osobowymi osobom nieuprawnionym.
4. Udostępniania osobom nieuprawnionym programów komputerowych zainstalowanych w systemie.
5. Używania oprogramowania w innym zakresie niż pozwala na to umowa licencyjna.
6. Przenoszenia programów komputerowych, dysków twardych z jednego stanowiska na inne.
7. Kopiowania danych na nośniki informacji, kopiowania na inne systemy celem wynoszenia ich poza szkołę.
8. Samowolnego instalowania i używania jakichkolwiek programów komputerowych, w tym równie ż programów do użytku prywatnego.
9. Używania nośników danych udostępnionych przez osoby postronne.
10. Przesyłania dokumentów i danych z wykorzystaniem konta pocztowego prywatnego.
11. Otwierania załączników i wiadomości poczty elektronicznej od nieznanych nadawców.
12. Używania nośników danych prywatnych, niesprawdzonych, niewiadomego pochodzenia. W sytuacji, gdyby zaistniała konieczność użycia niesprawdzonych przenośnych nośników danych, należy przeskanować je programem antywirusowymi, a w razie jakiś ostrzeżeń wyświetlonych przez program antywirusowy, zgłosić to Administratorowi Bezpieczeństwa Informacji.
13. Pozostawiania sprzętu komputerowego niezabezpieczonego przed dostępem osób nieuprawnionych, bez nadzoru osoby odpowiedzialnej za jego użytkowanie. Zalecane jest stosowanie wygaszaczy ekran
    * **18**

**Użytkownik zobowiązany jest do:**

1. Posługiwania się własnym loginem i hasłem w celu uzyskania dostępu do systemów informatycznych.
2. Tworzenia haseł trudnych do odgadnięcia dla innych.
3. Używania konta służbowego tylko w celach służbowych.
4. Nieprzerywania procesu skanowania przez program antywirusowy na komputerze.
5. Wykonywania kopii zapasowych danych przetwarzanych na stanowisku komputerowym.

Zabezpieczenia sprzętu komputerowego przenośnego (laptopy) przed kradzieżą lub nieuprawnionym dostępem do danych.

**Rozdział 13**

**ZALECENIA W ZAKRESIE PRZETWARZANIA**

**DANYCH OSOBOWYCH**

**SPOSOBEM TRADYCYJNYM**

* + - **19**

1. Miejscem tworzenia, uzupełniania i przechowywania dokumentacji dotyczącej przetwarzania danych osobowych sposobem tradycyjnym są pomieszczenia w szkole: sekretariat, pokój nauczycielski, gabinet dyrektora, gabinety wicedyrektorów, gabinet pedagoga/psychologa, biblioteka, świetlica, gabinet pielęgniarki, sale lekcyjne.
2. Osoby prowadzące dokumentację zobowiązane są do zachowania tajemnicy służbowej.
3. Dokumentacji, o której mowa w punkcie 1 nie można wynosić poza teren szkoły.
4. Dokumentację, o której mowa w punkcie 1 archiwizuje się zgodnie z Instrukcją kancelaryjną.
5. Osoby prowadzące dokumentację zobowiązane są do niezwłocznego poinformowania Pełnomocnika dyrektora ds. przetwarzania danych osobowych o podejrzeniu dostępu do dokumentacji przez osoby nieupoważnione.
6. Osobom prowadzącym dokumentację zabrania się:

* Wyrzucać dokumentów zawierających dane osobowe (dokumenty zawierające dane osobowe mogą być niszczone tylko w niszczarce).
* Pozostawiać dokumentów, kopii dokumentów zawierających dane osobowe w drukarkach czy kserokopiarkach.
* Pozostawiać kluczy w drzwiach, szafach, biurkach, pozostawiać otwartych pomieszczeń, w których przetwarza się dane osobowe.
* Pozostawiać bez nadzoru osoby trzecie przebywające w pomieszczeniach szkoły,   
  w których przetwarzane są dane osobowe.
* Pozostawiać dokumentów na biurku po zakończonej pracy, pozostawiać otwartych dokumentów na ekranie monitora bez blokady konsoli.
* Ignorować obecność nieznanych osób z zewnątrz, które poruszają się w obszarze przetwarzania danych osobowych.
* Przekazywać informacji zawierających dane osobowe osobom nieupoważnionym.
  + - **20**

1. Wszelkie przypadki naruszenia niniejszej Instrukcji należy zgłaszać Administratorowi Bezpieczeństwa lub bezpośredniemu przełożonemu.

