

# **POLITYKA BEZPIECZEŃSTWA**

**i**

## **INSTRUKCJA ZARZĄDZANIA SYSTEMEM PRZETWARZANIA DANYCH OSOBOWYCH**

**w**

**Gimnazjum  
im. ks. Wacława Rabczyńskiego w Wasilkowie  
ul. A. Mickiewicza 2  
16-010 Wasilków**

Wasilków 2014

## Podstawa prawna

- Konstytucja RP (art. 47 i 51)
- Konwencja nr 108 Rady Europy – dotycząca osób w związku z automatycznym przetwarzaniem danych osobowych
- Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, Dz.U. z 2002r. Nr 101, poz. 926 z późn. zm

Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. (Dz. U. z 2004 r. Nr100, poz. 1024) w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych

## Podstawowe pojęcia

### § 1

- **Szkoła** – w tym dokumencie jest rozumiana jako Gimnazjum im. ks. Wacława Rabczyńskiego, zlokalizowane przy ulicy A. Mickiewicza w Wasilkowie
- **Ustawa** — rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych z dnia 29 sierpnia 1997r. (tekst jedn. Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.)
- **Administrator Danych Osobowych (ADO)** – rozumie się przez to Dyrektora Gimnazjum im. ks. Wacława Rabczyńskiego w Wasilkowie
- **Lokalny Administrator Danych Osobowych (LADO)**– sekretarz szkoły, wicedyrektor, pedagog szkolny, wychowawcy świetlicy, wychowawcy klas, bibliotekarz, nauczyciele, intendent, pielęgniarka szkolna.
- **Administrator Bezpieczeństwa Informacji (ABI)** – osoba powołana zarządzeniem dyrektora, która odpowiada za bezpieczeństwo danych osobowych w systemie informatycznym szkoły, w tym w szczególności za przeciwdziałanie dostępowi osób niepowołanych do systemu, w których przetwarzane są dane osobowe oraz za podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń.
- **Dane osobowe** - w rozumieniu ustawy za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.
- **Przetwarzanie danych** - rozumie się przez to jakiegokolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych.
- **Zbiór danych** - każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów.
- **System informatyczny** - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
- **Identyfikator użytkownika (login)** - ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.
- **Hasło** - ciąg znaków literowych, cyfrowych lub innych, przypisany do identyfikatora użytkownika, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.
- **Uwierzytelnianie** — rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.
- **Integralność danych** — rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany.

- **Poufność danych** — rozumie się przez to właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym podmiotom.
- **Użytkownik systemu** – osoba upoważniona do przetwarzania danych osobowych w systemie. Użytkownikiem może być osoba zatrudniona w szkole, osoba wykonująca pracę na podstawie umowy zlecenia lub innej umowy cywilno-prawnej, osoba odbywająca staż w szkole.
- **Sieć lokalna** – połączenie komputerów pracujących w szkole w celu wymiany danych (informacji) dla własnych potrzeb, przy wykorzystaniu urządzeń telekomunikacyjnych
- **Sieć publiczna** – sieć telekomunikacyjna, niebędąca siecią wewnętrzną służąca do świadczenia usług telekomunikacyjnych w rozumieniu ustawy z dnia 21 lipca 2000r. – Prawo telekomunikacyjne (Dz.U. Nr 73, poz.852, z późn.zm.)
- **Sieć telekomunikacyjna** – urządzenia telekomunikacyjne zestawione i połączone w sposób umożliwiający przekaz sygnałów pomiędzy określonymi zakończeniami sieci za pomocą przewodów, fal radiowych, bądź optycznych lub innych środków wykorzystujących energię elektromagnetyczną w rozumieniu ustawy z dnia 21 lipca 2000r. – Prawo telekomunikacyjne (Dz.U.Nr 73, poz.852 z późn.zm.)
- **Teletransmisja** – przesłanie informacji za pomocą sieci telekomunikacyjnej.
- **Aplikacja** – program komputerowy wykonujący konkretne zadanie.
- **Wysoki poziom bezpieczeństwa** – musi występować wtedy, gdy przynajmniej jedno urządzenie systemu informatycznego, służące przetwarzania danych osobowych, połączone jest z siecią publiczną.

## 1. POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

### 1.1. Wykaz budynków, w których przetwarzane są dane osobowe

#### § 2

BUDYNEK - ADRES	POMIESZCZENIA
Gimnazjum im. ks. Wacława Rabczyńskiego w Wasilkowie ul. A. Mickiewicza 2 16-010 Wasilków	Gabinet dyrektora szkoły
	Kancelaria szkoły
	Sekretariat uczniowski
	Gabinet głównego księgowego
	Gabinet wicedyrektora szkoły
	Pokój nauczycielski
	Pokój nauczycieli w-f
	Gabinet pedagoga
	Gabinet psychologa
	Sale lekcyjne
	Biblioteka
	Archiwum

Kopie zapasowe zawierające zbiory danych osobowych przechowywane są w kancelarii szkoły, w budynku przy ul. A. Mickiewicza 2 w Wasilkowie.

