***Załącznik Nr 1***

*do Zarządzenia Nr 33/2017/2018 z dnia 28 lutego 2018r.*

**POLITYKA BEZPIECZEŃSTWA**

**OCHRONY DANYCH OSOBOWYCH**

Szkoła Podstawowa nr 16 z Oddziałami Integracyjnymi im. Tadeusza Kościuszki w Pabianicach, ul. 20 Stycznia 9/13

|  |  |  |  |
| --- | --- | --- | --- |
|  | | **pieczątka szkoły:** | |
| **opracował:** | **data:** | **zatwierdził:** | **data:** |
|  |  |  |  |

**I. POSTANOWIENIA OGÓLNE**

**§1.**

Polityka Bezpieczeństwa ochrony danych osobowych jest dokumentem opisującym zasady ochrony danych osobowych stosowane przez:

Szkołę Podstawową nr 16 z Oddziałami Integracyjnymi im. Tadeusza Kościuszki w Pabianicach, ul. 20 Stycznia 9/13

**Celem** Polityki Bezpieczeństwa ochrony danych osobowych, zwanej dalej Polityką Bezpieczeństwa, jest uzyskanie optymalnego i zgodnego z obowiązującym stanem prawnym sposobu przetwarzania informacji zawierających dane osobowe.

Całość procesów odbywa się przy zachowaniu poufności, integralności i dostępności informacji chronionych oraz dużym wsparciu i zaangażowaniu pracowników oraz Dyrekcji szkoły.

Dokument wskazuje działania, jakie należy podejmować w celu zwiększenia świadomości, wiedzy i poczucia odpowiedzialności osób przetwarzających dane osobowe, w tym ciążących na nich obowiązkach i konsekwencjach za niewłaściwe przetwarzanie danych osobowych osób fizycznych, tj. uczniów, rodziców i opiekunów prawnych uczniów, pracowników i współpracowników, osób odwiedzających i przebywających na terenie szkoły, gości oraz kontrahentów, zleceniobiorców współpracujących z placówką.

Bezpieczeństwo informacji rozumiane jest tutaj jako osiągnięcie takiego poziomu organizacyjnego i technicznego, który:

– zagwarantuje zachowanie poufności informacji chronionych;

– zapewni integralność informacji chronionych i jawnych oraz właściwą dostępność do nich;

– zagwarantuje wymagany poziom bezpieczeństwa przetwarzanych informacji;

– maksymalnie ograniczy występowanie zagrożeń dla bezpieczeństwa informacji;

– zapewni poprawne i bezpieczne funkcjonowanie systemów przetwarzania informacji;

– zapewni podejmowanie odpowiednich działań w sytuacjach naruszenia lub podejrzenia naruszenia bezpieczeństwa informacji oraz określi konsekwencje w przypadku naruszenia niniejszych zasad.

Polityka Bezpieczeństwa obowiązuje wszystkie osoby zatrudnione, osoby i podmioty pracujące na zasadach umów cywilno-prawnych oraz innych form współpracy w tut. placówce, zwraca uwagę na konsekwencje, jakie mogą ponosić osoby naruszające zasady obowiązujące w szkole.

Przetwarzanie danych osobowych w tut. szkole odbywa się zarówno za pomocą systemów informatycznych, jak i w postaci tradycyjnej – papierowej, za pośrednictwem poczty elektronicznej, telefonicznie, ustnie oraz za pomocą obrazu (w tym monitoringu wizyjnego).

**II. PODSTAWA PRAWNA**

**§2.**

1. Ustawa o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (tekst pierwotny: Dz. U. 1997r. Nr 133 poz. 883 z późn. zm., t. j. Dz. U. z 2016r. poz. 922 z późn. zm).
2. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024).
3. Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 10 grudnia 2014 r. w sprawie wzorów zgłoszeń powołania i odwołania administratora bezpieczeństwa informacji (Dz. U. 2014, poz. 1934).
4. Rozporządzenie Ministra Administracji i Cyfryzacji z 11 maja 2015 r. w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbiorów danych (Dz. U. z 2015, poz. 719).
5. Rozporządzenie Ministra Administracji i Cyfryzacji z dni 11 maja 2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewnienia przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji (Dz. U. z 2015, poz. 745).
6. Konstytucja Rzeczypospolitej Polskiej (art. 47, 51)
7. Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 2016/679 z 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) - RODO (Dz. Urz. UE L 119 z 4.05.2016).