Załącznik nr 3

**EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH**

…………………………………….

*(pieczęć szkoły)*

Na podstawie ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. 2018, poz. 1000) ustala się następującą listę osób zatrudnionych w Zespole Szkół Ogólnokształcących nr 5 z oddziałami integracyjnymi i specjalnymi w Sosnowcu upoważnionych do gromadzenia i przetwarzania danych osobowych związanych z działalnością szkoły:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  | Identyfikator | Zakres |  |
|  |  |  | Data nadania | Data ustania | upoważnienia |  |
| Lp. | Nazwisko i imię | Stanowisko | w systemie |  |
| upoważnienia | upoważnienia | (zawartość |  |
|  |  |  | informatycznym |  |
|  |  |  |  |  | zbioru danych) |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
| 1. |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
| 2. |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
| 3. |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
| 4. |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
| 5. |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
| 6. |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
| 7. |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
| 8. |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
| 9. |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
| 10. |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

......................................................................

*(podpis i pieczęć dyrektora)*

***Załącznik nr 4***

**UPOWAŻNIENIE**

.....................................................................

Sosnowiec, dn.……………

……..

*(pieczęć szkoły)*

**Upoważnienie nr**

……….

Na podstawie ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. 2018, poz. 1000) z dniem .......................................... upoważniam:

..........................................................................................................................................................

*(imię i nazwisko)*

zatrudnionego/ą na stanowisku .......................................................................................

w ZSO nr 5 w Sosnowcu, do dostępu, gromadzenia i przetwarzania danych osobowych, w formie papierowej i elektronicznej :

1. uczniów szkoły, jak też ich rodziców lub opiekunów prawnych\*,
2. pracowników szkoły, jak też ich rodzin\*,

które to dane są gromadzone w zakresie niezbędnym do prawidłowego funkcjonowania szkoły.

Równocześnie zobowiązuję Pana/ią do zachowania w tajemnicy wszelkich informacji dotyczących przetwarzanych danych osobowych oraz sposobów ich zabezpieczania.

Informuję, że udostępnianie danych osobowych lub umożliwienie dostępu do nich osobie nieupoważnionej podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 3   
(art. 107 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. 2018, poz. 1000)

Upoważnienie ważne jest do .............................

......................................................................

*(podpis i pieczęć dyrektora)*

\*niepotrzebne skreślić

Oświadczam, że zapoznałem/am się z przepisami ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. 2018, poz. 1000) oraz z treścią Instrukcji ochrony danych osobowych obowiązującą w ZSO nr 5 w Sosnowcu, szczególnie w zakresie dotyczącym zasad gromadzenia i przetwarzania danych osobowych. Zobowiązuję się do ich przestrzegania oraz zachowania w tajemnicy wszystkich danych osobowych, do których miałem/am dostęp w związku z zatrudnieniem oraz po ustaniu zatrudnienia w szkole.

……………………...................................................

*(data i podpis upoważnionego)*

***Załącznik nr 5***

**INFORMACJA DLA RODZICÓW/ PRAWNYCH OPIEKUNÓW UCZNIÓW**

.....................................................................

Sosnowiec, dn. ……

…………

*(pieczęć szkoły)*

Pan/Pani ............................................

...........................................................

...........................................................

Na podstawie ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. 2018, poz. 1000) informuję Pana/Panią, że dyrektor ZSO nr 5 w Sosnowcu jest administratorem danych osobowych uczniów szkoły.

Administrator danych osobowych zbiera i przetwarza dane osobowe Pana/Pani dziecka

i członków jego rodziny pozostających we wspólnym gospodarstwie domowym w zakresie dydaktyczno--wychowawczej i opiekuńczej działalności szkoły.