**1.2. Zbiory danych przetwarzanych w systemach informatycznych i opis struktury przetwarzanych danych osobowych**

**§ 3**

<b>ZBIÓR DANYCH OSOBOWYCH</b>	<b>PROGRAM INFORMATYCZNY SŁUŻĄCY DO PRZETWARZANIA ZBIORU DANYCH</b>	<b>STRUKTURA DANYCH</b>
PRACOWNICY	<ul style="list-style-type: none"> <li>• KADRY OPTIVUM</li> <li>• PŁACE OPTIVUM</li> </ul> <p>Kadry i Płace Optivum występują jako dwa oddzielne systemy, które przetwarzają dane zawarte w jednym zbiorze.</p> <ul style="list-style-type: none"> <li>• ARKUSZ OPTIVUM</li> <li>• SIO</li> </ul>	<ul style="list-style-type: none"> <li>• PESEL</li> <li>• NIP</li> <li>• imię (imiona) i nazwisko (nazwiska)</li> <li>• imiona rodziców</li> <li>• nazwisko rodowe</li> <li>• obywatelstwo</li> <li>• dowód osobisty (seria, numer, przez kogo wydany, data wydania)</li> <li>• paszport</li> <li>• data i miejsce urodzenia</li> <li>• adres zameldowania</li> <li>• adres zamieszkania</li> <li>• adres korespondencyjny</li> <li>• numer telefonu, faxu</li> <li>• adres e-mail,</li> <li>• strona WWW</li> <li>• wysyłanie informacji e-mailem</li> <li>• oddział NFZ</li> <li>• urząd skarbowy</li> <li>• informacje o przetwarzaniu danych</li> <li>• prawo do emerytury lub renty</li> <li>• stopień niepełnosprawności</li> <li>• historia zatrudnienia</li> <li>• kwalifikacje</li> <li>• uprawnienia</li> <li>• kursy doskonalące</li> <li>• umiejętności</li> <li>• stan rodziny</li> <li>• stosunek do służby wojskowej</li> <li>• wykształcenie</li> <li>• stopień awansu zawodowego</li> <li>• warunki zatrudnienia (umowy)</li> <li>• wysokość wynagrodzenia</li> <li>• konto osobiste</li> <li>• staż pracy</li> <li>• absencje (urlopy, zwolnienia lekarskie itp.)</li> <li>• awans – staże</li> <li>• BHP i badania</li> <li>• nagrody, odznaczenia, kary, ocena pracy</li> <li>• legitymacje</li> <li>• upoważnienia</li> </ul>

		<ul style="list-style-type: none"> <li>• odzież robocza</li> <li>• zgłoszenia do ZUS</li> </ul>
PRACOWNICY	<ul style="list-style-type: none"> <li>• INWENTARZ OPTIVUM</li> </ul>	<ul style="list-style-type: none"> <li>• PESEL</li> <li>• imię (imiona) i nazwisko (nazwiska)</li> </ul>
	<ul style="list-style-type: none"> <li>• KASA OPTIVUM</li> </ul>	<ul style="list-style-type: none"> <li>• PESEL</li> <li>• imię (imiona) i nazwisko (nazwiska)</li> <li>• adres</li> </ul>
UCZNIOWIE	<ul style="list-style-type: none"> <li>• SEKRETRIAT OPTIVUM</li> <li>• DZIENNIK OPTIVUM</li> <li>• SIO</li> <li>• WORD</li> <li>• EXCEL</li> </ul>	<ul style="list-style-type: none"> <li>• PESEL</li> <li>• imię (imiona) i nazwisko (nazwiska)</li> <li>• data i miejsce urodzenia</li> <li>• adres stały</li> <li>• adres tymczasowy</li> <li>• imiona i nazwiska rodziców (opiekunów prawnych)</li> </ul>

### 1.3. Zbiory danych przetwarzanych tradycyjnie.

#### § 4

ZBIÓR DANYCH OSOBOWYCH	DOKUMENTACJA SŁUŻĄCA DO PRZETWARZANIA ZBIORU DANYCH	STRUKTURA DANYCH
PRACOWNICY	AKTA OSOBOWE	<ul style="list-style-type: none"> <li>• PESEL</li> <li>• NIP</li> <li>• imię (imiona) i nazwisko (nazwiska)</li> <li>• imiona rodziców</li> <li>• nazwisko rodowe</li> <li>• nazwisko rodowe matki</li> <li>• pochodzenie społeczne</li> <li>• obywatelstwo</li> <li>• dowód osobisty (seria, numer, przez kogo wydany, data wydania)</li> <li>• data i miejsce urodzenia</li> <li>• adres zameldowania</li> <li>• adres zamieszkania</li> <li>• adres korespondencyjny</li> <li>• numer telefonu, faxu</li> <li>• adres e-mail,</li> <li>• strona WWW</li> <li>• wysyłanie informacji e-mailem</li> <li>• urząd skarbowy</li> <li>• informacje o przetwarzaniu danych</li> <li>• prawo do emerytury lub renty</li> <li>• stopień niepełnosprawności</li> <li>• historia zatrudnienia</li> <li>• uprawnienia</li> <li>• kursy doskonalące</li> </ul>

		<ul style="list-style-type: none"> <li>• umiejętności</li> <li>• stan rodziny</li> <li>• dane osoby do kontaktu (imię, nazwisko, adres, telefon)</li> <li>• stosunek do służby wojskowej</li> <li>• wykształcenie</li> <li>• stopień awansu zawodowego</li> <li>• informacje o stanie zdrowia (zaświadczenia, orzeczenia lekarskie)</li> <li>• warunki zatrudnienia (umowy, aneksy)</li> <li>• wysokość wynagrodzenia</li> <li>• konto osobiste</li> <li>• staż pracy</li> <li>• awans zawodowy – staże</li> <li>• BHP (zaświadczenia)</li> <li>• nagrody, odznaczenia, kary, ocena pracy</li> <li>• upoważnienia</li> </ul>
PRACOWNICY	Karty ewidencji czasu pracy (roczne)	<ul style="list-style-type: none"> <li>• imię i nazwisko</li> <li>• pesel</li> <li>• stanowisko</li> <li>• czas pracy</li> </ul>
	Kartoteki urlopowe (roczne)	<ul style="list-style-type: none"> <li>• imię i nazwisko</li> <li>• PESEL</li> <li>• roczna statystyka urlopowa</li> <li>• lista urlopów</li> </ul>
	Wykazy pracowników objętych opieką socjalną (roczne)	<ul style="list-style-type: none"> <li>• imię i nazwisko</li> <li>• stanowisko</li> </ul>
	Karty ewidencji korzystania ze środków ZFŚS	<ul style="list-style-type: none"> <li>• imię i nazwisko</li> <li>• adres zamieszkania</li> <li>• stanowisko</li> <li>• data zatrudnienia/zwolnienia</li> <li>• rodzaj otrzymanego świadczenia</li> <li>• data przyznania świadczenia</li> <li>• wysokość świadczenia</li> <li>• suma świadczeń otrzymanych w danym roku</li> </ul>
	Kartoteki wynagrodzeń (roczne)	<ul style="list-style-type: none"> <li>• imię i nazwisko</li> <li>• PESEL</li> <li>• Stopień awansu</li> <li>• wysokość wynagrodzenia</li> </ul>
	ZAŚWIADCZENIA	<ul style="list-style-type: none"> <li>• PESEL</li> <li>• NIP</li> <li>• Imiona/nazwisko</li> <li>• Nazwisko rodowe</li> <li>• Data i miejsce urodzenia</li> <li>• Adres stały</li> <li>• Miejsce pracy</li> </ul>
	PROTOKOŁY POWYPADKOWE	<ul style="list-style-type: none"> <li>• Imiona i nazwisko</li> <li>• Nazwisko rodowe</li> <li>• Data i miejsce urodzenia</li> <li>• Adres stały</li> <li>• Informacje o stanie zdrowia</li> </ul>