**III. SŁOWNIK POJĘĆ**

**§3.**

1. ustawa – ustawa o ochronie danych osobowych z dnia 29 sierpnia 1997r. (tekst pierwotny: Dz. U. 1997r. Nr 133 poz. 883 z późn. zm., t. j. Dz. U. z 2016r. poz. 922 z późn. zm),
2. dane osobowe – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej,
3. zbiór danych osobowych – posiadający strukturę zestaw danych o charakterze osobowym, dostępny według określonych kryteriów,
4. przetwarzanie danych osobowych – jakiekolwiek operacje wykonywane na danych osobowych, jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie danych osobowych, niszczenie, w systemach informatycznych, jak i tradycyjnych,
5. osoba upoważniona - osoba upoważniona do przetwarzania danych osobowych w Szkole Podstawowej nr 16 z Oddziałami Integracyjnymi w Pabianicach,
6. Administrator Danych (AD) – Dyrektor Szkoły Podstawowej nr 16 z Oddziałami Integracyjnymi w Pabianicach,
7. Administrator Bezpieczeństwa Informacji (ABI) – osoba powołana przez Administratora Danych do realizowania zadań z zakresu bezpieczeństwa informacji i ochrony danych osobowych, zgłoszona do ogólnokrajowego rejestru Administratorów Bezpieczeństwa Informacji prowadzonego przez Generalnego Inspektora Ochrony Danych Osobowych, działająca na zasadzie umowy cywilno-prawnej,
8. Administrator Systemów Informatycznych (ASI) – pracownik szkoły, osoba upoważniona, wyznaczona i odpowiedzialna za administrowanie systemami informatycznymi oraz nadzór nad bieżącą konserwacją sprzętu i oprogramowania,
9. Administrator elektronicznego dziennika – osoba odpowiedzialna za dokonywanie zmian w programie e-oceny, w tym nadawanie, zmianę i odbieranie uprawnień w  programie – uprawniony pracownik szkoły,
10. osoba trzecia - osoba nieupoważniona do przetwarzania danych osobowych w tut. szkole,
11. system informatyczny – współpracujące ze sobą urządzenia, systemy, programy, procedury służące do przetwarzania danych,
12. zabezpieczenie danych w systemie informatycznym – wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym dostępem.

**IV. ADMINISTRATOR BEZPIECZEŃSTWA INFORMACJI**

**§4.**

Administrator Danych (AD) wyznaczył Administratora Bezpieczeństwa Informacji (ABI), którego zadaniem jest zapewnienie przestrzegania przepisów o ochronie danych osobowych (zgodnie z art. 36a ust. 2 pkt.1-2 ustawy). Administrator Danych zgłosił Administratora Bezpieczeństwa Informacji do ogólnokrajowego rejestru prowadzonego przez Generalnego Inspektora Danych Osobowych.

Do zadań Administratora Bezpieczeństwa Informacji (ABI) należy szczególności:

1) zapewnianie przestrzegania przepisów o ochronie danych osobowych, w szczególności przez:

a) sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania dla administratora danych,

b) nadzorowanie opracowania i aktualizowania dokumentacji z ww. zakresu oraz przestrzegania zasad w niej określonych,

c) zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych.

2) prowadzenie rejestru zbiorów danych przetwarzanych przez administratora danych.

Każda osoba upoważniona do przetwarzania danych osobowych w Szkole Podstawowej nr 16 z Oddziałami Integracyjnymi w Pabianicach, zobowiązana jest do bezzwłocznego informowania Administratora Bezpieczeństwa Informacji o wszelkich zdarzeniach mających wpływ na prawidłową realizację przepisów z zakresu ochrony danych osobowych (drogą e-mail, telefonicznie, osobiście, za pośrednictwem poczty tradycyjnej, Sekretariatu szkoły, Dyrektora szkoły).

**V. WYKAZ BUDYNKÓW, POMIESZCZEŃ LUB CZĘŚCI POMIESZCZEŃ, TWORZĄCYCH OBSZAR, W KTÓRYM PRZETWARZANE SĄ DANE OSOBOWE**

**§ 5.**

Dane osobowe przetwarzane są w budynku przy ul. 20 Stycznia 9/13, 95-200 Pabianice:

|  |  |
| --- | --- |
| Nazwa pomieszczenia | Liczba pomieszczeń |
| Sale lekcyjne – 27 pomieszczeń | nowy budynek - parter: 3,  I piętro: 6, II piętro: 3,  stary budynek – I piętro: 6,  II piętro: 7,  III piętro: 2 |
| Pracownie szkolne – informatyczna | 2 |
| Pracownie szkolne –chemiczna | 2 |
| Pracownie szkolne –fizyczna | 2 |
| Pracownie szkolne –techniczna | 1 |
| Pracownie szkolne –biologiczna | 1 |
| Biblioteka 1 pomieszczenie | 1 |
| Świetlica | 2 |
| Sale gimnastyczne | 3 |
| Siłownia | 1 |
| ~~Kuchnia,~~ stołówka Intendent na stołówce pomieszczenie internet | 1 |
| Gabinet opieki przedmedycznej, pielęgniarki umowa PCM | 1 |
| Gabinet psychologa i pedagoga. | 1 |
| Księgowość | 2 pomieszczenia  stary budynek - parter  nowy budynek - I piętro |
| Sekretariat | stary budynek – parter: 1 |
| Gabinet Dyrektora | stary budynek – parter: 1 |
| Gabinet Wicedyrektora | stary budynek – parter: 2 |
|  |  |
| Główny specjalista | nowy budynek – I piętro: 1 |
| Kierownik Gospodarczy | parter - 1 |
| Kasa | pater stary - 1 |
| Portiernia - podgląd monitoring | wejście do szkoły |

oraz u procesorów (przetwarzających) dane osobowe placówki, zgodnie z aktualnymi umowami powierzenia przetwarzania danych osobowych.

