

ZARZĄDZENIE Nr 6 / 2015

Dyrektora Zespołu Szkół Ekonomiczno – Hotelarskich im. E. Gierczak w Kołobrzegu z dnia
15 kwietnia 2015 roku

w sprawie: wprowadzenia Polityki Bezpieczeństwa Informacji.

Na podstawie art. 36 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U.z 2002 r. Nr 101, poz. 926 ze zmianami) oraz § 3 i 4 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. z 2004 r. Nr 100, poz. 1024).

§ 1

Wprowadzam w Zespole Szkół Ekonomiczno – Hotelarskich im. Emilii Gierczak w Kołobrzegu Politykę Bezpieczeństwa Informacji , której treść stanowi załącznik nr 1 do zarządzenia.

§ 2

Każdy pracownik, zgodnie z wykazem, jest obowiązany zapoznać się z treścią załącznika nr 1.

§ 3

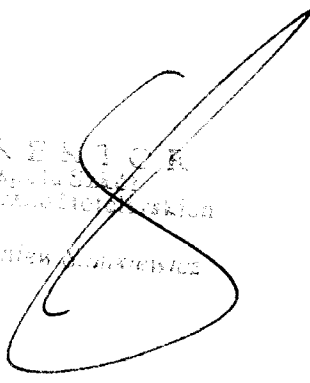
Oświadczenie o zapoznaniu się z treścią Polityki Bezpieczeństwa Informacji zaopatrzone w podpis pracownika i datę, dołącza się do akt osobowych. Wzór oświadczenia stanowi załącznik nr 4 Polityki Bezpieczeństwa Informacji.

§ 4

Pracodawca zobowiązuje wszystkich pracowników do przestrzegania Polityki Bezpieczeństwa Informacji oraz stosowania w pracy Instrukcji pod groźbą konsekwencji służbowych, przewidzianych prawem.

§ 5

Zarządzenie wchodzi w życie z dniem 15 kwietnia 2015 roku


Dyrektor
Zespołu Szkół Ekonomiczno-Hotelarskich
im. Emilii Gierczak w Kołobrzegu

Polityka Bezpieczeństwa Informacji

**w Zespole Szkół Ekonomiczno - Hotelarskich
im. Emilii Gierczak
w Kołobrzegu**

SPIS TREŚCI

Podstawa prawna.....	3
Wstęp.....	4
Podstawowe pojęcia.....	5
I. POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH	
I.1 Wykaz miejsc w których przetwarzane są dane.....	7
I.2 Zbiory danych przetwarzanych w systemach informatycznych.....	11
I.2.1 Programy informatyczne służące do przetwarzania danych osobowych.....	13
I.3 Zbiory danych przetwarzanych tradycyjnie.....	13
I.4 System przetwarzania danych osobowych.....	14
I.5 Środki techniczne i organizacyjne stosowane w przetwarzaniu danych.....	16
I.5.1 Cele i zasady funkcjonowania polityki bezpieczeństwa.....	16
I.5.2 Kompetencje i odpowiedzialność w zarządzaniu bezpieczeństwem danych osobowych.....	16
I.5.3 Zasady udzielania dostępu do danych osobowych.....	18
I.5.4 Udostępnianie i powierzanie danych osobowych.....	18
I.5.5 Bezpieczeństwo w przetwarzaniu danych osobowych w formie tradycyjnej.....	19
I.5.6 Bezpieczeństwo w przetwarzaniu danych osobowych w systemach Informatycznych.....	20
I.6 Analiza ryzyka związanego z przetwarzaniem danych osobowych.....	20
I.6.1 Identyfikacja zagrożeń.....	20
I.6.2 Sposób zabezpieczenia danych.....	21
I.6.3 Określenie wielkości ryzyka.....	22
I.6.4 Identyfikacja obszarów wymagających szczególnych zabezpieczeń ryzyka.....	22
II. INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM	
II.1 Nadawanie i rejestrowanie uprawnień do przetwarzania danych w systemie informatycznym.....	23
II.2 Zabezpieczenie danych w systemie informatycznym.....	23
II.3 Zasady bezpieczeństwa podczas pracy w systemie informatycznym.....	24
II.4 Tworzenie kopii zapasowych.....	25
II.5 Udostępnienie danych.....	25
II.6 Przeglądy i konserwacje systemów.....	26
II.7 Niszczenie wydruków i nośników danych.....	26
III. INSTRUKCJA POSTĘPOWANIA W SYTUACJI NARUSZENIA DANYCH	
III.1 Istota naruszenia danych osobowych.....	27
III.2 Postępowanie w przypadku naruszenia danych osobowych.....	27
III.3 Sankcje karne.....	28
ZAŁĄCZNIKI:	
nr 1 – upoważnienie do przetwarzania danych osobowych.....	29
nr 2 – odwołanie upoważnienia do przetwarzania danych osobowych.....	30
nr 3 – rejestr osób upoważnionych do przetwarzania danych osobowych.....	31
nr 4 – oświadczenie o zachowaniu poufności i zapoznaniu się z przepisami.....	32
nr 5 – informacja o zawartości zbioru danych osobistych.....	33
nr 6 – tabela form naruszeń danych osobistych.....	34
nr 7 – raport o naruszeniu danych osobowych.....	37

Podstawa prawna

1. Konstytucja Rzeczypospolitej Polskiej (art. 47 i 51 Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. Dz.U. 1997 nr 78 poz. 483).
2. Ustawa o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (Dz. U. z 2002 r. nr 101 poz. 926 z późn. zm.).
3. 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 z późn. zm.).
4. Konwencja nr 108 Rady Europy – dotycząca ochrony osób w związku z automatycznym przetwarzaniem danych osobowych.
5. Dyrektywa PE i RE z dnia 24 października 1995 r. (95/46/EC) w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych.
6. Ustawa z dnia 26 czerwca 1974 r. – Kodeks pracy (Dz. U. 1974 nr 24 poz. 141 z późn. zm.).

Wstęp

Cele i zasady funkcjonowania "Polityki bezpieczeństwa informacji"

Realizując Politykę bezpieczeństwa informacji zapewnia się ich:

- ✓ poufność – informacja nie jest udostępniana lub ujawniana nieupoważnionym osobom, podmiotom i procesom,
- ✓ integralność – dane nie zostają zmienione lub zniszczone w sposób nie autoryzowany,
- ✓ 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.

Polityka bezpieczeństwa informacji w Szkole ma na celu zredukowanie możliwości wystąpienia negatywnych konsekwencji naruszeń w tym zakresie, tj.:

- ✓ naruszeń danych osobowych rozumianych jako prywatne dobro powierzone Szkole;
- ✓ naruszeń przepisów prawa oraz innych regulacji;
- ✓ utraty lub obniżenia reputacji Szkoły;
- ✓ strat finansowych ponoszonych w wyniku nałożonych kar;
- ✓ zakłóceń organizacji pracy spowodowanych nieprawidłowym działaniem systemów.

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

- ✓ przetwarzane zgodnie z prawem,
- ✓ zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu 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 niż jest to niezbędne do osiągnięcia celu przetwarzania.

Szkoła – w tym dokumencie jest rozumiana, jako Zespół Szkół Ekonomiczno – Hotelarskich im. Emilii Gierczak w Kołobrzegu ul. Łopuskiego 13 wraz z warsztatami szkolnymi CKP w Kołobrzegu ul. Katedralna 12 zwanym dalej ZSE-H w Kołobrzegu

Polityka – w tym dokumencie jest rozumiana jako „Polityka bezpieczeństwa informacji” obowiązująca w Zespole Szkół Ekonomiczno – Hotelarskich im. Emilii Gierczak w Kołobrzegu ul. Łopuskiego 13 wraz z warsztatami szkolnymi CKP w Kołobrzegu ul. Katedralna 12

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.