	ARKUSZ ORGANIZACYJNY	<ul style="list-style-type: none"> <li>• Imiona i nazwisko</li> <li>• Staż pracy</li> <li>• Historia pracy</li> <li>• Tytuł zawodowy</li> <li>• Ukończone szkoły, kursy</li> <li>• Uzyskane kwalifikacje</li> <li>• Zawód wyuczony i zawód wykonywany</li> <li>• Warunki zatrudnienia</li> </ul>
	DOKUMENTACJA AWANSU ZAWODOWEGO NAUCZYCIELI	<ul style="list-style-type: none"> <li>• Imiona i nazwisko</li> <li>• Data i miejsce urodzenia</li> <li>• Adres zamieszkania</li> <li>• Wykształcenie</li> <li>• Historia pracy</li> <li>• Uzyskane kwalifikacje</li> </ul>
UCZNIOWIE	DOKUMENTACJA UCZNIÓW	<ul style="list-style-type: none"> <li>• PESEL</li> <li>• imię (imiona) i nazwisko</li> <li>• data i miejsce urodzenia</li> <li>• adres stały</li> <li>• adres tymczasowy</li> <li>• imiona i nazwiska rodziców (prawnych opiekunów)</li> <li>• numer legitymacji szkolnej</li> <li>• informacje o wynikach w nauce</li> <li>• karty zdrowia dziecka</li> <li>• numer telefonu rodziców</li> <li>• e-mail</li> <li>• adresy zamieszkania rodziców</li> </ul>
	DOKUMENTACJA UCZNIÓW	<ul style="list-style-type: none"> <li>• PESEL</li> <li>• imię (imiona) i nazwisko</li> <li>• data i miejsce urodzenia</li> <li>• adres stały</li> <li>• adres tymczasowy</li> <li>• imiona i nazwiska rodziców (prawnych opiekunów)</li> <li>• numer legitymacji szkolnej</li> <li>• informacje o wynikach w nauce</li> <li>• karty zdrowia dziecka</li> <li>• numer telefonu rodziców</li> <li>• e-mail</li> <li>• adresy zamieszkania rodziców</li> </ul>
	KSIĘGA UCZNIÓW	<ul style="list-style-type: none"> <li>• PESEL</li> <li>• imię (imiona) i nazwisko</li> <li>• data i miejsce urodzenia</li> <li>• adres stały</li> <li>• adres tymczasowy</li> <li>• imiona i nazwiska rodziców (prawnych opiekunów)</li> <li>• adresy rodziców (prawnych opiekunów)</li> </ul>
	ARKUSZE OCEN	<ul style="list-style-type: none"> <li>• PESEL</li> <li>• imię (imiona) i nazwisko</li> <li>• data i miejsce urodzenia</li> </ul>

		<ul style="list-style-type: none"> <li>• adres zamieszkania</li> <li>• imiona i nazwiska rodziców (prawnych opiekunów)</li> </ul>
	DZIENNIKI LEKCYJNE	<ul style="list-style-type: none"> <li>• PESEL</li> <li>• imię (imiona) i nazwisko</li> <li>• data i miejsce urodzenia</li> <li>• adres zamieszkania</li> <li>• imiona i nazwiska rodziców (prawnych opiekunów)</li> <li>• adresy i numery telefonów rodziców (prawnych opiekunów)</li> <li>• nieobecności w szkole</li> <li>• informacje o wynikach w nauce</li> </ul>
	KSIĘGA WYDANYCH LEGITYMACJI I LEGITYMACJE SZKOLNE	<ul style="list-style-type: none"> <li>• imię (imiona) i nazwisko</li> <li>• data i miejsce urodzenia</li> <li>• adres zamieszkania</li> <li>• numer legitymacji</li> </ul>
	REJESTR ZAŚWIADCZEŃ I ZAŚWIADCZENIA	<ul style="list-style-type: none"> <li>• imię (imiona) i nazwisko</li> <li>• data i miejsce urodzenia</li> <li>• adres zamieszkania</li> <li>• klasa</li> </ul>
	ŚWIADECTWA I DUPLIKATY	<ul style="list-style-type: none"> <li>• PESEL</li> <li>• imię (imiona) i nazwisko</li> <li>• data i miejsce urodzenia</li> </ul>
	DOKUMENTACJA UBEZPIECZENIOWA	<ul style="list-style-type: none"> <li>• PESEL</li> <li>• imię (imiona) i nazwisko</li> <li>• data i miejsce urodzenia</li> <li>• adres zamieszkania</li> </ul>
	PROTOKOŁY POWYPADKOWE	<ul style="list-style-type: none"> <li>• PESEL</li> <li>• imię (imiona) i nazwisko</li> <li>• data i miejsce urodzenia</li> <li>• adres zamieszkania</li> <li>• informacje o stanie zdrowia</li> </ul>
	KARTY BIBLIOTECZNE	<ul style="list-style-type: none"> <li>• imię (imiona) i nazwisko</li> <li>• data i miejsce urodzenia</li> <li>• adres zamieszkania</li> </ul>

#### I.4. System przetwarzania danych osobowych

##### § 5

W skład systemu wchodzi:

- dokumentacja papierowa (korespondencja, dokumenty pracowników i uczniów);
- wydruki komputerowe;
- urządzenia i oprogramowanie komputerowe służące do przetwarzania informacji;
- procedury przetwarzania danych w tym systemie, w tym procedury awaryjne.