**VI. WYKAZ ZBIORÓW DANYCH OSOBOWYCH WRAZ ZE WSKAZANIEM PROGRAMÓW ZASTOSOWANYCH DO PRZETWARZANIA TYCH DANYCH**

**§6.**

Zbiory danych osobowych przetwarzane są w architekturze centralnej, z użyciem systemów informatycznych połączonych z siecią publiczną (Internetem). Zbiór danych poz. 2, 3, 5, 6, 8, 9, 11, 12, podlegają zwolnieniu z obowiązku rejestracji zarówno w rejestrze prowadzonym przez Administratora Bezpieczeństwa Informacji, jak i rejestrze prowadzonym przez Generalnego Inspektora Danych Osobowych – zgodnie z art. 43 ust. 1 oraz 1a ustawy.

Zbiory poz. 1, 4, 7, 10, 13 podlegają wpisowi w wewnętrznym rejestrze prowadzonym przez Administratora Bezpieczeństwa Informacji, a zbiór poz. 1 i dodatkowo podlega zgłoszeniu do rejestru prowadzonego przez Generalnego Inspektora Ochrony Danych Osobowych ze względu na zawartość danych osobowych z zakresu art. 27 ustawy.

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Nazwa zbioru danych osobowych** | **Program zastosowany do przetwarzania** | **Sposób/forma przetwarzania** |
| 1. | Rekrutacja uczniów do szkoły | Pakiet biurowy | papierowa, wydruk |
| 2. | Dane osobowe uczniów, ich rodziców i opiekunów prawnych | Dziennik elektroniczny, Vulcan Optivum moduły: MOL, Sputnik: Faktury, SIO, pakiet biurowy | elektroniczna, papierowa- wydruk |
| 3. | Upoważnienia do odbioru uczniów ze szkoły | Pakiet biurowy | papierowa, wydruk |
| 4. | |  |  |  | | --- | --- | --- | | |  |  | | --- | --- | | |  | | --- | | Księga ewidencji uczniów realizujących obowiązek szkolny w innych szkołach | | | |  | | Vulcan Optivum: UONET, pakiet biurowy | elektroniczna, papierowa, wydruk |
| 5. | Umowy najmu | Pakiet biurowy | papierowa, wydruk |
| 6. | Zbiór danych osobowych pracowników oraz członków ich rodzin | Vulcan Optivum moduły: Kadry, Płace, (Sekretariat, Zastępstwa, Plan lekcji), MOL, dziennik elektroniczny,UONET+, SIO, Płatnik ZUS, eRU - PZU, PUE – ZUS, Sputnik: Faktury, bankowość elektroniczna | elektroniczna, papierowa – wydruk |
| 7. | Rejestr korespondencji | e-PUAP | Papierowa - dziennik korespondencji, elektroniczna – platforma e-PUAP, wydruk, poczta e-mail |
| 8. | Zamówienia publiczne | Pakiet biurowy | papierowa, wydruk |
| 9. | Składnica akt | - | papierowa |
| 10. | Rejestr biblioteczny | Vulcan Optivum: moduł MOL | elektroniczna, papierowa, wydruk |
| 11. | Konkursy międzyszkolne | Pakiet biurowy | Papierowa, wydruk |
| 12. | Rejestr faktur | Sputnik: moduł Faktury | elektroniczna, papierowa- wydruk |
| 13. | Monitoring wizyjny | Oprogramowanie rejestratora URMET 1093/008 H264 8CH – 1zt, URMET 1093/005 H264 8CH – 3szt, 28 kanałów | elektroniczna |