Instrukcja – w tym dokumencie rozumiana jest jako „Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Zespole Szkół Ekonomiczno – Hotelarskich w Kołobrzegu”.

Administrator Danych Osobowych (ADO) – dyrektor Zespołu Szkół Ekonomiczno – Hotelarskich w Kołobrzegu

Administrator Bezpieczeństwa Informacji (ABI) – pracownik szkoły wyznaczony przez Administratora Danych Osobowych (Dyrektora) do nadzorowania przestrzegania zasad ochrony danych osobowych, oraz przygotowania dokumentów wymaganych przez przepisy ustawy o ochronie danych osobowych w Zespole Szkół Ekonomiczno – Hotelarskich w Kołobrzegu. ABI powołany jest zarządzeniem Dyrektora Zespołu Szkół Ekonomiczno – Hotelarskich w Kołobrzegu.

Administrator Systemu Informatycznego (ASI) – pracownik odpowiedzialny za funkcjonowanie systemu teleinformatycznego, oraz stosowanie technicznych i organizacyjnych środków ochrony stosowanych w tym systemie

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.

Identyfikator użytkownika (login) – jest to ciąg znaków jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.

System informatyczny – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

Przetwarzanie danych – rozumie się to w tym dokumencie, jako jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie.

Zabezpieczenie danych w systemie informatycznym – wdrożenie i wykorzystywanie stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem.

Wysoki poziom bezpieczeństwa – musi występować wtedy, gdy przynajmniej jedno urządzenie systemu informatycznego, służące do przetwarzania danych osobowych, połączone jest z siecią publiczną.

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 własność zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom

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 2000 r. - 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 2000 r. – Prawo telekomunikacyjne (Dz. U. nr 73, poz.852 z późn. zm.).

POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

I.1 Wykaz miejsc, w których przetwarzane są dane osobowe

§ 2

W szkole dane osobowe przetwarzane są:

A. budynek nr 1 – ul. Łopuskiego 13, 78 – 100 Kołobrzeg

L.p.	Miejsce przechowywania danych / zabezpieczenie	Zbiory lub opis przechowywanych danych osobowych	Sposób przetwarzania i gromadzenia	Osoba/osoby odpowiedzialna
1	Gabinet Dyrektora Szkoły Kluczami dysponuje Dyrektor Szkoły, sekretarka szkoły, klucze deponowane są na recepcji szkoły	Dokumentacja związana z nadzorem pedagogicznym	Tradycyjna	Dyrektor szkoły
		Listy obecności nauczycieli na posiedzeniach rad pedagogicznych	Tradycyjna	Dyrektor szkoły
		Protokoły rad pedagogicznych	Tradycyjna	Dyrektor szkoły
		Dokumenty związane z dyscypliną pracy nauczyciela	Tradycyjna	Dyrektor szkoły
2	Gabinet Vicedyrektora ds. szkolnictwa zawodowego Kluczami dysponuje Vicedyrektor ds. szkolnictwa zawodowego, sekretarka szkoły, klucze deponowane są na recepcji szkoły	Arkusze organizacyjne	Tradycyjna / elektroniczna	Vicedyrektor Szkoły
		Dokumentacja związana z funduszami europejskimi	Tradycyjna / elektroniczna	Vicedyrektor Szkoły
		Dokumentacja związana z egzaminami potwierdzającymi kwalifikacje zawodowe	Tradycyjna / elektroniczna	Vicedyrektor Szkoły
		Dokumentacja współpracy szkoły instytucjami w kraju i zagranicą	Tradycyjna / elektroniczna	Vicedyrektor Szkoły
		Rejestr i dokumentacja dotycząca próbnych egzaminów potwierdzających kwalifikacje zawodowe	Tradycyjna / elektroniczna	Vicedyrektor Szkoły
3	Gabinet Vicedyrektora ds. dydaktyczno - wychowawczych Kluczami dysponuje Vicedyrektor ds. dydaktyczno - wychowawczych, klucze deponowane są na recepcji szkoły	Arkusze organizacyjne	Tradycyjna / elektroniczna	Vicedyrektor Szkoły
		Zestawienia wyników klasyfikacji	Tradycyjna / elektroniczna	Vicedyrektor Szkoły
		Rejestr przystępujących do matury i dokumentacja związana z egzaminami maturalnymi	Tradycyjna / elektroniczna	Vicedyrektor Szkoły
		Dokumentacja organizacji procesu dydaktycznego	Tradycyjna / elektroniczna	Vicedyrektor Szkoły
		Zestawienie rozliczeń godzin dodatkowych nauczycieli	Tradycyjna	Vicedyrektor Szkoły
		Rejestr zastępstw nauczycieli	Tradycyjna / elektroniczna	Vicedyrektor Szkoły
		Dokumentacja związana z organizacją egzaminów poprawkowych i klasyfikacyjnych	Tradycyjna / elektroniczna	Vicedyrektor Szkoły
		Rejestr i dokumentacja dotycząca próbnych egzaminów maturalnych	Tradycyjna	Vicedyrektor Szkoły
		Plan zajęć szkolnych	Tradycyjna / elektroniczna	Vicedyrektor Szkoły
4	Kancelaria szkoły Kluczami dysponuje inspektor ds.	Rejestr korespondencji przychodzącej i wychodzącej	Tradycyjna / elektroniczna	Inspektor ds. kancelarii

	kancelarii szkoły, Dyrektor szkoły, Vicedyrektor ds. szkolnictwa zawodowego, sekretarka szkoły, klucze deponowane są na recepcji szkoły	Dokumentacja wycieczek szkolnych oraz wyjść klas po za teren szkoły	Tradycyjna	Inspektor ds. kancelarii
		Księga uchwał	Tradycyjna	Inspektor ds. Kancelarii
		Rejestr delegacji służbowych	Tradycyjna	Inspektor ds. kancelarii
		Ewidencja wydanych zwolnień uczniów z przedmiotów	Tradycyjna	Inspektor ds. kancelarii
		Ewidencja osób upoważnionych do przetwarzania danych osobowych	Tradycyjna	ABI
		Zgłoszenia uczestników konkursów międzyszkolnych	Tradycyjna / elektroniczna	Inspektor ds. kancelarii
		Arkusze organizacyjne	Tradycyjna / elektroniczna	Dyrektor szkoły
		Aktualne listy uczniów w klasach na wypadek ewakuacji szkoły	Tradycyjna	Inspektor ds. kancelarii
5	Biblioteka Kluczami dysponują pracownicy biblioteki, klucze deponowane są na recepcji szkoły	Ewidencja uczniów i pracowników korzystających z biblioteki	Tradycyjna/ elektroniczna	Bibliotekarze
6	Sekretariat ds. uczniów i słuchaczy Kluczami dysponuje sekretarz szkoły, kierownik praktyk zawodowych, klucze deponowane są na recepcji szkoły	Ewidencja uczniów	Tradycyjna	Inspektor ds. uczniowskich
		Dokumentacja rekrutacyjna uczniów	Tradycyjna / elektroniczna	Inspektor ds. uczniowskich
		Arkusze ocen	Tradycyjna	Inspektor ds. uczniowskich
		Teczki z aktami osobowymi uczniów	Tradycyjna	Inspektor ds. uczniowskich
		Ewidencja wydanych legitymacji	Tradycyjna	Inspektor ds. uczniowskich
		Ewidencja wydanych świadectw ukończenia szkoły	Tradycyjna	Inspektor ds. uczniowskich
		Rejestr dokumentów zarchiwizowanych	Tradycyjna	Inspektor ds. uczniowskich
		Listy uczniów w klasach na wypadek ewakuacji	Tradycyjna	Inspektor ds. uczniowskich
		Ewidencja wydanych zaświadczeń	Tradycyjna	Inspektor ds. uczniowskich
		Ewidencja zasobów szkoły System Informacji Oświatowej	Elektroniczna	Inspektor ds. uczniowskich
		Rejestr uczniów odbywających praktyki zawodowe z dokumentacją	Tradycyjna	Kierownik praktyk zawodowych
		Księga akt osobowych pracowników	Tradycyjna / elektroniczna	Specjalista ds. kadr
7	Pokój działu Kadr ds. Szkół i ds. CKP Kluczami dysponują referent ds. kadrowych i referent ds. BHP, klucze deponowane są na recepcji szkolnej	Listy obecności pracowników	Tradycyjna	Specjalista ds. kadr
		Rejestr pism jednolity rzeczowy dziesiętny wykaz akt	Tradycyjna	Specjalista ds. kadr
		Rejestr skarg	Tradycyjna	Specjalista ds. kadr
		Rejestr nagród Dyrektora	Tradycyjna	Specjalista ds. kadr
		Wykaz etatów pracowniczych	Tradycyjna / elektroniczna	Specjalista ds. kadr
		Wykaz dodatków motywacyjnych i premii	Tradycyjna	Specjalista ds. kadr
		Rejestr zawartych umów cywilno – prawnych	Tradycyjna	Specjalista ds. kadr
		Ewidencja zwolnień lekarskich	Tradycyjna	Specjalista ds. kadr