Informuję, że przysługuje Panu/Pani prawo do wglądu do zebranych danych oraz uzupełnienie, uaktualnienie lub sprostowanie w razie stwierdzenia, że dane są niekompletne, nieaktualne lub nieprawdziwe.

Jednocześnie zapewniam, że dyrektor ZSO nr 5 w Sosnowcu jako administrator danych dołoży wszelkich starań, aby dane były zbierane, przetwarzane i chronione zgodnie z prawem.

......................................................................

*(podpis i pieczęć dyrektora)*

Oświadczenie woli

Zapoznałem/am się z informacją dotyczącą zbierania i przetwarzania danych osobowych moich i członków mojej rodziny pozostającej we wspólnym gospodarstwie domowym.

Oświadczam, że wyrażam zgodę na zbieranie i przetwarzanie danych osobowych mojego dziecka/moich dzieci uczęszczających do ZSO nr 5 w Sosnowcu, a także moich i członków mojej rodziny pozostających we wspólnym gospodarstwie domowym, w zakresie dydaktyczno-opiekuńczo-wychowawczej działalności szkoły.

……………… ……………… .............................................

*(data i podpis rodzica/opiekuna)*

***Załącznik nr 6***

**INFORMACJA I OŚWIADCZENIE PRACOWNIKÓW** **SZKOŁY**

..................................................................... Sosnowiec, dn…………… ……..

*(pieczęć szkoły)*

Pan/Pani ..........................................................................

zatrudniony/ -a w ZSO nr 5 w Sosnowcu

na stanowisku ...........................................................

Na podstawie ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. 2018, poz. 1000) informuję Pana/Panią, że dyrektor Szkoły ZSO nr 5 w Sosnowcu (dalej: szkoła) jest administratorem danych osobowych pracowników szkoły.

Administrator danych osobowych zbiera i przetwarza dane osobowe Pana/Pani i członków rodziny pozostających we wspólnym gospodarstwie domowym (dalej: dane) zgodnie z zakresem Pana/Pani praw i obowiązków wynikających z pracy w szkole.

Informuję, że przysługuje Panu/Pani prawo do wglądu do zebranych danych oraz uzupełnianie, uaktualnianie lub sprostowanie w razie stwierdzenia, że dane są niekompletne, nieaktualne lub nieprawdziwe.

Jednocześnie zapewniam, że dyrektor ZSO nr 5 w Sosnowcu jako administrator danych dołoży wszelkich starań, aby dane były zbierane, przetwarzane i chronione zgodnie z prawem.

......................................................................

*(podpis i pieczęć dyrektora)*

Oświadczenie woli

Zapoznałem/-am się z informacją dotyczącą zbierania i przetwarzania danych osobowych moich   
i członków mojej rodziny pozostającej we wspólnym gospodarstwie domowym.

Oświadczam, że wyrażam zgodę na zbieranie i przetwarzanie danych osobowych moich   
i członków mojej rodziny pozostających we wspólnym gospodarstwie domowym zgodnie z zakresem moich praw i obowiązków wynikających z pracy w szkole.

Jednocześnie oświadczam, że podałem/-am dane osobowe moje i członków mojej rodziny pozostających we wspólnym gospodarstwie domowym dobrowolnie.

……………………………… .............................................

*(data i podpis pracownika)*

***Załącznik nr 7***

**Wniosek o udzielenie upoważnienia dostępu do danych osobowych**

.....................................................................

Sosnowiec, dn……

*(pieczęć szkoły)*

**Wniosek**

Proszę o udzielenie upoważnienia dostępu do danych osobowych

…………………………………………………………………………………………………….…………

………………………………................... w zakresie dotyczącym przetwarzania danych   
w celu…………………………………………………………………………………,

od dnia …………………. do dnia…………………

Jednocześnie zobowiązuję się do zachowania w tajemnicy informacji, z którymi za poznam się podczas korzystania z ……………………………………………………………

…………………………………………………………………………..