**VII. OPIS STRUKTURY ZBIORÓW DANYCH WSKAZUJĄCY ZAWARTOŚĆ POSZCZEGÓLNYCH PÓL INFORMACYJNYCH I POWIĄZAŃ MIĘDZY NIMI**

**§7.**

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Nazwa zbioru danych osobowych** | **Zawartość pól informacyjnych** | **Powiązania** |
| 1. | Rekrutacja uczniów do szkoły | Dane osobowe niezbędne do procesu rekrutacji - spełnienie obowiązku wynikającego z przepisu prawa, w tym:  imiona, nazwiska, imiona rodziców, data i miejsce urodzenia, adres zameldowania i zamieszkania (pobytu), nr Pesel,  nr telefonu, e-mail, stan zdrowia, w tym orzeczenia i opinie wydane w postępowaniu sądowym lub administracyjnym, oświadczenia | Powiązania ze zbiorami:  Dane osobowe uczniów, ich rodziców i opiekunów prawnych (2) |
| 2. | Dane osobowe uczniów, ich rodziców i opiekunów prawnych | Dane osobowe niezbędne do dopełnienia obowiązków określonych w przepisach prawa, związanych z:  - systemem oświaty,  - prowadzeniem dokumentacji z przebiegu działalności wychowawczej i opiekuńczej,  - udzielaniem pomocy psychologiczno-pedagogicznej,  - wydawaniem dyplomów i innych druków,  - organizowaniem wycieczek, konkursów  - ubezpieczeniem następstw nieszczęśliwych wypadków  - bhp,  - przekonaniami religijnymi,  - stanem zdrowia,  - innymi orzeczeniami wydanymi w postępowaniu sądowym lub administracyjnym,  w tym:  imiona, nazwiska, imiona rodziców, data i miejsce urodzenia, adres zamieszkania lub pobytu, nr Pesel,  seria oraz numer dokumentu tożsamości, nr telefonu, e-mail, stan zdrowia,  dane identyfikacyjne rodziców lub opiekunów prawnych, oświadczenia za zgodą rodzica/opiekuna prawnego:  - oświadczenie w sprawie nauki religii,  - dane do ubezpieczenia grupowego,  - organizowania wycieczek szkolnych,  - udziału w olimpiadach, konkursach,  - wizerunek (zdjęcie, film) | Powiązania ze zbiorami:  Rekrutacja uczniów do szkoły (1), Upoważnienia do odbioru uczniów ze szkoły (3), Rejestr korespondencji (7), Składnica akt (9), Rejestr biblioteczny (10),Konkursy międzyszkolne (11), Rejestr faktur (12), Monitoring wewnętrzny oraz zewnętrzny (13) – przepływy manualne, poczta elektroniczna, automatycznie w ramach modułów Vulcan Optivum |
| 3. | Upoważnienia do odbioru uczniów ze szkoły | imiona, nazwiska, data i miejsce urodzenia, miejsce pracy, stopień pokrewieństwa, seria oraz numer dokumentu tożsamości, nr telefonu, e-mail | Powiązania ze zbiorem: Dane osobowe uczniów, ich rodziców i opiekunów prawnych  (2) – przepływ manualny |
| 4. | |  |  |  | | --- | --- | --- | | |  |  | | --- | --- | | |  | | --- | | Księga ewidencji uczniów realizujących obowiązek szkolny w innych szkołach | | | |  | | Imiona, nazwiska, imiona rodziców, data i miejsce urodzenia, adres zamieszkania, pobytu, PESEL, nazwa i adres placówki oświatowej | Powiązania ze zbiorem: Rejestr korespondencji (7) - przepływ manualny |
| 5. | Umowy najmu | Imiona, nazwiska, adres zamieszkania, NIP, seria oraz numer dokumentu tożsamości, nr telefonu, adres e-mail | Powiązania ze zbiorem: Rejestr korespondencji (7) - przepływ manualny |
| 6. | Zbiór danych osobowych pracowników oraz członków ich rodzin | Dane osobowe pracowników, niezbędne do dopełnienia obowiązków określonych w przepisach prawa (art. 221 Kodeksu Pracy), wynikających/związanych:  - ze stosunkiem pracy/umową cywilno-prawną, w tym prowadzeniem dokumentacji pracowniczej,  - kartą nauczyciela,  - prowadzeniem SIO, arkusza organizacyjnego,  - ubezpieczeniami społeczno-emerytalnymi, rentowymi, zdrowotnymi,  - do celów podatkowych,  - dot. niekaralności,  - funduszem świadczeń socjalnych (w tym dane osobowe członków rodzin),  - dobrowolnym ubezpieczeniem pracowniczym (grupowym),  - bankowości elektronicznej,  - bhp,  - sanitarno-epidemiologicznym  oraz dodatkowo: dane kontaktowe pracownika: nr telefonu, adres e-mail,  wizerunek | Powiązania ze zbiorami: składnica akt (9) – przepływ manualny; rejestr korespondencji (7) - przepływ manualny, poczta e-mail, platforma e-PUAP, Rejestr biblioteczny (10), Rejestr faktur (12), Monitoring wewnętrzny oraz zewnętrzny (13) – manualnie |
| 7. | Rejestr korespondencji | Imiona, nazwiska, adres do korespondencji, adres zamieszkania lub pobytu, adres e-mail, nr telefonu, identyfikator użytkownika (e-PUAP) | Powiązania z pozostałymi zbiorami w zakresie korespondencji papierowej, elektronicznej (e-mail, platforma e-PUAP) |
|  | Zamówienia publiczne | Imiona, nazwiska osób fizycznych prowadzących działalność gospodarczą, nazwa firmy, adres zamieszkania, adres prowadzenia działalności, adres do korespondencji, NIP, Regon, KRS, polisa ubezpieczeniowa OC, nr rachunku bankowego, nr telefonu, adres e-mail, wydruk CEIDG | Powiązania ze zbiorami: składnica akt (9) - przepływ manualny, Rejestr korespondencji (7) - przepływ manualny, poczta elektroniczna, platforma e-PUAP, |
|  | Składnica akt | Dane osobowe zawarte w pozostałych zbiorach danych, przekazane do archiwizacji, zgodnie z obowiązującymi przepisami i procedurami wewnętrznymi | Powiązania z pozostałymi zbiorami w zakresie wynikającym z obowiązku archiwizacji dokumentów, przepływ manualny |
|  | Rejestr biblioteczny | Imiona, nazwiska, nazwa i adres placówki oświatowej, klasa | Powiązania ze zbiorami:  Dane osobowe uczniów, ich rodziców i opiekunów prawnych (2) – przepływ manualny z możliwością importu danych z modułu Vulcan Optivum |
|  | Konkursy międzyszkolne | Imiona, nazwiska, data urodzenia, klasa, nazwa i adres placówki macierzystej,  dane nauczyciela/opiekuna, (dane kontaktowe nr tel., e-mail) | Powiązania ze zbiorami: Składnica akt (9), Dane osobowe uczniów, ich rodziców i opiekunów prawnych (2) – przepływy manualne |
|  | Rejestr faktur | Imiona, nazwiska, nazwa firmy, NIP, adres prowadzenia działalności gospodarczej | Powiązania ze zbiorami:  Dane osobowe uczniów, ich rodziców i opiekunów prawnych (2), Umowy najmu (5), Rejestr korespondencji (7)  Zamówienia publiczne (8),  Składnica akt (9) - przepływy manualne |
|  | Monitoring wewnętrzny oraz zewnętrzny | Obraz bez dźwięku, czas i miejsce | Brak bezpośrednich powiązań, w nagłych zdarzeniach możliwość uzyskania wizerunku osób przebywających na terenie szkoły, w tym wizerunku pracowników, uczniów, opiekunów prawnych i innych osób |