		Rejestr wypadków pracowniczych i dokumentacja powypadkowa	Tradycyjna / elektroniczna	Inspektor ds. BHP
		Rejestr ważności okresowych badań lekarskich	Tradycyjna	Referent ds. kadr
		Rejestr wypadków uczniowskich	Tradycyjna	Inspektor ds. BHP
		Rejestr ważności szkoleń BHP	Tradycyjna / elektroniczna	Inspektor ds. BHP
8	Gabinet pielęgniarki Kluczami dysponuje pielęgniarka, klucz deponowany jest na recepcji	Karty zdrowia uczniów	Tradycyjna	Pielęgniarka
		Rejestr wizyt i porad	Tradycyjna	Pielęgniarka
9	Pokój działu finansów ds. Szkół i ds. CKP Kluczami dysponują pracownicy działu finansów, klucze deponowane są na recepcji szkoły	Listy płac	Tradycyjna / elektroniczna	Pracownicy działu finansów
		Kartoteki wynagrodzeń pracowniczych	Tradycyjna / elektroniczna	Pracownicy działu finansów
		Deklaracje i kartoteki ZUS pracowników	Tradycyjna / elektroniczna	Pracownicy działu finansów
		Przelewy i faktury	Tradycyjna / elektroniczna	Pracownicy działu finansów
		Oświadczenia podatkowe pracowników	Tradycyjna / elektroniczna	Pracownicy działu finansów
10	Pokój działu administracji i obsługi Kluczem dysponuje referent ds. administracji i obsługi, klucz deponowany jest na recepcji szkolnej	Ewidencja kontrahentów handlowych i usługowych	Tradycyjna / elektroniczna	Samodzielny referent ds. administracyjno - gospodarczych
		Ewidencja zamówień publicznych	Tradycyjna / elektroniczna	Samodzielny referent ds. administracyjno - gospodarczych
11	Pokój serwera szkolnego Kluczem dysponuje ASI, klucz deponowany jest na recepcji szkolnej	Ewidencja loginów	Tradycyjna / elektroniczna	ASI
12	Pokój nauczycielski Kluczami magnetycznymi i tradycyjnymi dysponują nauczyciele, klucze magnetyczne są indywidualnie przypisane do nauczyciela, klucz tradycyjny deponowany jest na recepcji	Dziennik lekcyjny	Elektroniczna / tradycyjna	Nauczyciele
		Rejestr zastępstw	Tradycyjny	Wicedyrektor
		Dokumentacja dotycząca organizacji pracy szkoły	Tradycyjna	Wicedyrektor
		Dokumentacja dotycząca spraw wychowawczych	Tradycyjna / elektroniczna	Wychowawcy klas / członkowie Szkolnego Zespołu Wychowawczego
13	Salę lekcyjne Kluczami dysponują nauczyciele, klucze deponowane są w pokoju nauczycielskim	Dziennik lekcyjny	Elektroniczna	Nauczyciele
14	Pokój nauczycieli wf Kluczami dysponują nauczyciele wf, klucz deponowany jest na recepcji	Dziennik lekcyjny	Elektroniczna	Nauczyciele wf
		Dokumentacja dotycząca spraw wychowawczych	Tradycyjna / elektroniczna	Wychowawcy klas
15	Pokój nauczycieli przedmiotów gastronomicznych Kluczami dysponują nauczyciele przedmiotów gastronomicznych, klucz deponowany jest na recepcji	Dziennik lekcyjny	Elektroniczna	Nauczyciele przedmiotów gastronomicznych
		Dokumentacja dotycząca spraw wychowawczych	Tradycyjna / elektroniczna	wychowawcy klas
16	Pokój składnicy akt Szkoły	Archiwum Szkoły	Tradycyjna	Samodzielny referent ds. administracyjno - biurowych

B. budynek nr 2 – ul. Katedralna 12, 78 – 100 Kołobrzeg

L.p.	Miejsce przechowywania danych / zabezpieczenie	Zbiory przechowywanych danych osobowych	Sposób przetwarzania i gromadzenia	Osoba/osoby odpowiedzialna
1	Gabinet Wicedyrektora ds. CKP Kluczami dysponuje Wicedyrektor ds. CKP, sekretarka szkoły, klucze deponowane są na recepcji CKP	Ewidencja osób przystępujących do egzaminów w ośrodku egzaminacyjnym OKE	Elektroniczna / tradycyjna	Wicedyrektor ds. CKP
2	Sekretariat Wicedyrektora ds. CKP Kluczami dysponuje sekretarz wicedyrektora CKP, klucze deponowane są na recepcji CKP	Ewidencja praktykantów odbywających praktykę w warsztatach szkolnych	Elektroniczny / tradycyjny	Sekretarz Wicedyrektora ds. CKP
		Dokumenty związane z Zakładowym Funduszem Świadczeń Socjalnych	Tradycyjny	Sekretarz Wicedyrektora ds. CKP
		Dzienniki praktyk zawodowych i zajęć praktycznych	Tradycyjny	Sekretarz Wicedyrektora ds. CKP/ nauczyciel przedmiotów zawodowych
		Dokumentacja organizacji warsztatów hotelowych i gastronomicznych szkoły.	Tradycyjna	Wicedyrektor ds. CKP
		Dokumentacja kursów i szkoleń organizowanych przez CKP	Tradycyjna / elektroniczna	Sekretarz Wicedyrektora ds. CKP
3	Pokój pedagoga / psychologa szkolnego Kluczami dysponuje pedagog i psycholog, klucze deponowane są na recepcji CKP	Dziennik pedagoga	Tradycyjna	Pedagog
		Dziennik psychologa	Tradycyjna	Psycholog
		Ewidencja opinii i orzeczeń	Tradycyjna	Pedagog / Psycholog
		Ewidencja opinii psychologiczno – pedagogicznych	Tradycyjna	Pedagog / Psycholog
		Ewidencja wyprawek szkolnych	Tradycyjna	Pedagog / Psycholog
		Dokumentacja programu Przeciwdziałania przemocy w rodzinie	Tradycyjna	Pedagog / Psycholog
		Ewidencja przyznanych stypendiów, zasiłków i obiadów	Tradycyjna	Pedagog / Psycholog
4	Pokój referenta ds. finansowych CKP Kluczami dysponuje referent ds. finansowych CKP, klucze deponowane są na recepcji CKP	Dokumenty księgowe dotyczące obsługi warsztatów szkolnych CKP	Tradycyjna	Referent ds. finansowych
5	Pokój Hotelowego Biura Obsługi Kluczami dysponują pracownicy HBU, klucze deponowane są na recepcji CKP	Ewidencje klientów hotelowych	Elektroniczna / tradycyjna	Pracownicy Hotelowego Biura Obsługi
		Ewidencja kontrahentów i usługodawców CKP	Elektroniczna / tradycyjna	Pracownicy Hotelowego Biura Obsługi
6	Pokój referenta ds. administracji i obsługi Kluczami dysponuje samodzielny referent ds. administracyjno – gospodarczych, klucze deponowane są na recepcji KP	Ewidencja kart wyposażenia osobistego pracownika	Tradycyjna	Samodzielny referent ds. administracyjno - gospodarczych
7	Pokój składnicy akt Szkoły	Archiwum Szkoły	Tradycyjna	Samodzielny referent ds. administracyjno -