#### Sposób przepływu danych pomiędzy poszczególnymi Systemami

System / Moduł „A”	System / Moduł „B”	Kierunek przepływu danych osobowych	Sposób przesyłania danych osobowych
Programy kadrowo			Programy

placowe Optivum Vulcan	Program Płatnik	Jednokierunkowo	jednostanowiskowe
Programy kadrowo placowe Optivum Vulcan	Program PFRON	Jednokierunkowo	Programy jednostanowiskowe
Programy pakietu Uczniowie Optivum Net Vulcan	Programy pakietu Uczniowie Optivum Net Vulcan	Dwukierunkowo	Dane przekazywane są automatycznie przez Internet miedzy poszczególnymi modułami
Programy pakietu Organizacja Optivum Vulcan	Sigma	Jednokierunkowo ze szkoły do organu prowadzącego	Manualnie: wydruki, płyta CD.
MOL Vulcan	brak	brak	Program jednostanowiskowy
PEFS	brak	Jednokierunkowo ze szkoły do Urzędu Marszałkowskiego	Program jednostanowiskowy, manualnie: wydruki , płyta CD zabezpieczone zamkniętymi kopertami

## I.5 Środki techniczne i organizacyjne stosowane w przetwarzaniu danych

### I.5.1 Cele i zasady funkcjonowania polityki bezpieczeństwa

#### § 6

Realizując Politykę Bezpieczeństwa informacji zapewnia ich:

- Poufność – informacja nie jest udostępniania lub ujawniana nieupoważnionym osobom, podmiotom i procesom,
- Integralność – dane nie zostaną zmienione lub zniszczone w sposób nieautoryzowany,
- Dostępność – istnieje możliwość wykorzystania ich na żądanie, w założonym czasie, przez autoryzowany podmiot,
- Rozliczalność – możliwość jednoznacznego przypisania działań poszczególnym osobom,
- Autentyczność – zapewnienie, że tożsamość podmiotu lub zasobu jest taka, jak deklarowana,
- Niezaprzeczalność – uczestnictwo w całości lub części wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie jest niepodważalne,
- niezawodność – zamierzone zachowania i skutki są spójne.

#### § 7

Polityka Bezpieczeństwa informacji w Gimnazjum im. ks. Wacława Rabczyńskiego w Wasilkowie ma na celu zredukowanie możliwości wystąpienia negatywnych konsekwencji naruszeń w tym zakresie, tj.:

1. naruszeń danych osobowych rozumianych jako prywatne dobro powierzone Szkole;
2. naruszeń przepisów prawa oraz innych regulacji;
3. utraty lub obniżenia reputacji Szkoły;

4. strat finansowych ponoszonych w wyniku nałożonych kar;
5. zakłóceń organizacji pracy spowodowanych nieprawidłowym działaniem systemów.

## § 8

Realizując Politykę Bezpieczeństwa w zakresie ochrony danych osobowych Szkoła dokłada szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności zapewnia, aby dane te były:

- przetwarzane zgodnie z prawem,
- zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnego z tymi celami,
- merytorycznie poprawne i adekwatne w stosunku do celu, w jakim są przetwarzane,
- przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej jednak niż jest to niezbędne do osiągnięcia celu przetwarzania.

### **I.5. 2 Kompetencje i odpowiedzialność w zarządzaniu bezpieczeństwem danych osobowych**

## § 9

Za przetwarzanie danych osobowych niezgodnie z prawem, z powierzonymi celami przetwarzania lub przechowywanie ich w sposób niezapewniający ochrony interesów osób, których te dane dotyczą, grozi odpowiedzialność karna wynikająca z przepisów ustawy o ochronie danych osobowych lub pracownicza na zasadach określonych w kodeksie pracy.

## § 10

Funkcję **Administradora Danych Osobowych (ADO)** sprawuje Dyrektor Szkoły.

Do zadań ADO należy:

- formułowanie i wdrażanie warunków technicznych i organizacyjnych służących ochronie danych osobowych, zabezpieczających dane przed dostępem osób nieupoważnionym, zabraniam przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem,
- podejmowanie decyzji o zakresie, celach oraz metodach przetwarzania i ochrony danych osobowych,
- ponoszenie odpowiedzialności za zgodne z prawem przetwarzanie danych osobowych w Szkole.
- ADO powołuje Administratora Bezpieczeństwa Informacji

## § 11

**Administratorem Bezpieczeństwa Informacji (ABI)** jest pracownik Szkoły wyznaczony przez Dyrektora. Do zadań ABI w szczególności należy:

- zarządzanie bezpieczeństwem przetwarzania danych osobowych w systemie informatycznym zgodnie z wymogami prawa i wskazówkami ADO
- doskonalenie i rozwijanie metod zabezpieczania danych przed zagrożeniami związanymi z ich przetwarzaniem,
- przydzielanie identyfikatorów użytkownikom systemu informatycznego oraz zaznajamianie ich z procedurami ustalania i zmiany haseł dostępu,
- nadzorowanie prac związanych z rozwojem, modyfikacją, serwisowaniem i konserwacją systemu,
- zapewnianie bezpieczeństwa zewnętrznego i wewnętrznego obiegu informacji w sieci i zabezpieczania łączy zewnętrznych,
- prowadzenie nadzoru nad archiwizacją zbiorów danych oraz zabezpieczanie elektroniczne nośników informacji zawierających dane osobowe.

## § 12

**Pracownikiem przetwarzającym dane (PPD)** jest każdy pracownik posiadający upoważnienie do przetwarzania danych osobowych i tym samym jest dopuszczony przez ADO do przetwarzania danych osobowych.

PPD ma obowiązek:

- znać zasady określone w Polityce Bezpieczeństwa i Instrukcji Zarządzania Systemem Informatycznym Szkoły i złożyć oświadczenie o znajomości tych przepisów.
- chronić prawo do prywatności osób fizycznych powierzających Szkole swoje dane osobowe, poprzez przetwarzanie ich zgodnie z przepisami prawa oraz zasadami określonymi w polityce bezpieczeństwa i Instrukcji Zarządzania Systemem informatycznym Szkoły,

### **I. 5. 3 Zasady udzielania dostępu do danych osobowych**

#### **§ 13**

Dostęp do danych osobowych może mieć wyłącznie osoba zaznajomiona z przepisami ustawy o ochronie danych osobowych oraz zasadami zawartymi w obowiązującej w Szkole Polityce Bezpieczeństwa i Instrukcji Zarządzania Systemem Informatycznym. Osoba zaznajomiona z zasadami ochrony danych potwierdza to w pisemnym oświadczeniu.

#### **§ 14**

Dostęp do danych osobowych może mieć wyłącznie osoba posiadająca pisemne oraz imienne upoważnienie wydane przez ADO.

### **I. 5. 4 Udostępnianie i powierzanie danych osobowych**

#### **§ 15**

Powierzenie danych może nastąpić wyłącznie na podstawie zgody osoby, której dane dotyczą. Rozumie się przez to oświadczenia woli, którego treścią jest zgoda na przetwarzanie danych osobowych. Zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści.