**VIII. SPOSÓB PRZEPŁYWU DANYCH MIĘDZY SYSTEMAMI**

**§8.**

|  |  |  |
| --- | --- | --- |
| **Lp.** | **System informatyczny** | **Sposób przepływu danych** |
| 1. | VULCAN OPTIVUM – złoty abonament | sieć wewnętrzna, moduły: Kadry, Płace, UONET+, e-dziennik, Sekretariat, Zastępstwa, Plan Lekcji, MOL.  Przepływ automatyczny między poszczególnymi modułami, możliwość przepływu jednokierunkowo oraz dwukierunkowo.  Eksport danych do sieci telekomunikacyjnej za pomocą bezpiecznego połączenia do systemu bankowość elektroniczna, ZUS – Płatnik oraz przepływ manualny pomiędzy modułami i systemami. Import danych z PUE –ZUS. |
| 2. | SIO (System Informacji Oświatowej) | przepływ poprzez sieć telekomunikacyjną – teletransmisja danych za pomocą bezpiecznego połączenia, przepływ dwukierunkowo – manualnie do systemu SIO. |
| 3. | Pakiet biurowy - Microsoft Office | Manualnie - za pośrednictwem zewnętrznych nośników danych pomiędzy zbiorami lub w postaci papierowej, dźwięku, obrazu. |
| 4. | Płatnik – ZUS | przepływ poprzez sieć telekomunikacyjną – teletransmisja danych za pomocą bezpiecznego połączenia, przepływ jednokierunkowo z systemem Vulcan Optivum. |
| 5. | eRU – PZU | przepływ poprzez sieć telekomunikacyjną – teletransmisja danych za pomocą bezpiecznego połączenia, przepływ manualny do systemu eRU-PZU. |
| 6. | PUE – ZUS | przepływ poprzez sieć telekomunikacyjną – teletransmisja danych za pomocą bezpiecznego połączenia, przepływ dwukierunkowo z PUE-ZUS. |
| 7. | ePUAP | przepływ poprzez sieć telekomunikacyjną – teletransmisja danych za pomocą bezpiecznego połączenia, przepływ dwukierunkowo, manualnie. |
| 8. | Bankowość elektroniczna | przepływ poprzez sieć telekomunikacyjną, teletransmisja danych za pomocą bezpiecznego połączenia, przepływ jednokierunkowy z systemu Vulcan Optivum oraz manualnie. |
| 9. | Sputnik | moduły: Ewka, Faktury, przepływ między modułami dwukierunkowo, brak bezpośrednich połączeń z innymi systemami, teletransmisja danych za pomocą bezpiecznego połączenia do administratora systemu, przepływ automatyczny do: Urząd Miejski w Pabianicach |
| 10. | Program do obsługi i zarządzaniamonitoringiem wizyjnymzainstalowany przez ZOM sp. z o.o.w Pabianicach | brak przepływów między systemami, możliwość przepływów manualnych |
| 11 | Dziennik elektroniczny (e-oceny) | brak przepływów między systemami, możliwość przepływów manualnych |