				biurowych
8	Recepcja warsztatów hotelowych Recepcja czynna całodobowo. Do zamkniętej części recepcji kluczami dysponują pracownicy recepcji	Książka meldunkowa gości	Elektroniczna / tradycyjna	Pracownicy recepcji
		Ewidencja klientów hotelowych	Elektroniczna	Pracownicy recepcji
9	Restauracja warsztatów szkolnych Kluczami dysponują pracownicy restauracji, klucze deponowane są na recepcji CKP	Ewidencja kart abonamentowych	Elektroniczna	Pracownik HBU
10	Pomieszczenie magazynów warsztatów szkolnych Kluczami dysponują pracownicy magazynu, klucze deponowane są na recepcji CKP	Ewidencja dostawców	Tradycyjna	Pracownik magazynu

Uwagi dodatkowe:

- Teren wewnątrz szkoły i na zewnątrz szkoły jest monitorowany
- Wejście do szkoły i miejsc ogólnodostępnych na podstawie indywidualnych magnetycznych kart wejściowych dotyczy pracowników szkoły oraz uczniów - dotyczy budynku nr 1
- Do w/w pomieszczeń dostęp posiada pracownik obsługi tj. personel sprząający właściwy dla wskazanego rejonu pracy – dotyczy zarówno budynku nr 1 oraz nr 2

I.2 Zbiory danych przetwarzanych za pomocą systemów informatycznych

§ 3

L.p.	Nazwa zbioru danych osobowych / opis	Struktura danych osobowych
1	Arkusze organizacyjny	Imię, nazwisko, data urodzenia, nr PESEL, wykształcenie, stopień awansu zawodowego, staż pedagogiczny, pensum, dane płacowe, stanowisko i przydzielone zadania
2	Zgłoszenia uczestników konkursów międzyszkolnych	Imię i nazwisko, wiek, placówka do której uczęszcza
3	Ewidencja osób uczestniczących w programach związanych z funduszami europejskimi	Nazwisko, imiona, data i miejsce urodzenia, Pesel, adres zamieszkania
4	Ewidencja uczniów przystępujących do egzaminu potwierdzającego kwalifikacje zawodowe	Nazwisko, imiona, data i miejsce urodzenia, Pesel, dysleksja, mniejszość narodowa
5	Dokumentacja współpracy szkoły instytucjami w kraju i zagranicą	Nazwisko, imiona, data i miejsce urodzenia, Pesel, adres zamieszkania
6	Rejestr i dokumentacja dotycząca próbnych egzaminów potwierdzających kwalifikacje zawodowe	Nazwisko, imiona, data i miejsce urodzenia, Pesel, dysleksja,
7	Zestawienia wyników klasyfikacji	Nazwiska i imiona, oceny, informacje o egzaminach poprawkowych i klasyfikacyjnych i ich wynikach
8	Ewidencja uczniów przystępujących do egzaminu maturalnego	Nazwisko, imiona, data i miejsce urodzenia, Pesel, dysleksja, mniejszość narodowa
9	Dokumentacja związana z organizacją egzaminów poprawkowych i klasyfikacyjnych	Nazwisko, imiona, data i miejsce urodzenia, Pesel, dysleksja, mniejszość narodowa
10	Rejestr i dokumentacja dotycząca próbnych egzaminów maturalnych	Nazwisko, imiona, data i miejsce urodzenia, Pesel, dysleksja, mniejszość narodowa
11	Plan zajęć szkolnych	Rozkład zajęć uczniów w poszczególnych klasach, rozkład zajęć nauczycieli,
12	Rejestr zastępstw nauczycieli	Informacja o nieobecnościach i zastępstwach nauczycieli
13	Rejestr korespondencji przychodzącej i wychodzącej	Nazwisko, imię, nazwa firmy, adres
14	Rejestr wypadków pracowniczych i dokumentacja powypadkowa	Nazwiska i imiona, data urodzenia, adres zamieszkania lub pobytu, stan zdrowia
15	Rejestr ważności szkoleń BHP	Nazwiska i imiona, data urodzenia, adres zamieszkania, okres ważności szkoleń BHP

16	Biblioteka	Imię i nazwisko, data urodzenia, miejsce urodzenia, adres, dane o wypożyczeniach
17	Ewidencja ubezpieczeń uczniów	Nazwiska i imiona, data urodzenia, adres zamieszkania, pesel
18	Księgowość i finanse	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, dane kontrahentów i usługodawców,
19	Kadry	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, ubezpieczenie
20	Ewidencja loginów	Imię, nazwisko, stanowisko, numeryczny nr loginu
21	Dokumentacja dotycząca spraw wychowawczych	Nazwiska i imiona, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, pesel, wyniki nauki
22	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
23	Arkusze ocen	Nazwiska i imiona, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, pesel, nr książki uczniów, przebieg nauki, wyniki nauki
24	Ewidencja uczniów i rodziców (opiekunów prawnych)	Imię, nazwisko, adres, imiona i nazwisko rodziców, nr tel. stacjonarnego lub komórkowego, data urodzenia, nr PESEL
25	Ewidencja osób odbywających praktykę zawodową w CKP	Nazwiska i imiona, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, pesel, adres placówki oświatowej z której pochodzi praktykant
26	Książka meldunkowa gości	Nazwisko i imię, imiona rodziców, datę i miejsce urodzenia, adres miejsca pobytu stałego, datę przybycia i zamierzony czas trwania pobytu, oznaczenie dowodu osobistego lub innego dokumentu stwierdzającego tożsamość, a w tym numer i serię, datę jego wydania, datę ważności oraz oznaczenie organu, który go wydał,
27	Ewidencja kart rabatowych i pracowniczych	Nazwisko i imię, adres, ważność karty, wysokość rabatu, stan środków
28	Ewidencja kontrahentów i usługodawców	Nazwa firmy lub nazwisko imię oferenta, adres, zakres świadczonych usług, wyraz dostarczonych towarów i produktów