*(data i podpis wnioskodawcy)*

***Załącznik nr 8***

**WNIOSEK O UDOSTĘPNIENIE DANYCH ZE ZBIORU DANYCH OSOBOWYCH**

1.Wniosek do .....................................................................................................................................

*(dokładne oznaczenie Administratora Danych Osobowych)*

2.Wnioskodawca ............................................................................................................................................

.........................................................................................................................................................................

*(nazwa firmy i jej siedziba albo nazwisko, imię i adres zamieszkania wnioskodawcy)*

3.Podstawa prawna upoważniająca do pozyskania danych albo wskazanie wiarygodnie uzasadnionej potrzeby posiadania danych w przypadku osób innych niż wymienione w ustawie z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. 2018, poz. 1000)

..………………………………………………………………………………………………….……………………

..………………………………………………………………………………………………….……………………

4. Wskazanie przeznaczenia dla udostępnionych danych

..……………………………… ………………………………………………………………….……………………

..………………………………………………………………………………………………….……………………

5. Oznaczenie lub nazwa zbioru, z którego mają być udostępnione dane

..………………………………………………………………………………………………….……………………

..………………………………………………………………………………………………….……………………

6. Zakres żądanych informacji ze zbioru

..………………………………………………………………………………………………….……………………

..………………………………………………………………………………………………….……………………

7. Informacje umożliwiające wyszukiwanie w zbiorze danych

..………………………………………………………………………………………………….……………………

..………………………………

………………………………………………………………….……………………

........................................................................

*(data, podpis ew. pieczęć wnioskodawcy)*

Pokwitowanie nr...................................

Kwituję odbiór dnia ........................................................

***Załącznik nr 9***

klasa ……

Sosnowiec, dn.

……………………….

w ZSO nr 5  
w Sosnowcu

ul.Bohaterów Monte Cassino 46

**ZGODA NA WYKORZYSTANIE WIZERUNKU DZIECKA**

Oświadczam, że wyrażam zgodę na rejestrowanie wizerunku mojego dziecka podczas zajęć i uroczystości szkolnych organizowanych przez Szkołę oraz wykorzystanie tego wizerunku poprzez umieszczanie zdjęć   
na stronie internetowej szkoły, w gablotach szkolnych, w gazetce szkolnej oraz w celu informacji i promocji Szkoły.

|  |  |  |
| --- | --- | --- |
| Nazwisko i imię rodzica/opiekuna prawnego |  |  |
| Lp. Nazwisko i imię ucznia | Podpis rodzica/opiekun prawnego |  |
|  |  |

1

2

3

…

Podstawa prawna:

*Ustawa o ochronie danych osobowych z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. 2018, poz. 1000)*

…………………..…………………………..

*(data, podpis wychowawcy)*

***Załącznik nr 10***

**UMOWA POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH**

Zawarta w ……………….., w dniu……………..

pomiędzy:

* ………………………………………………………………………………………..

reprezentowanym przez

………………………………………………………………………………………………

zwanym dalej **Administratorem Danych Osobowych,**

a

……………………………………………………………………………………………..

reprezentowanym przez

1. ……………………………………………………………………………………

2. ………………………………………………

……………………………………

zwanym dalej **zleceniobiorcą.**

* + **1**

1. Administrator Danych Osobowych na podstawie *ustawy z dnia 10 maja 2018 r. o ochronie* *danych osobowych* (DzU 2018, poz.1000 ), zwanej dalej ustawąo ochronie danychosobowych, powierza zleceniobiorcy przetwarzanie danych osobowych, wyłącznie w zakresie i celu przewidzianym niniejszą umową.
2. Szczegółowy zakres przetwarzania, struktur ę baz danych, metody zabezpieczania, stanowią załącznik do niniejszej umowy.
   * **2**
3. Zleceniobiorca będzie przetwarzał dane osobowe pracowników i dane os osobowe uczniów oraz ich rodziców i opiekunów prawnych w zakresie wynikającym z:
   1. ustawy z dnia 26 stycznia 1982 r. – Karta Nauczyciela (DzU 2006 nr 97, poz. 674 ze zm.),
   2. ustawy z dnia 26 czerwca 1974 r. – Kodeks Pracy (Dz U 1998 nr 21, poz 94 ze zm.).
      * **3**

Administrator Danych Osobowych powierza zleceniobiorcy przetwarzanie danych, o których mowa w § 2

niniejszej umowy, w celu …………… ………………………………...