Przepływ danych miedzy systemami odbywa się w następujący sposób:

1. Manualnie - za pośrednictwem zewnętrznych nośników danych pomiędzy zbiorami lub w postaci papierowej, dźwięku, obrazu,
2. Jednokierunkowo – do odczytu
3. Dwukierunkowo – do odczytu i zapisu
4. Półautomatycznie (eksport/import danych)
5. Automatycznie

**IX. OKREŚLENIE ŚRODKÓW TECHNICZNYCH I ORGANIZACYJNYCH NIEZBĘDNYCH DLA ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZY PRZETWARZANIU DANYCH**

**§9.**

1. **Opis zdarzeń naruszających ochronę danych osobowych - INCYDENTY:**

Za naruszenie ochrony danych osobowych, zarówno zdarzeń losowych, jak i działań zamierzonych uważa się w szczególności:

1. Zagrożenia losowe, na które upoważniony do przetwarzania danych osobowych nie miał wpływu, lub miał ograniczony wpływ:

- zewnętrzne sytuacje, takie jak klęski żywiołowe (pożar, zalanie), awarie zasilania, utrata łączności,

- wewnętrzne, takie jak błąd ludzki, przypadkowe zniszczenie dokumentów, danych zapisanych na nośnikach informacji (utrata danych), awarie sprzętu, awaria systemu informatycznego.

1. Świadome, zamierzone działania osób uprawnionych i nieuprawnionych do przetwarzania danych osobowych w tut. placówce:

- dostęp lub próba dostępu do pomieszczeń, w których znajdują się dane osobowe przez osobę nieuprawnioną,

- nieuprawniony dostęp osób trzecich do danych osobowych – naruszenie poufności danych, poprzez udostępnienie przez osobę uprawnioną danych osobowych osobom nieupoważnionym/nieuprawnionym do ich dostępu (udostępnienie w formie dokumentu, e-maila pomyłkowo wysłanego w postaci pliku, dźwięku lub obrazu, np. zdjęcia, udostępnienia w formie ustnej), udostępnienie kodów alarmowych, innych informacji dot. zabezpieczeń pomieszczeń,

- wszelkie modyfikacje danych osobowych w systemach informatycznych oraz dokumentacji papierowej przez osoby nieuprawnione (np. zmiana zawartości danych, utrata całości lub części danych) - naruszenia integralności systemu,

- zmiana lub utrata danych zapisanych na kopiach zapasowych,

- nieuprawniony dostęp do systemu informatycznego (sygnał o nielegalnym logowaniu lub inny objaw wskazujący na próbę lub działanie związane z nielegalnym dostępem do systemu informatycznego),

- zniszczenie, uszkodzenie dokumentów, nośników informacji,

- wszelkie próby nieuprawnionej ingerencji w systemy informatyczne, zmierzające do zakłócenia ich działania bądź pozyskania w sposób niedozwolony (lub w celach niezgodnych z przeznaczeniem) danych zawartych w systemach informatycznych lub kartotekach,

- nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka / ekranu, brak ochrony haseł, niezamykanie pomieszczeń po opuszczeniu miejsca pracy, szaf, biurek z danymi chronionymi, niezabezpieczenie pieczęci służbowych, niewylogowanie się z systemu informatycznego.

1. Każdy zobowiązany do przestrzegania zasad ochrony danych osobowych w tut. placówce powinien zwrócić szczególną uwagę na inny stan systemu informatycznego lub pomieszczeń, niż pozostawiony po zakończeniu przez niego pracy.
2. Każde stwierdzone i odnotowane zdarzenie naruszające ochronę danych osobowych, skutkuje wdrożeniem postępowania wyjaśniającego przeprowadzonego przez Administratora Bezpieczeństwa Informacji, zgodnie z trybem i sposobem realizacji jego zadań.
3. **Środki zabezpieczające przed naruszeniem danych osobowych**

Środki organizacyjne:

1. Administrator Bezpieczeństwa Informacji przeprowadza nie rzadziej niż raz w roku oraz każdorazowo przy wystąpieniu incydentu, tj. naruszenia ochrony danych osobowych, analizę ryzyka przetwarzania danych osobowych, zakończoną audytem.
2. Każdy nowo zatrudniany pracownik, a także stażysta, praktykant oraz osoba pracująca na zasadzie umowy cywilno-prawnej, przed dopuszczeniem do dostępu, do danych osobowych podlega zapoznaniu z niniejszą dokumentacją oraz przeszkoleniu z obowiązujących zasad ochrony tych danych, co potwierdza podpisem na upoważnieniu do przetwarzania danych osobowych lub oświadczeniu o zachowaniu poufności (w zależności od zakresu dostępu do danych) oraz podlega wpisowi do „Ewidencji osób przeszkolonych z zakresu ochrony danych osobowych”.
3. Każdy upoważniony zostaje zobowiązany do bezwzględnego przestrzegania zasad ochrony przetwarzanych danych osobowych i zachowania ich w tajemnicy również po ustaniu zatrudnienia/umowy.
4. Wicedyrektor odpowiedzialny za sprawy organizacyjne, lub wyznaczony przez Wicedyrektora pracownik przekazuje do Administratora Bezpieczeństwa Informacji wszelkie dane niezbędne do identyfikacji osób nowozatrudnionych oraz informacje o zmianach w zakresie kadrowo-organizacyjnym placówki, celem dopełnienia zasad określonych w niniejszej dokumentacji.
5. Przetwarzać dane osobowe w tut. placówce może jedynie osoba, która otrzymała imienne upoważnienie nadane przez Administratora Danych (AD), na wniosek Administratora Bezpieczeństwa Informacji (ABI). Upoważnienie sporządza się w dwóch egzemplarzach - dla upoważnionego oraz do akt osobowych/dokumentacji upoważnionego. Administrator Bezpieczeństwa Informacji prowadzi i uaktualnia „Ewidencję osób upoważnionych do przetwarzania danych osobowych”