I.2.1 Programy informatyczne służące do przetwarzania danych osobowych

§ 4

1. Struktura informatyczna Szkoły składa się z komputerów połączonych siecią wewnętrzną LAN. Komputery Szkoły poprzez system firewall posiadają dostęp INTERNET, którego operatorem jest Orange S.A..
2. W ramach tej infrastruktury funkcjonują systemy informatyczne:
 - a) Dziennik elektroniczny LIBRUS służący do rejestrowania i przetwarzania danych związanych z procesem nauczania (oceny, frekwencja, informacje o uczniach rodzicach oraz inne dane), arkusze ocen, e-sekretariat oraz e-świadectwa
 - b) VULCAN – wykorzystywany w tworzeniu arkusza organizacyjnego, w prowadzeniu rekrutacji,
 - c) SIO - program do obsługi systemu informacji oświatowej,
 - d) PŁATNIK – System dwustronnej wymiany informacji do wysłania do ZUS zestawu dokumentów (korekty danych – pobieranych składek na ubezpieczenie emerytalne, rentowe, chorobowe, wypadkowe i zdrowotne) i odbierania informacji z ZUS,
 - e) VULKAN/Płace – program służący do obsługi płacowej Szkoły
 - f) VULKAN/Kadry – program służący od obsługi kadrowej Szkoły
 - g) Symfonia – program do obsługi księgowo – finansowej Szkoły, wykorzystywany również przy administrowaniu Szkołą
 - h) MOL/Biblioteka – program obsługi biblioteki
 - i) Forum/Przetargi – program wykorzystywany w przeprowadzaniu przetargów w Szkole
 - j) Hotelowy Chart – program obsługi klientów hotelowych w warsztatach szkolnych
 - k) Gastro Pos – program obsługi klientów restauracji w warsztatach szkolnych
 - l) Pakiet Microsoft Office

I.3 Zbiory danych przetwarzanych tradycyjnie

§ 4

L.p.	Nazwa zbioru danych osobowych / opis	Struktura danych osobowych
1	Arkusz organizacyjny	Imię, nazwisko, data urodzenia, nr PESEL, wykształcenie, stopień awansu zawodowego, staż pedagogiczny, pensum, dane płacowe, stanowisko i przydzielone zadania
2	Zgłoszenia uczestników konkursów międzyszkolnych	Imię i nazwisko, wiek, placówka do której uczęszcza
3	Księga uczniów	Nazwisko i imię ucznia, data i miejsce urodzenia, pesel, adresy zamieszkania ucznia, nazwiska i imiona rodziców, adres rodziców, Przyjęcie do szkoły: data, klasa/semestr, obwód szkolny, profil kierunku zawód specjalność, wypisanie ze szkoły: data, klasa, powody, data: wydania dokumentów, ukończenia szkoły, numer wydanego świadectwa (dyplomu)
4	Ewidencja osób uczestniczących w programach związanych z funduszami europejskimi	Nazwisko, imiona, data i miejsce urodzenia, Pesel, adres zamieszkania
5	Ewidencja uczniów przystępujących do egzaminu potwierdzającego kwalifikacje zawodowe	Nazwisko, imiona, data i miejsce urodzenia, Pesel, dysleksja, mniejszość narodowa
6	Ewidencja uczniów i pracowników dotycząca współpracy szkoły instytucjami w kraju i zagranicą	Nazwisko, imiona, data i miejsce urodzenia, Pesel, adres zamieszkania
7	Rejestr i dokumentacja dotycząca próbnych egzaminów potwierdzających kwalifikacje zawodowe	Nazwisko, imiona, data i miejsce urodzenia, Pesel, dysleksja,
8	Zestawienia wyników klasyfikacji	Nazwiska i imiona, oceny, informacje o egzaminach poprawkowych i klasyfikacyjnych i ich wynikach

9	Ewidencja uczniów przystępujących do egzaminu maturalnego	Nazwisko, imiona, data i miejsce urodzenia, Pesel, dysleksja, mniejszość narodowa
10	Ewidencja uczniów przystępujących egzaminów poprawkowych i klasyfikacyjnych	Nazwisko, imiona, klasa, wyniki nauczania
11	Rejestr i dokumentacja dotycząca próbnych egzaminów maturalnych	Nazwisko, imiona, data i miejsce urodzenia, Pesel, dysleksja, mniejszość narodowa
12	Plan zajęć szkolnych	Rozkład zajęć uczniów w poszczególnych klasach, rozkład zajęć nauczycieli,
13	Rejestr zastępstw nauczycieli	Informacja o nieobecnościach i zastępstwach nauczycieli
14	Rejestr korespondencji przychodzącej i wychodzącej	Nazwisko, imię, nazwa firmy, adres
15	Rejestr wypadków pracowniczych	Imię i nazwisko, data i rodzaj wypadku, miejsce wypadku i rodzaj zajęć, rodzaj urazu, okoliczności wypadku
16	Rejestr wypadków uczniowskich	Imię i nazwisko, data i rodzaj wypadku, miejsce wypadku i rodzaj zajęć, rodzaj urazu, okoliczności wypadku
17	Rejestr ważności szkoleń BHP	Nazwiska i imiona, data urodzenia, adres zamieszkania, okres ważności szkoleń BHP
18	Ewidencja ubezpieczeń uczniów	Nazwiska i imiona, data urodzenia, adres zamieszkania, pesel
19	Dziennik pedagoga	Imię i nazwisko, klasa, forma pomocy
20	Dziennik psychologa	Imię i nazwisko, klasa, forma pomocy
21	Ewidencja opinii i orzeczeń	Imię i nazwisko, data urodzenia, miejsce zamieszkania, stan zdrowia, zalecenia
22	Książka korespondencji przychodzącej i wychodzącej	Imię i nazwisko, adres zamieszkania lub dane adresowe instytucji lub firmy
23	Ewidencja wyprawek szkolnych	Imię i nazwisko rodzica, data urodzenia, adres zamieszkania, dochody, seria i nr dowodu osobistego, nr konta bankowego; imię i nazwisko ucznia, adres zamieszkania
24	Dokumentacja programu Przeciwdziałania przemocy w rodzinie	Imię i nazwisko rodzica, data urodzenia, adres zamieszkania, dochody
25	Ewidencja przyznanych stypendiów, zasiłków i obiadów	Imię i nazwisko rodzica, data urodzenia, adres zamieszkania, dochody, seria i nr dowodu osobistego, nr konta bankowego; imię i nazwisko ucznia, adres zamieszkania
26	Ewidencja Kart Zdrowia uczniów	Imię, nazwisko, adres, nr PESEL, imiona i nazwisko rodziców, karta zdrowia, bilans zdrowia
27	Księgowość i finanse	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, dane kontrahentów i usługodawców,
28	Kadry	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, ubezpieczenie
29	Ewidencja loginów	Imię, nazwisko, stanowisko, numeryczny nr loginu
30	Dokumentacja dotycząca spraw wychowawczych	Nazwiska i imiona, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, pesel, wyniki nauki
31	Biblioteka	Imię i nazwisko, data urodzenia, miejsce urodzenia, adres, dane o wypożyczeniach
32	Arkusze ocen	Nazwiska i imiona, imiona rodziców, data urodzenia,

		miejsce urodzenia, adres zamieszkania lub pobytu, pesel, nr księgi uczniów, przebieg nauki, wyniki nauki
33	Ewidencja decyzji dyrektora szkoły zwolnienie z niektórych przedmiotów,	Imię i nazwisko rodzica, adres zamieszkania, imię i nazwisko ucznia
34	Ewidencja osób odbywających praktykę zawodową w CKP	Nazwiska i imiona, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, pesel, adres placówki oświatowej z której pochodzi praktykant
35	Książka meldunkowa gości	Nazwisko i imię, imiona rodziców, datę i miejsce urodzenia, adres miejsca pobytu stałego, datę przybycia i zamierzony czas trwania pobytu, oznaczenie dowodu osobistego lub innego dokumentu stwierdzającego tożsamość, a w tym numer i serię, datę jego wydania, datę ważności oraz oznaczenie organu, który go wydał,
36	Ewidencja kart rabatowych i pracowniczych	Nazwisko i imię, adres, ważność karty, wysokość rabatu, stan środków
37	Ewidencja kontrahentów i usługodawców	Nazwa firmy lub nazwisko imię oferenta, adres, zakres świadczonych usług, wyraz dostarczonych towarów i produktów

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.

§ 6

Sposób przepływu danych pomiędzy poszczególnymi systemami jest następujący:

KADRY → PŁATNIK

Z aplikacji Vulcan/Kadry do programu Płatnik przekazywane są dane dotyczące zarejestrowania i wyrejestrowania pracowników.