#### **§ 16**

Dane osobowe mogą być udostępnione osobom i podmiotom z mocy przepisów prawa lub jeżeli w sposób wiarygodny uzasadniają potrzebę ich posiadania, a ich udostępnienie nie naruszy praw i wolności osób, których one dotyczą.

#### **§ 17**

Udostępnienie danych może nastąpić na pisemny wniosek zawierający następujące elementy:

- określenie adresata wniosku (administrator danych),
- dane wnioskodawcy,
- podstawę prawną
- wskazanie przeznaczenia
- wskazanie zakresu informacji.

#### **§ 18**

Administrator odmawia udostępnienia danych jeśli spowodowałoby to naruszenie dóbr osobistych osób, których te dane dotyczą lub innych osób.

#### **§ 19**

Odbiór danych osobowych następuje w drodze pisemnej umowy, w której osoba przyjmująca dane zobowiązuje się do przestrzegania obowiązujących przepisów ustawy o ochronie danych osobowych. Umowa powinna zawierać informacje o podstawie prawnej powierzenia danych, celu i sposobie ich przetwarzania.

## § 20

1. Sprawy związane z udzielaniem informacji o zbiorze danych osobowych prowadzi ADO, udzielając informacji na piśmie.
2. Każda osoba fizyczna, której dane przetwarzane są w Szkole ma prawo do informacji, kontroli i poprawiania swoich danych osobowych, a także w przypadkach określonych w art.32 ust 1 pkt 7 i 8 ustawy o ochronie danych osobowych, prawo wniesienia umotywowanego żądania zaprzestania przetwarzania danych oraz sprzeciwu wobec przekazywania ich innym podmiotom.
3. Informacji o których mowa w punkcie 1 udziela się na wniosek osoby, której dane dotyczą. W imieniu Administratora danych, ABI jest zobowiązany w terminie 30 dni poinformować osobę o jej prawach i udzielić informacji na piśmie.

## § 21

W razie wskazania przez osobę, której dane osobowe dotyczą, że są one niekompletne, nieaktualne, nieprawdziwe, lub zostały zebrane z naruszeniem ustawy ADO bez zbędnej zwłoki dokonuje uzupełnienia, uaktualnienia, sprostowania danych, czasowego lub stałego wstrzymania przetwarzania kwestionowanych danych lub ich usunięcia ze zbioru i informuje o zaistniałym fakcie LADO.

### **I. 5. 5 Bezpieczeństwo w przetwarzaniu danych osobowych w formie tradycyjnej**

## § 22

Pomieszczenia, w których znajdują się przetwarzane zbiory danych osobowych pozostają zawsze pod bezpośrednim nadzorem upoważnionego do ich przetwarzania pracownika. Opuszczenie pomieszczenia, w którym znajdują się zbiory danych osobowych musi być poprzedzone przeniesieniem zbioru danych do odpowiednio zabezpieczonego miejsca. Przy nieobecności pracownika pomieszczenie powinno być bezwzględnie zamknięte na klucz.

## § 23

Klucze do szaf, w których przechowywane są dane osobowe mają jedynie pracownicy upoważnieni do przetwarzania danych osobowych w zakresie zgodnym z kategorią danych.

## § 24

Korzystanie ze zbiorów danych osobowych przez osoby niezatrudnione w Szkole jest dopuszczalne tylko w szczególnie uzasadnionych przypadkach, po uzyskaniu upoważnienia wydanego przez ADO /ABI w oparciu o ogólnie obowiązujące przepisy.

### **I. 5. 6 Bezpieczeństwo w przetwarzaniu danych osobowych w systemach informatycznych**

## § 25

Zasady bezpiecznego użytkownika systemu informatycznego zawarte są w *Instrukcji Zarządzania Systemem Informatycznym*, obligatoryjnej do zapoznania się i stosowania przez wszystkich użytkowników systemu informatycznego Szkoły.

## I. 6 Analiza ryzyka związanego z przetwarzaniem danych osobowych

### I. 6. 1 Identyfikacja zagrożeń

#### § 25

FORMA PRZETWARZANIA DANYCH	ZAGROŻENIA
Dane przetwarzane w sposób tradycyjny	<ul style="list-style-type: none"><li>- oszustwo, kradzież, sabotaż;</li><li>- zdarzenia losowe (powódź, pożar);</li><li>- zaniedbania pracowników szkoły (niedyskrecja, przypadkowe/celowe udostępnienie danych osobie nieupoważnionej);</li><li>- niekontrolowana obecność osób nieupoważnionych w obszarze przetwarzania danych;</li><li>- pokonanie zabezpieczeń fizycznych;</li><li>- podsłuchy, podglądy;</li><li>- atak terrorystyczny;</li><li>- brak rejestrowania udostępniania danych</li><li>- niewłaściwe miejsce i sposób przechowywania dokumentacji</li></ul>
Dane przetwarzane w systemach informatycznych	<ul style="list-style-type: none"><li>- wadliwe zarządzanie systemem identyfikatorów;</li><li>- niewłaściwa administracja systemem;</li><li>- niewłaściwa konfiguracja systemu;</li><li>- zniszczenie (sfalszowanie) kont użytkowników;</li><li>- kradzież danych kont;</li><li>- pokonanie zabezpieczeń programowych;</li><li>- zaniedbanie pracowników szkoły (niedyskrecja, udostępnianie danych osobom nieupoważnionym)</li><li>- niekontrolowana obecność nieuprawnionych osób</li><li>- zdarzenia losowe (powódź, pożar)</li><li>- niekontrolowane wytwarzanie i wypływ danych poza obszar przetwarzania za pomocą nośników informacji i komputerów przenośnych;</li><li>- naprawy i konserwacja systemu lub sieci teleinformatycznej wykonane przez osoby nieuprawnione;</li><li>- przypadkowe lub celowe uszkodzenie systemów i aplikacji informatycznych lub sieci;</li><li>- przypadkowe lub celowe wprowadzanie zmian do chronionych danych osobowych;</li><li>- brak rejestrowania zdarzeń, tworzenia lub modyfikowania danych</li></ul>