Środki techniczne

1. Dane osobowe przetwarzane są w obszarach przetwarzania – pomieszczeniach zamykanych na klucz, zabezpieczonych poprzez system alarmowy, z wykorzystaniem monitoringu wizyjnego. Dane przechowywane są w szafach i elementach meblowych zamykanych na klucz oraz w kasie pancernej.
2. Każdy kto opuszcza pomieszczenie jako ostatni (również w godzinach pracy) zobowiązany jest zabezpieczyć to pomieszczenie przed dostępem osób trzecich, zamykając je na klucz.
3. Przebywanie osób trzecich w pomieszczeniu, w którym przetwarzane są dane osobowe, dopuszczalne jest tylko w obecności osób upoważnionych.
4. W pomieszczeniach, gdzie dostęp mają osoby trzecie, monitory komputerów ustawione zostały w taki sposób, by uniemożliwić wgląd osobom nieupoważnionym.
5. W przypadku opuszczenia stanowiska komputerowego, upoważniony zobowiązany jest zastosować automatyczny wygaszacz ekranu, a w przypadku braku możliwości zastosowania automatycznego wygaszacza ekranu, zobowiązany jest zastosować skrót klawiszy „WINDOWS” plus „L”.
6. Dostęp do pomieszczeń objęty jest systemem całodobowego monitoringu.
7. Kontrola dostępu do pomieszczeń odbywa się poprzez pobieranie i zdawanie kluczy od pomieszczeń z portierni budynku przez pracowników obsługi. W przypadku pomieszczeń administracyjnych pracownicy dysponują indywidualnymi kluczami, zgodnie z wewnętrznymi procedurami.
8. Dokumenty podlegające archiwizacji przekazywane są za pośrednictwem upoważnionego pracownika placówki do Składnicy akt, a następnie przechowywane zgodnie z okresem ich przechowywania.
9. Pomieszczenia, w których przechowywane są dane osobowe zostały zabezpieczone przed skutkami pożaru zgodnie z przepisami prawa w zakresie ochrony przeciwpożarowej.
10. Dokumenty papierowe zawierające dane osobowe, których przydatność już ustała, niszczone są w sposób mechaniczny za pomocą niszczarek dokumentów, a elektroniczne nośniki informacji w sposób uniemożliwiających odczytanie danych (anonimizacja danych), zgodnie z zapisami instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych.
11. **Zasady postępowania w przypadku naruszenia (incydentu) oraz podejrzenia naruszenia ochrony danych osobowych**
12. Każda osoba upoważniona do przetwarzania danych osobowych jest zobowiązana do bezzwłocznego zawiadomienia Administratora Bezpieczeństwa Informacji (ABI) o naruszeniu lub podejrzeniu naruszenia ochrony danych osobowych. Ww. informację może przekazać osobiście, w formie informacji drogą e-mail, telefonicznie oraz za pośrednictwem Dyrektora, Wicedyrektora lub Sekretarza szkoły. Celem analizy skutków ryzyka i powzięcia dalszych czynności.
13. W przypadku stwierdzenia naruszenia ochrony danych osobowych Administrator Bezpieczeństwa Informacji wdraża procedurę INCYDENTU - przywraca w miarę możliwości stan zgodny z przepisami prawa, a w przypadku działań noszących znamiona przestępstwa – powiadamia organa ścigania.
14. Administrator Bezpieczeństwa Informacji po powzięciu informacji o naruszeniu lub uzasadnionym podejrzeniu naruszenia ochrony danych osobowych, powiadamia Administratora Danych (AD) o rozpoczęciu „Sprawdzenia/audytu doraźnego”, a następnie ocenia skalę Incydentu i dokumentuje czynności przeprowadzone w toku sprawdzenia, na podstawie których opracowuje dla Administratora Danych sprawozdanie w ww. zakresie. W części dotyczącej systemów informatycznych, wszelkie czynności dokonywane są w uzgodnieniu z Administratorem Systemów Informatycznych (ASI).
15. Osoba której dotyczy sprawdzenie, bierze w nim udział lub umożliwia Administratorowi Bezpieczeństwa Informacji przeprowadzenie czynności w toku sprawdzenia.
16. Administrator Bezpieczeństwa Informacji odnotowuje w „Ewidencji incydentów” zdarzenie naruszające ochronę danych osobowych, a następnie przedstawia Administratorowi Danych sprawozdanie ze sprawdzenia oraz propozycje wdrożenia środków zaradczych i naprawczych w celu zminimalizowania prawdopodobieństwa wystąpienia podobnego naruszenia w przyszłości.
17. Administrator Bezpieczeństwa Informacji w porozumieniu z Administratorem Danych wprowadza stosowne środki zaradcze, adekwatne do skali incydentu.
18. **Udostępnianie danych osobowych**