Sposób przekazywania danych: manualny

PŁACE → PŁATNIK

Z aplikacji Vulcan/Płace do programu Płatnik przekazywane są dane dotyczące składek na ubezpieczenia.

Sposób przekazywania danych: manualny

PŁACE → Bank

Z programu Vulcan/Płace do Banku BGŻ o/Kołobrzeg przekazywane są dane dotyczące należnych kwot przelewanych na konto pracowników.
Sposób przekazywania danych: manualny

PŁACE → SIO

Z programu Vulcan/Płace do Systemu Informacji Oświatowej przekazywane są dane o wynagrodzeniach nauczycieli

Sposób przekazania danych: automatyczny

Pozostałe programy są niezależne i posiadają samodzielne bazy danych wprowadzane do systemu manualnie.

Komputery przynależne działom administracyjnym Szkoły działają niezależnie od sieci wewnętrznej Szkoły

Przetwarzanie danych osobowych w systemie informatycznym odbywa się przy zachowaniu wysokiego poziom bezpieczeństwa.

I.5 Środki techniczne i organizacyjne stosowane w przetwarzaniu danych

I.5.1 Cele i zasady funkcjonowania polityki bezpieczeństwa

§ 7

Polityka bezpieczeństwa informacji w Szkole 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 informacji 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 niezgodnemu 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 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 obowiązującym prawem, celami przetwarzania lub przechowywanie ich w sposób nie zapewniający 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

Administrator Danych Osobowych (ADO) – Dyrektor Szkoły:

- formułuje i wdraża warunki techniczne i organizacyjne służące ochronie danych osobowych przed ich udostępnieniem osobom nieupoważnionym, zabraniam przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem,
- decyduje o zakresie, celach oraz metodach przetwarzania i ochrony danych osobowych,
- odpowiada za zgodne z prawem przetwarzanie danych osobowych w Szkole,

§ 11

Administrator Bezpieczeństwa Informacji (ABI) – pracownik Szkoły wyznaczony przez Dyrektora:

- egzekwuje zgodnie z prawem przetwarzanie danych osobowych w Szkole w imieniu ADO,
- wydaje upoważnienie do przetwarzania danych osobowych określając w nich zakres i termin ważności – wzór upoważnienia określa **załącznik nr 1**,
- odwołuje upoważnienie – **załącznik nr 2**,
- prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych – wzór rejestru określa **załącznik nr 3**,
- ewidencjonuje oświadczenia osób upoważnionych o zaznajomieniu się z zasadami zachowania bezpieczeństwa danych – wzór oświadczenia określa **załącznik nr 4**,
- udziela wyjaśnień i interpretuje zgodność stosowanych rozwiązań w zakresie ochrony danych osobowych z przepisami prawa,
- bierze udział w podnoszeniu świadomości i kwalifikacji osób przetwarzających dane osobowe w Szkole i zapewnia odpowiedni poziom przeszkolenia w tym zakresie.
- określa potrzeby w zakresie stosowanych w Szkole zabezpieczeń, wnioskuje do ADO o zatwierdzenie proponowanych rozwiązań i nadzoruje prawidłowość ich wdrożenia,

§ 12

Administrator Systemu Informatycznego (ASI) – pracownik Szkoły wyznaczony przez Dyrektora:

- zarządza bezpieczeństwem przetwarzania danych osobowych w systemie informatycznym zgodnie z wymogami prawa i wskazówkami ABI lub ADO
- doskonali i rozwija metody zabezpieczenia danych przed zagrożeniami związanymi z ich przetwarzaniem,
- przydziela identyfikatory użytkownikom systemu informatycznego oraz zaznajamia ich z procedurami ustalania i zmiany haseł dostępu,
- nadzoruje prace związane z rozwojem, modyfikacją, serwisowaniem i konserwacją systemu,
- zapewnia bezpieczeństwo wewnętrznego i zewnętrznego obiegu informacji w sieci i zabezpieczenie łączny zewnętrznych,

- prowadzi nadzór nad archiwizacją zbiorów danych oraz zabezpiecza elektroniczne nośniki informacji zawierających dane osobowe.

§ 13

Pracownik przetwarzający dane (PPD) – pracownik upoważniony przez ABl:

- chroni 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,
- zapoznaje się zasadami określonymi w Polityce bezpieczeństwa informacji i Instrukcji zarządzania systemem informatycznym Szkoły i składa oświadczenie o znajomości tych przepisów.

I.5.3 Zasady udzielania dostępu do danych osobowych

§ 14

1. 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.

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

3. ABl może wyznaczyć upoważnionych do przetwarzania danych osobowych pracowników Szkoły do nadzoru nad upoważnionymi pracownikami podmiotów zewnętrznych lub innymi upoważnionymi osobami przetwarzającymi dane osobowe w Szkole.

I.5.4 Udostępnianie i powierzanie danych osobowych

§ 15

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

§ 16

Udostępnienie danych może nastąpić na **pisemny wniosek (załącznik nr 5)** zawierający następujące elementy:

- adresat wniosku (administrator danych),
- wnioskodawca,
- podstawa prawna (wskazanie potrzeby),
- wskazanie przeznaczenia,
- zakres informacji.

§ 17

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

§ 18

Powierzenie danych może nastąpić wyłącznie 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.

§ 19

Każda osoba fizyczna, której dane przetwarzane są w Szkole, ma prawo zwrócić się z **wnioskiem** o udzielenie informacji związanych z przetwarzaniem tych danych, prawo do 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.

I.5.5 Bezpieczeństwo w przetwarzaniu danych osobowych w formie tradycyjnej

§ 20

1. Pomieszczenia, w których znajdują się przetwarzane zbiory danych osobowych pozostają zawsze pod bezpośrednim nadzorem upoważnionego do ich przetwarzania pracownika.
2. Opuszczenie pomieszczenia, w których znajdują się zbiory danych osobowych musi być poprzedzone przeniesieniem zbioru danych do odpowiednio zabezpieczonego miejsca. Przy planowanej dłuższej nieobecności pracownika pomieszczenie winno być zamknięte na klucz. Dostęp do wybranych pomieszczeń kontrolowany za pomocą monitoringu wizyjnego.
3. Klucze do szaf, w których przechowywane są dane osobowe mają jedynie pracownicy upoważnieni do przetwarzania danych osobowych w zakresie zgodnym z kategorią danych.
4. Dostęp do pomieszczeń poza godzinami pracy szkoły jest kontrolowany za pomocą systemu monitoringu wizyjnego.
5. Korzystanie ze zbiorów danych osobowych przez osoby niezatrudnione w Szkole powinno odbywać się po uzyskaniu upoważnienia lub skonsultowane z ABI w przypadku osób upoważnionych do przetwarzania tych danych na podstawie ogólnie obowiązujących przepisów.
6. Dokumentacji, która zawiera zbiory danych osobowych, nie można wnosić poza teren szkoły. Wyjątek stanowi dokumentacja związana z realizacją określonych zadań edukacyjno – wychowawczych po za terenem szkoły w sytuacjach regulowanych innymi przepisach prawa. Za zabezpieczenia dokumentacji odpowiedzialna jest wskazana przez ADO osoba.
7. Osoby prowadzące dokumentację zobowiązane są do niezwłocznego poinformowania ABI lub ADO o podejrzeniu dostępu do dokumentacji przez osoby nieupoważnione.
8. Ponadto zabrania się:

- a. wyrzucania dokumentów zawierających dane osobowe bez uprzedniego ich trwałego zniszczenia - anonimizacji
- b. pozostawiania dokumentów, kopii dokumentów zawierających dane osobowe w drukarkach, kserokopiarkach,
- c. pozostawiania kluczy w drzwiach, szafach, biurkach, zostawiania otwartych pomieszczeń, w których przetwarza się dane osobowe,
- d. pozostawiania bez nadzoru osób trzecich przebywających w pomieszczeniach szkoły, w których przetwarzane są dane osobowe,
- e. pozostawiania dokumentów na biurku po zakończonej pracy, pozostawiania otwartych dokumentów na ekranie monitora bez blokady konsoli,
- f. ignorowania nieznanych osób z zewnątrz poruszających się w obszarze przetwarzania danych osobowych,
- g. przekazywania informacji będącymi danymi osobowymi osobom nieupoważnionym,

§ 21

Korzystanie ze zbiorów danych osobowych przez osoby niezatrudnione w Szkole powinno odbywać się po uzyskaniu **upoważnienia** lub skonsultowane z ABl w przypadku osób upoważnionych do przetwarzania tych danych na podstawie ogólnie obowiązujących przepisów.