### I. 6. 2 Sposób zabezpieczenia danych

## § 26

FORMA PRZETWARZANIA DANYCH	STOSOWANE ŚRODKI OCHRONY
Dane przetwarzane w sposób tradycyjny	<ul style="list-style-type: none"> <li>- przechowywanie danych w zamykanych pomieszczeniach;</li> <li>- przechowywanie danych osobowych w szafach zamykanych na klucz;</li> <li>- przetwarzanie danych wyłącznie przez osoby upoważnione przez ADO</li> <li>- zapoznanie pracowników z zasadami przetwarzania danych osobowych oraz obsługą systemu służącego do ich przetwarzania</li> </ul>
Dane przetwarzane w systemach informatycznych	<ul style="list-style-type: none"> <li>- kontrola dostępu do systemów;</li> <li>- zastosowanie programów antywirusowych i innych regularnie aktualizowanych narzędzi ochrony;</li> <li>- stosowanie ochrony zasilania (UPS);</li> <li>- systematyczne tworzenie kopii zapasowych zbiorów danych przetwarzanych w systemach informatycznych;</li> <li>- składowanie danych sensytywnych oraz nośników wymiennych i nośników kopii zapasowych w odpowiednio zabezpieczonych szafach;</li> <li>- przydzielenie pracownikom indywidualnych kont użytkowników i haseł dostępu;</li> <li>- stosowanie indywidualnych haseł logowania do poszczególnych programów;</li> <li>- właściwa budowa hasła;</li> </ul>

### I. 6. 3 Określenie wielkości ryzyka

#### § 28

Poziom ryzyka naruszenia bezpieczeństwa danych jest niski. Zastosowane techniczne i organizacyjne środki ochrony są adekwatne do stwierdzonego poziomu ryzyka dla poszczególnych systemów, rodzajów zbiorów i kategorii danych osobowych.

### I. 6. 4 Identyfikacja obszarów wymagających szczególnych zabezpieczeń

#### § 29

Uwzględniając kategorie przetwarzanych danych oraz zagrożenia zidentyfikowane w wyniku przeprowadzonej analizy ryzyka dla systemów informatycznych stosuje się wysoki poziom bezpieczeństwa. ABI przeprowadza okresową analizę ryzyka dla poszczególnych systemów i na tej podstawie przedstawia ADO propozycje dotyczące zastosowania środków technicznych i organizacyjnych, celem zapewnienia właściwej ochrony przetwarzanym danym.

## **INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM**

### **II.1 Nadawanie i rejestrowanie uprawnień do przetwarzania danych w systemie informatycznym**

#### **§ 29**

Przetwarzać dane osobowe w systemach informatycznych może wyłącznie osoba posiadająca pisemne upoważnienie do przetwarzania danych osobowych w Szkole.

#### **§ 30**

Za tworzenie, modyfikację i nadawanie uprawnień kontom użytkowników odpowiada ABI.

#### **§ 31**

ABI nadaje uprawnienia w systemie informatycznym na podstawie upoważnienia nadanego pracownikowi przez ADO.

#### **§ 32**

Usuwanie kont stosowane jest wyłącznie w uzasadnionych przypadkach, standardowo, przy ustalaniu potrzeby utrzymywania konta danego użytkownika ulega ono dezaktywacji w celu zachowania historii jego aktywności.

#### **§ 33**

Osoby dopuszczone do przetwarzania danych osobowych zobowiązane są do zachowania tajemnicy w zakresie tych danych oraz sposobów ich zabezpieczania. Obowiązek ten istnieje również po ustaniu stosunku pracy.

Ustanie stosunku pracy jest równoznaczne z cofnięciem uprawnień do przetwarzania danych osobowych.

### **II. 2 Zabezpieczenie danych w systemie informatycznym**

#### **§ 34**

Ochronę przed awariami zasilania oraz zakłóceniami w energii elektrycznej stacji roboczych, na których przetwarzane są dane osobowe zapewniają zasilacze UPS.

#### **§ 35**

Oprogramowanie wykorzystywane do przetwarzania danych posiada własny system kont (zabezpieczonych hasłami) i uprawnień.

#### **§ 36**

Hasła do systemu stacji roboczych mają długość przynajmniej 8 znaków (duże i małe litery oraz znaki cyfry lub znaki specjalne) i okres ważności ustawiony na nie dłużej niż 1 miesiąc. Hasło nie może być zapisywane i przechowywane w miejscu dostępnym dla osób nieuprawnionych.

### § 37

W przypadku utraty hasła użytkownik ma obowiązek skontaktować się z ABI celem uzyskania nowego hasła.

### § 38

Hasła użytkowników uprzywilejowanych, posiadających uprawnienia na poziomie administratorów systemów informatycznych objęte są takimi samymi restrykcjami dotyczącymi ich poufności jak pozostałe hasła.

### § 39

System informatyczny przetwarzający dane osobowe musi posiadać mechanizmy pozwalające na odnotowaniu faktu wykonania operacji na danych. W szczególności zapis ten powinien obejmować:

- rozpoczęcie i zakończenie pracy przez użytkownika systemu,
- operacje wykonywane na przetwarzanych danych,
- przesyłanie za pośrednictwem systemu danych osobowych przetwarzanych w systemie informatycznym innym podmiotom, nie będącym właścicielami ani współwłaścicielami systemu,
- nieudane próby dostępu do systemu informatycznego przetwarzającego dane osobowe oraz nieudane próby wykonania operacji na danych osobowych,
- błędy w działaniu systemu informatycznego podczas pracy danego użytkownika.

### § 40

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

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

### § 41

System antywirusowy zainstalowany jest na każdym komputerze z dostępem do danych osobowych. Programy antywirusowe, winny być uaktywnione cały czas podczas pracy danego systemu, zaś wszystkie pliki otrzymywane z zewnątrz, jak również wysyłane na zewnątrz, należy sprawdzać pod kątem występowania wirusów zaktualizowaną wersją programu antywirusowego. Sprawdzenie odbywa się automatycznie przez system antywirusowy lub ręcznie przez użytkowników.

W przypadku stwierdzenia pojawienia się wirusa, każdy użytkownik winien powiadomić ABI

## **II. 3 Zasady bezpieczeństwa podczas pracy w systemie informatycznym**

### § 42

W celu rozpoczęcia pracy w systemie informatycznym użytkownik:

- 1) loguje się do systemu operacyjnego przy pomocy identyfikatora i hasła
- 2) loguje się do programów i systemów wymagających dodatkowego wprowadzania unikalnego identyfikatora i hasła.