Każde udostępnienie danych osobowych może nastąpić wyłącznie w granicach obowiązujących przepisów prawa, a w przypadku wątpliwości co do podstaw prawnych udostępnienia danych osobowych należy skontaktować się z Administratorem Bezpieczeństwa Informacji.

1. **MONITORING WIZYJNY**

Jest to zamknięty system dający możliwość monitorowania potencjalnie niepokojących zachowań w obrębie chronionej strefy, tj. na terenie szkoły oraz terenach przyległych (wejście główne, parking).

Obiekt jest odpowiednio oznaczony, co pozwala osobom użytkującym pomieszczenia na właściwą identyfikację monitoringu (zamieszczono informacje przy każdym wejściu do szkoły, wraz z danymi Administratora Danych Osobowych oraz wskazaniem możliwości kontaktu dla osób przebywających na terenie placówki).

Sygnał udostępniony:

- do wglądu w gabinecie Dyrektora,

- do wglądu – portiernia budynku.

Podstawa prawna przetwarzania danych:

„w celu *zapewnienia bezpieczeństwa, porządku publicznego oraz ochrony osób i mienia.”*

*-* dostęp do rejestratora (hasło):

- dla Dyrektora placówki,

- dla wyznaczonego i upoważnionego pracownika szkoły.

Za zarządzanie kamerami odpowiadają rejestratory.

Nagrywanie odbywa się 24/h/dobę, zapis ciągły.

Obraz zapisywany jest na bieżąco i nadpisywany w czasookresach:

36 godzin – dla rejestratora w pomieszczeniu Kasy,

15 godzin, 17 godzin, 20 godzin – dla rejestratorów w pomieszczeniu Ochrony.

**X. OBOWIĄZKI I ODPOWIEDZIALNOŚĆ OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH**

**§10.**

Osoby upoważnione do przetwarzania danych osobowych w Szkole Podstawowej nr 16 z Oddziałami Specjalnymi w Pabianicach zobowiązane są do:

1. przetwarzania danych osobowych zgodnie z obowiązującymi przepisami prawa,
2. postępowania zgodnie z obowiązującą Polityką Bezpieczeństwa ochrony danych osobowych, Instrukcją zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych oraz innymi dokumentami wewnętrznymi z zakresu bezpieczeństwa informacji i ochrony danych osobowych,
3. zachowania w poufności danych osobowych oraz innych informacji poufnych uzyskanych w trakcie realizacji obowiązków służbowych/umów cywilno-prawnych, a także treści dokumentów wewnętrznych z zakresu bezpieczeństwa informacji i ochrony danych osobowych, również po ustaniu upoważnienia,
4. informowania Administratora Bezpieczeństwa Informacji o każdym naruszeniu lub podejrzeniu naruszenia bezpieczeństwa danych osobowych w tut. placówce.

Naruszenie ww. obowiązków może zostać uznane za naruszenie obowiązków pracowniczych w rozumieniu Kodeksu Pracy, a w przypadku naruszania przepisów o ochronie danych osobowych noszących znamiona przestępstwa, skutkować będzie zawiadomieniem właściwych organów ścigania – odpowiedzialność karna.

Za nieprzestrzeganie przepisów z zakresu ochrony danych osobowych grozi kara grzywny lub ograniczenia, pozbawienia wolności, zgodnie z zapisami rozdziału 8 ustawy.

**Załączniki:**

1. Wzór ewidencji osób przeszkolonych w zakresie ochrony danych osobowych i dokumentacji wewnętrznej z zakresu bezpieczeństwa informacji
2. Wzór upoważnienia do przetwarzania danych osobowych

2a) wzór oświadczenia osoby przebywającej w obszarze przetwarzania danych osobowych

1. Wzór ewidencji osób upoważnionych do przetwarzania danych
2. Wzór odwołania upoważnienia do przetwarzania danych osobowych
3. Wzór rejestru zbiorów danych osobowych prowadzony przez Administratora Bezpieczeństwa Informacji
4. Wzór ewidencji incydentów – naruszeń ochrony danych osobowych
5. Wzór ewidencji umów powierzenia przetwarzania danych osobowych