I.5.6 Bezpieczeństwo w przetwarzaniu danych osobowych w systemach informatycznych

§ 22

Zasady bezpiecznego użytkowania 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

§ 23

Ze względu na formę przetwarzania danych osobowych	Rodzaje możliwych zagrożeń
Dane przetwarzane i przechowywane w formie tradycyjnej – „papierowej”	▪ zdarzenia losowe (powódź, pożar); ▪ kradzież danych, oszustwo, celowe działanie na szkodę szkoły ▪ zaniedbania pracowników szkoły (niedyskrecja, udostępnienie danych osobie nieupoważnionej); ▪ niekontrolowana obecność nieuprawnionych osób w obszarze

	przetwarzania; ▪ pokonanie zabezpieczeń fizycznych, włamania ▪ podsłuchy, podglądy w celu wyłudzenia danych ▪ ataki terrorystyczne; ▪ brak rejestrowania udostępniania danych; ▪ niewłaściwe miejsce i sposób przechowywania dokumentacji.
Dane przetwarzane i przechowywane za pomocą systemów informatycznych	▪ nie przydzielenie użytkownikom systemu informatycznego identyfikatorów; ▪ niewłaściwa administracja systemem; ▪ niewłaściwa konfiguracja systemu; ▪ fałszowanie kont użytkowników; ▪ kradzież danych kont; ▪ pokonanie zabezpieczeń programowych; ▪ zaniedbania pracowników szkoły (niedyskrecja, udostępnienie danych osobie nieupoważnionej); ▪ niekontrolowana obecność nieuprawnionych osób w obszarze przetwarzania; ▪ zdarzenia losowe np. pożar; ▪ niekontrolowane wytwarzanie i wypływ danych poza obszar przetwarzania z pomocą nośników informacji i komputerów przenośnych; ▪ naprawy i konserwacje systemu lub sieci teleinformatycznej wykonywane przez osoby nieuprawnione; ▪ przypadkowe bądź celowe uszkodzenie systemów i aplikacji informatycznych lub sieci; ▪ przypadkowe bądź celowe modyfikowanie systemów i aplikacji informatycznych lub sieci; ▪ przypadkowe bądź celowe wprowadzenie zmian do chronionych danych osobowych; ▪ brak rejestrowania zdarzeń tworzenia lub modyfikowania danych.

I.6.2 Sposób zabezpieczenia danych

§ 24

Ze względu na formę przetwarzania danych osobowych	Formy wprowadzonych zabezpieczeń
Dane przetwarzane i przechowywane w	▪ przechowywanie danych w

formie tradycyjnej – „papierowej”	▪ pomieszczeniach zamykanych na klucz; ▪ przechowywanie danych osobowych w szafach zamykanych na klucz; ▪ przetwarzanie danych wyłącznie przez osoby posiadające upoważnienie nadane przez ABI; ▪ zapoznanie pracowników z zasadami przetwarzania danych osobowych oraz obsługą systemu służącego do ich przetwarzania.
Dane przetwarzane i przechowywane za pomocą systemów informatycznych	▪ kontrola dostępu do systemów; ▪ zastosowanie programów antywirusowych i innych regulamie aktualizowanych narzędzi ochrony; ▪ systematyczne tworzenie kopii zapasowych zbiorów danych przetwarzanych w systemach informatycznych; ▪ składowanie nośników wymiennych i nośników kopii zapasowych w odpowiednio zabezpieczonych szafach; ▪ przydzielenie pracownikom indywidualnych kont użytkowników i haseł; ▪ stosowanie indywidualnych haseł logowania do poszczególnych programów; ▪ właściwa budowa hasła (zawiera litery i cyfry).

I.6.3 Określenie wielkości ryzyka

§ 25

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

§ 26

Uwzględniając kategorie przetwarzanych danych oraz zagrożenia zidentyfikowane w wyniku przeprowadzonej analizy ryzyka dla systemów informatycznych, stosuje się wysoki poziom bezpieczeństwa. Administrator Bezpieczeństwa Informacji i Administrator Systemów Informatycznych przeprowadzają okresową analizę ryzyka dla poszczególnych systemów i na tej podstawie przedstawiają Administratorowi Danych Osobowych 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

§ 27

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

§ 28

1. Za tworzenie, modyfikację i nadawanie uprawnień kontom użytkowników odpowiada ASI.
2. ASI nadaje uprawnienia w systemie informatycznym na podstawie upoważnienia nadanego pracownikowi przez ADO lub ABI.

§ 29

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

§ 30

Osoby dopuszczone do przetwarzania danych osobowych zobowiązane są do zachowania tajemnicy w zakresie tych danych oraz sposobów ich zabezpieczenia. Obowiązek ten istnieje również po ustaniu stosunku pracy, co jest równoznaczne z cofnięciem uprawnień do przetwarzania danych osobowych.

II.2 Zabezpieczenie danych w systemie informatycznym

§ 31

1. Oprogramowanie wykorzystywane do przetwarzania danych posiada własny system kont (zabezpieczonych hasłami) i uprawnień. Zmiana hasła jest wymuszona automatycznie przez system.
2. W przypadku oprogramowania, które nie ma automatycznego wymuszania zmiany hasła, zaleca się dokonywać zmiany hasła co 30 dni.
3. W przypadku utracenia hasła użytkownik ma obowiązek skontaktować się z ASI celem uzyskania nowego hasła.

§ 32

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.

§ 33

1. Stosuje się aktywną ochronę antywirusową każdym komputerze, na którym przetwarzane są dane osobowe.
2. Za dokonywanie skanowania systemu w poszukiwaniu złośliwego oprogramowania (w przypadku braku ochrony rezydentnej) i aktualizację bazy wirusów odpowiada użytkownik stacji roboczej.

II.3 Zasady bezpieczeństwa podczas pracy w systemie informatycznym

§ 34

W celu rozpoczęcia pracy w systemie informatycznym użytkownik:

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

§ 35

1. 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 chroniony hasłem.
2. W sytuacji gdy wgląd w wyświetlane na monitorze dane może mieć nieuprawniona osoba należy tymczasowo zmienić widok wyświetlany na monitorze lub obrócić monitor (przymknąć ekran laptopa) w sposób uniemożliwiający wgląd w wyświetlaną treść.
3. Użytkownik wyrejestrowuje się z systemu informatycznego przed wyłączeniem stacji komputerowej poprzez zamknięcie programu przetwarzającego dane oraz wylogowanie się z systemu operacyjnego.