### § 43

W sytuacji tymczasowego zaprzestania pracy na skutek nieobecności przy stanowisku komputerowym należy uniemożliwić osobom postronnym korzystanie z systemu informatycznego poprzez wylogowanie się z systemu lub uruchomienie wygaszacza ekranu chronionego hasłem.

### § 44

W sytuacji gdy wgląd w wyświetlane na monitorze dane może mieć osoba nieuprawniona należy tymczasowo zmienić widok wyświetlany na monitorze lub obrócić monitor (przymknąć ekran komputera przenośnego) w sposób uniemożliwiający wgląd w wyświetlaną treść.

### § 45

Użytkownik wyrejestrowuje się z systemu informatycznego przed wyłączeniem stacji komputerowej poprzez zamknięcie programu przetwarzającego dane oraz wylogowanie się z systemu operacyjnego.

### § 46

Zawieszenie korzystania z systemu informatycznego może nastąpić losowo wskutek awarii lub planowo (np. w celu konserwacji sprzętu). Planowe zawieszenie prac jest poprzedzone poinformowaniem pracowników Szkoły przez ABI na co najmniej 30 minut przed planowanym zawieszeniem.

### § 47

Pracownik korzystający z systemu informatycznego zobowiązany jest do powiadomienia ABI w razie:

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

Na fakt naruszenia zabezpieczeń systemów mogą wskazywać:

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

## II. 4 Tworzenie kopii zapasowych

### § 48

Dane systemów kopiowane są w trybie semestralnym (kopie baz danych). Kopie awaryjne danych zapisywanych w programach wykonane są semestralnie.

### § 49

Odpowiedzialnym za wykonanie kopii danych i kopii awaryjnych jest pracownik obsługujący dany program przetwarzające dane.

### § 50

Dodatkowe kopie wynikające np. ze zmiany platformy sprzętowej i kopie awaryjne przechowywane są w Kancelarii Szkoły. Osobą odpowiedzialną za wymianę kopii awaryjnych na aktualne jest ABI.

#### **§ 51**

Okresową weryfikację kopii bezpieczeństwa pod kątem ich przydatności do odtworzenia danych przeprowadza ABI.

#### **§ 52**

Usuwanie kopii danych następuje poprzez bezpieczne kasowanie. Nośniki tych danych, na których zapisywane są kopie bezpieczeństwa niszczy się na trwale w sposób mechaniczny.

### **II. 5 Udostępnienie danych**

#### **§ 53**

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

Administrator danych może powierzyć innemu podmiotowi przetwarzanie danych tylko i wyłącznie w drodze umowy zawartej na piśmie, określającej zakres i cel przetwarzania danych.

Podmiot zewnętrzny ponosi odpowiedzialność za szkody będące następstwem jego zachowań związanych z niezgodnym z umową przetwarzaniem danych osobowych, niewłaściwym przechowywaniem lub posłużeniem się dokumentami, które są nośnikiem danych osobowych.

Administrator Bezpieczeństwa Informacji prowadzi rejestr podmiotów zewnętrznych posiadających dostęp do systemu informatycznego Szkoły i danych osobowych celem identyfikacji i zapewnienia nadzoru nad bezpiecznym ich przetwarzaniem.

### **II. 6 Przeglądy i konserwacje systemów**

#### **§ 54**

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

#### **§ 55**

Prace wymienione w § 54 powinny uwzględniać wymagany poziom zabezpieczenia tych danych przed dostępem do nich osób nieupoważnionych.

#### **§ 56**

Przed rozpoczęciem prac wymienionych w § 54 przez osoby nie będące pracownikami Szkoły należy dokonać potwierdzenia tożsamości tychże osób.

### **II. 7 Niszczenie wydruków i nośników danych**

#### **§ 57**

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

## **§ 58**

Niszczenie zapisów na nośnikach danych powinno odbywać się poprzez wymazywanie informacji oraz formatowanie nośnika.

## **§ 59**

Uszkodzone nośniki danych przed ich wyrzuceniem należy fizycznie zniszczyć w niszczarce.

# **INSTRUKCJA POSTĘPOWANIA W SYTUACJI NARUSZENIA DANYCH**

## **III. 1 Istota naruszenia danych osobowych**

### **§ 60**

Naruszeniem danych osobowych jest każdy stwierdzony fakt nieuprawnionego ujawnienia danych osobowych, udostępnienia lub umożliwienia dostępu do nich osobom nieupoważnionym, zabrania danych przez osobę nieupoważnioną, uszkodzenia jakiegokolwiek elementu systemu informatycznego, a w szczególności:

- nieautoryzowany dostęp do danych,
- nieautoryzowane modyfikacje lub zniszczenie danych,
- udostępnienie danych nieautoryzowanym podmiotom,
- nielegalne ujawnienie danych,
- pozyskiwanie danych z nielegalnych źródeł

## **III. 2 Postępowanie w przypadkach naruszenia danych osobowych**

### **§ 61**

Każdy pracownik Szkoły, który stwierdzi fakt naruszenia bezpieczeństwa danych przez osobę przetwarzającą dane osobowe, bądź posiada informacje mogąca mieć wpływ na bezpieczeństwo danych osobowych jest zobowiązany zgłosić to niezwłocznie do ABI lub ADO.

### **§ 62**

W przypadku stwierdzenia naruszenia bezpieczeństwa danych należy zaniechać wszelkich działań mogących utrudnić analizę wystąpienia naruszenia i udokumentowania zdarzenia oraz nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia ABI.

### **§ 64**

ABI podejmuje następujące kroki:

- zapoznaje się z zaistniałą sytuacją i wybiera sposób dalszego postępowania po dokładnej analizie relacji z zaistniałego naruszenia, uwzględniając zagrożenie w prawidłowości pracy Szkoły,
- wdraża stosowne środki administracyjne, techniczne i fizyczne w celu zabezpieczenia zasobów technicznych.
- Identyfikuje źródło naruszenia
- rozważa celowość i potrzebę powiadomienia o zaistniałym naruszeniu ADO,
- nawiązuje kontakt ze specjalistami spoza Szkoły (jeśli zachodzi taka potrzeba)

### **§ 65**

ABI dokumentuje zaistniały przypadek naruszenia bezpieczeństwa danych osobowych sporządzając raport i przekazuje go ADO.