**§ 4**

Zleceniobiorca zobowiązuje się do:

1. zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności   
   do zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem prawa oraz zmianą, utratą, uszkodzeniem lub zniszczeniem,
2. prowadzenia dokumentacji opisującej sposób przetwarzania danych oraz środki, o których mowa   
   w pkt 1,
3. wyznaczenia Administratora Bezpieczeństwa Informacji, nadzorującego przestrzeganie zasad ochrony,   
   o których mowa w pkt 1, chyba, że wykonuje te czynności sam,
4. dopuszczania do przetwarzania danych wyłącznie osób posiadających upoważnienie,
5. zapewnienia kontroli nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane,
6. prowadzenia ewidencji osób upoważnionych do przetwarzania danych osobowych,
7. prowadzenia dokumentacji w sposób i w zakresie określonym w *rozporządzeniu 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* (DzU 2004 nr 100, poz. 1024),zwanym dalej rozporządzeniem Ministra Spraw Wewnętrznych i Administracji,
8. spełnienia warunków technicznych i organizacyjnych, urządzeń i systemów informatycznych służących do przetwarzania danych osobowych, zgodnie z rozporządzeniem Ministra Spraw Wewnętrznych   
   i Administracji.
   * **5**

Za wykonanie umowy zleceniobiorcy nie przysługuje/przysługuje wynagrodzenie w wysokości……………………

**§ 6**

Wszelkie zmiany do niniejszej umowy wymagają formy pisemnej pod rygorem nieważności.

**§ 7**

W sprawach nieuregulowanych w niniejszej umowie zastosowanie mają przepisy Kodeksu cywilnego oraz ustawy o ochronie danych osobowych.

**§ 8**

Umowę sporządzono w dwóch, jednobrzmiących egzemplarzach, po jednym dla każdej ze stron.

……………………………………………………………

………………………………………………..