#### **§ 66**

ABI zasięga potrzebnych mu opinii i proponuje działania naprawcze (w tym także ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń oraz terminu wznowienia przetwarzania danych osobowych).

### **III. 3 Sankcje karne**

#### **§ 67**

Wobec osoby, która w przypadku naruszenia ochrony danych osobowych nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami wszczyna się postępowanie dyscyplinarne.

#### **§ 68**

Kara dyscyplinarna, wobec osoby uchylającej się od powiadomienia o naruszeniu danych osobowych nie wyklucza odpowiedzialności karnej tej osoby zgodnie z ustawą o ochronie danych osobowych.

#### **Załączniki:**

**Załącznik nr 1 – Upoważnienie do przetwarzania danych osobowych**

**Załącznik nr 2 – Rejestr osób upoważnionych do przetwarzania danych osobowych**

**Załącznik nr 3 – Oświadczenie pracownika o zapoznaniu się z zasadami zachowania bezpieczeństwa danych osobowych**

**Załącznik nr 4 – Informacja o zawartości zbioru danych**

**Załącznik nr 5 – Raport z naruszenia bezpieczeństwa danych osobowych**

Wasilków, dnia ..... 201...r.

.....  
(pieczęć szkoły)

**UPOWAŻNIENIE nr ...../201....  
do przetwarzania danych osobowych  
w Gimnazjum im. Ks. W. Rabczyńskiego w Wasilkowie**

Na podstawie art.37 ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz.U. z 2002r. Nr 10 poz.926 z późn.zm.) upoważniam Panią/Pana

.....  
Zatrudnioną/zatrudnionego w Gimnazjum im. Ks. W Rabczyńskiego w Wasilkowie na stanowisku ..... do przetwarzania danych osobowych zgromadzonych w formie tradycyjnej oraz w systemach informatycznych w Gimnazjum im. ks. W Rabczyńskiego w Wasilkowie w zakresie określonym w obowiązkach służbowych.

Upoważnienie obowiązuje do .....  
Wyżej wymieniona osoba została wpisana do ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych w Gimnazjum im. Ks. W Rabczyńskiego w Wasilkowie.

.....  
(podpis Administratora Danych Osobowych)



Wasilków, dnia ..... 20.....r.

.....  
(imię i nazwisko)

.....  
(stanowisko)

**OŚWIADCZENIE O ZAPOZNANIU SIĘ Z PRZEPISAMI PBI  
OBOWIĄZUJĄCYMI  
W GIMNAZJUM IM. KS. W RABCZYŃSKIEGO W WASILKOWIE  
ORAZ ZACHOWANIU POUFNOŚCI**

Ja niżej podpisany/a oświadczam, że zobowiązuję się do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia, do których mam lub będę miał/a dostęp w związku z wykonywaniem zadań i obowiązków służbowych wynikających ze stosunku pracy, zarówno w czasie trwania umowy, jak i po jej ustaniu. Oświadczam, że zostałem/am poinformowany/a o obowiązujących w Gimnazjum zasadach dotyczących przetwarzania danych osobowych określonych w *Polityce Bezpieczeństwa Informacji w Gimnazjum im. Ks. W Rabczyńskiego w Wasilkowie* i zobowiązuję się ich przestrzegać.

Zostałem/am zapoznany/a z przepisami Ustawy o ochronie danych osobowych (Dz.U. 2002r. Nr 101 poz.926 z późn.zm.) oraz Rozporządzenia MSWiA w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakimi powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. z 2004r. Nr 100 poz. 1024). Poinformowano mnie również o grożącej stosownie do przepisów rozdziału 8 Ustawy o ochronie danych osobowych odpowiedzialności karnej. Niezależnie od odpowiedzialności przewidzianej w wymienionych przepisach, mam świadomość, że złamanie zasad ochrony danych osobowych, obowiązujących w Gimnazjum im. ks. W. Rabczyńskiego w Wasilkowie może zostać uznane za ciężkie naruszenie podstawowych obowiązków pracowniczych i skutkować odpowiedzialnością dyscyplinarną.

.....  
(podpis pracownika)

Wasilków, dn.....20.....r.

.....  
*pieczęć szkoły*

.....  
*imię i nazwisko*

.....  
*adres*

### INFORMACJA O ZAWARTOŚCI ZBIORU DANYCH OSOBOWYCH

W związku z Pani/Pana wnioskiem z dnia ..... r. o udzielenie informacji związanych z przetwarzaniem danych osobowych w Gimnazjum im. Ks. W Rabczyńskiego w Wasilkowie działając na podstawie art. 33 ust. 1 Ustawy o ochronie danych osobowych informuję, że zbiór danych zawiera następujące Pani/Pana dane osobowe:

.....  
Powyższe dane przetwarzane są w Gimnazjum im. Ks. W Rabczyńskiego w Wasilkowie w celu

..... z zachowaniem

wymaganych zabezpieczeń i zostały uzyskane .....

*(podać sposób).*

Powyższe dane nie były/były udostępniane .....

*(podać komu)*

w celu .....

*(podać cel przekazania danych).*

Zgodnie z rozdziałem 4 Ustawy o ochronie danych osobowych przysługuje Pani/Panu prawo do kontroli danych osobowych, prawo ich poprawiania, a także w przypadkach określonych w art. 32 ust. 1 pkt 7 i 8 Ustawy, prawo wniesienia umotywowanego żądania zaprzestania przetwarzania danych oraz prawo sprzeciwu wobec przetwarzania danych w celach marketingowych lub wobec przekazywania danych innemu administratorowi danych osobowych.

.....  
(podpis Administratora Bezpieczeństwa Informacji )

Wasilków, dn.....20.....r.

.....  
*pieczęć szkoły*

## **RAPORT Z NARUSZENIA BEZPIECZEŃSTWA DANYCH OSOBOWYCH W GIMNAZJUM IM. KS. W RABCZYŃSKIEGO W WASILKOWIE**

1. Data: ..... r. Godzina: .....

2. Osoba powiadamiająca o zaistniałym zdarzeniu:

.....  
*(imię, nazwisko, stanowisko służbowe, nazwa użytkownika - jeśli występuje)*

3. Lokalizacja zdarzenia:

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

4. Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące:

.....  
5. Przyczyny wystąpienia zdarzenia:

.....  
6. Podjęte działania:

.....  
7. Postępowanie wyjaśniające:

.....  
*(podpis Administratora Bezpieczeństwa Info*