*Administrator Danych Osobowych*

*Zleceniobiorca*

***Załącznik nr 11***

**KONTROLA WEWNĘTRZNA – PODSTAWOWE ZAGADNIENIA**

|  |  |  |  |
| --- | --- | --- | --- |
| Lp. | Zagadnienie | **Tak** | **Nie** |
|  |  |  |  |
| 1 | Czy wszyscy pracownicy przetwarzający dane osobowe posiadają odpowiednie |  |  |
|  | upoważnienia zgodnie z art. 37 ustawy? |  |  |
|  |  |  |  |
| 2 | Czy prowadzona jest ewidencja osób upoważnionych do przetwarzania danych |  |  |
|  | osobowych zgodnie z art. 39 ust. 2 ustawy? |  |  |
|  |  |  |  |
| 3 | Czy wyznaczono Administratora Bezpieczeństwa Informacji zgodnie z art. 36 ust. 3 |  |  |
|  | ustawy (o ile nadzór nad przestrzeganiem zasad ochrony danych osobowych nie jest |  |  |
|  | sprawowany przez dyrektora osobiście)? |  |  |
|  |  |  |  |
| 4 | Czy zawarto umowy powierzenia przetwarzania danych osobowych |  |  |
|  | z podmiotami, którym powierzono przetwarzanie danych osobowych zgodnie |  |  |
|  | z art. 31 ustawy? |  |  |
|  |  |  |  |
| 5 | Czy wprowadzono zabezpieczenia w zakresie zabezpieczenia danych osobowych |  |  |
|  | odpowiednie do zagrożeń oraz kategorii danych będących przedmiotem ochrony |  |  |
|  | zgodnie z art. 36 ustawy1? |  |  |
| 6 | Czy w każdym przypadku, w którym dane osobowe przekazywane są podmiotom |  |  |
|  | trzecim, istnieje do tego podstawa prawna? |  |  |
|  |  |  |  |
| 7 | Czy istnieje podstawa prawna do przetwarzania każdej kategorii danych osobowych |  |  |
|  | pobieranych przez szkoły? |  |  |
|  |  |  |  |
| 8 | Czy dane przetwarzane są zgodnie z celem, dla którego zostały zebrane? |  |  |
|  |  |  |  |
| 9 | Czy osobom, których dane s ą przetwarzane, zapewnia się możliwość korzystania |  |  |
|  | z uprawnień przewidzianych w rozdziale IV ustawy (prawo do kontroli, uzupełniania |  |  |
|  | i prostowania przetwarzanych danych)? |  |  |
|  |  |  |  |
| 10 | Czy sporządzono dokumentację opisującą przetwarzanie danych osobowych, o której |  |  |
|  | mowa w § 1 ust. 1 rozporządzenia tj.: |  |  |
|  | • Politykę bezpieczeństwa, |  |  |
|  | • Instrukcję zarządzania systemem informatycznym? |  |  |
|  |  |  |  |
| 11 | Czy urządzenia i systemy informatyczne, w których przetwarzane są dane osobowe, |  |  |
|  | spełniają wymagania rozporządzenia, a szczególnie 2: |  |  |
|  | • każdy użytkownik ma swój identyfikator i hasło; |  |  |
|  | • hasło służące do uwierzytelniania użytkowników składa się co najmniej |  |  |
|  | z 8 znaków i zawiera małe i wielkie litery oraz cyf ry lub znaki specjalne oraz jego |  |  |
|  | zmiana jest dokonywana nie rzadziej niż co 30 dni; |  |  |
|  | • system chroniony jest przed zagro żeniami pochodzącymi z sieci publicznej (wirusami, |  |  |
|  | tzw. trojanami)? |  |  |
|  |  |  |  |
| 12 | Czy zarejestrowano u Generalnego Inspektora zbiory danych osobowych |  |  |
|  | niepodlegające zwolnieniu na podstawie art. 43 ustawy? |  |  |
|  |  |  |  |

1. Ustalenie, jakie zabezpieczenia należy zastosować i czy spełniają swoją rolę, jest kwestią cenną i wymaga każdorazowej ewaluacji okoliczności i warunków, w których przetwarzane są dane osobowe.
2. Ze względu na obszerność wymagań stawianych przez rozporządzenie wskazano jedynie podstawowe obowiązki. Wskazane jest, by weryfikacja, czy system teleinformatyczny spełnia wszystkie wymagania, została dokonana wspól nie z informatykiem.

***Załącznik nr 12***

**RAPORT**

**Z NARUSZENIA BEZPIECZEŃSTWA ZASAD OCHRONY DANYCH OSOBOWYCH**

w ……………………………………………………………………………….

Data i godzina zgłoszenia naruszenia: ............................................

1. Osoba powiadamiająca o zaistniałym zdarzeniu:

………………………………………………………..……………………………………

*(imię, nazwisko, stanowisko służbowe)*

1. Lokalizacja zdarzenia:

………………………………………………………..………………………………………

*(np.: nr pokoju, nazwa pomieszczenia)*

1. Rodzaj naruszenia bezpieczeństwa:

………………………………………………………..………………………………………

1. Ustalenia dotyczące charakteru i rodzaju naruszenia oraz metody działania osób naruszających zabezpieczenie systemu:

………………………………………………………..………………………………………

1. Opis przebiegu naruszenia:

………………………………………………………..…………………………………

1. Przyczyny wystąpienia zdarzenia:

………………………………………………………..…………………………………

1. Podjęte działania:

………………………………………………………..…………………………………

1. Wnioski wynikające ze zdarzenia:

……………………………………………………………………………........................

1. Postępowanie wyjaśniające:

……………………………………………………..…………………………………

1. Działania, które należy podjąć:………………………………………………………..…………………………………

…………………………………..………………………………………………….

*(data, podpis Administrator Danych Osobowych)*