§ 36

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

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

§ 37

Na fakt naruszenia zabezpieczeń systemu mogą wskazywać:

- nietypowy stan stacji roboczej (np. brak zasilania, problemy z uruchomieniem);
- 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

§ 38

1. Pełne kopie zapasowe zbiorów danych tworzone są 2 razy w ciągu roku – wykonuje ASI
2. Odpowiedzialnym za wykonanie bieżących kopii danych (dziennych) jest pracownik obsługujący dany program przetwarzający dane, w sytuacji gdy wystąpiła zmiana danych.
3. Pełne kopie danych przechowywane są w szafie metalowej w sekretariacie Szkoły.
4. Kopie dzienne danych przechowywane są na serwerze Szkoły.

§ 39

1. Usuwanie kopii danych następuje poprzez bezpieczne kasowanie. Nośniki danych, na których zapisywane są kopie bezpieczeństwa niszczy się trwale w sposób mechaniczny.
2. Za usuwanie kopii odpowiedzialny jest ABI.

II.5 Udostępnienie danych

§ 40

1. Dane osobowe przetwarzane w systemach informatycznych mogą być udostępnione osobom i podmiotom z mocy przepisów prawa.
2. Do podmiotów, dla których dopuszczalne jest udostępnianie danych przez szkołę należą:
 - Organ Nadzorujący (w związku z awansem zawodowym, wyniki badań psychologiczno-pedagogicznych dzieci i młodzieży),
 - Organ Prowadzący (wykaz z czasem pracy pracowników, udostępnianie dzienników zajęć, wykazy wygenerowane z SIO, wszystkie dane dotyczące pracowników i uczniów),
 - Centralna Komisja Egzaminacyjna w zakresie umożliwiającym przeprowadzenia egzaminów
 - Dzienniki lekcyjne (dane rodziców w zakresie opisanym w Rozporządzeniu MEN z dnia 19 lutego 2002 r. w sprawie sposobu prowadzenia dokumentacji),
 - Strona www szkoły (dane osobowe ucznia i np. jego osiągnięcia, publikowanie list z wynikami, zdjęciem – tylko za zgodą, imiona i nazwiska pracowników, tytuły naukowe, plan zajęć, informacje o pracy szkoły),

- Szkolna tablica ogłoszeń (informacje o pracy szkoły, plan zajęć, dane osobowe ucznia i np. jego osiągnięcia, publikowanie list z wynikami, zdjęciem – tylko za zgodą),
- Formularz rekrutacyjny do szkoły, karta potwierdzenia woli (dane osobowe rodziców/prawnych opiekunów i ucznia: adres zamieszkania, nr telefonu, PESEL ucznia, itp. – tylko za zgodą),
- Podmioty świadczące usługi w zakresie oświaty, np. towarzystwa ubezpieczeniowe (w zależności od celu),
- Podmioty nadzorujące realizację projektu EFS (dane osobowe uczestników projektu i ich rodziców, w zależności od celu).
- Inne podmioty – po określeniu celu i zakresu przekazanych danych, na podstawie wniosku (np. sądy rodzinne)

II.6 Przeglądy i konserwacje systemów

§ 41

1. Wszelkie prace związane z naprawami i konserwacją systemu informatycznego przetwarzającego dane osobowe mogą być wykonywane wyłącznie przez pracowników Szkoły lub przez upoważnionych przedstawicieli wykonawców.
2. Powyższe prace powinny uwzględniać wymagany poziom zabezpieczenia tych danych przed dostępem do nich osób nieupoważnionych.
3. Wszelkie prace konserwacyjne systemów informatycznych Szkoły wykonywane są przez ASI lub za jego wiedzą i nadzorem.
4. Przed rozpoczęciem prac przez osoby niebędące pracownikami Szkoły należy dokonać potwierdzenia tożsamości tychże osób.

II.7 Niszczenie wydruków i nośników danych

§ 42

1. Wszelkie 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 /w sposób uniemożliwiający ich odczytanie (pocięte w poprzeczne paski).
2. Niszczenie zapisów na nośnikach danych powinno odbywać się poprzez wymazywanie informacji oraz formatowanie nośnika.
3. Uszkodzone nośniki danych przed ich wyrzuceniem należy fizycznie zniszczyć w niszczarce.

INSTRUKCJA POSTĘPOWANIA W SYTUACJI NARUSZENIA DANYCH

III.1 Istota naruszenia danych osobowych

§ 43

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 przypadku naruszenia danych osobowych

§ 44

1. Każdy pracownik Szkoły, który stwierdzi fakt naruszenia bezpieczeństwa danych przez osobę przetwarzającą dane osobowe, bądź posiada informację mogącą mieć wpływ na bezpieczeństwo danych osobowych jest zobowiązany niezwłocznie zgłosić to ADO lub ABI.
2. Każdy pracownik Szkoły, który stwierdzi fakt naruszenia bezpieczeństwa danych ma obowiązek podjąć czynności niezbędne do powstrzymania skutków naruszenia ochrony oraz ustalić przyczynę i sprawcę naruszenia ochrony.
3. W przypadku stwierdzenia naruszenia bezpieczeństwa danych należy zaniechać wszelkich działań mogących utrudnić analizę wystąpienia naruszenia i udokumentowanie zdarzenia oraz nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia ADO lub ABI. Formy naruszeń danych osobowych zawiera **załącznik nr 6**

§ 45

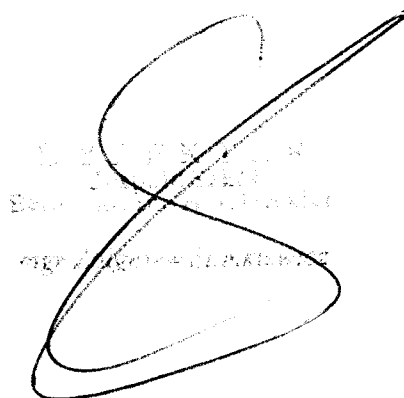
1. ABI podejmuje następujące kroki:
 - zapoznaje się z zaistniałą sytuacją i wybiera sposób dalszego postępowania uwzględniając zagrożenie w prawidłowości pracy Szkoły,
 - może zażądać dokładnej relacji z zaistniałego naruszenia bezpieczeństwa danych osobowych od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje w związku z zaistniałym naruszeniem,
 - rozważa celowość i potrzebę powiadomienia o zaistniałym naruszeniu ADO,
2. ABI dokumentuje zaistniały przypadek naruszenia bezpieczeństwa danych osobowych sporządzając raport wg wzoru stanowiącego **załącznik nr 7** i przekazuje go ADO.

3. ABl 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).

IV.3 Sankcje karne

§ 46

1. 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.
2. Kara dyscyplinarna, wobec osoby uchylającej się od powiadomienia o naruszeniu danych osobowych nie wyklucza odpowiedzialności kamej tej osoby zgodnie z ustawą o ochronie danych osobowych.

A handwritten signature in black ink is written over a faint, circular official stamp. The stamp contains text in Polish, including "Urząd Ochrony Danych Osobowych" and "Urząd Gminy".

.....
(pieczęć Szkoły)

Kołobrzeg, dnia r.

**UPOWAŻNIENIE nr/20.....
do przetwarzania danych osobowych**

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

upoważniam Panią/Pana.....
zatrudnioną (ego) w Zespole Szkół Ekonomiczno – Hotelarskich w Kołobrzegu na
stanowisku do przetwarzania danych osobowych
zgromadzonych w formie tradycyjnej oraz w systemach informatycznych w zakresie
wynikającym z zajmowanego stanowiska pracy, w okresie od dnia
..... 20..... r. do

Wyżej wymieniona osoba została wpisana do ewidencji osób zatrudnionych przy
przetwarzaniu danych osobowych w Szkole.

.....
(podpis Administratora Bezpieczeństwa Informacji)

Przyjmuję do wiadomości i stosowania.

.....
(Czytelny podpis osoby upoważnionej)

.....
(pieczęć Szkoły)

Kołobrzeg, dnia r.

**ODWOŁANIE UPOWAŻNIENIA nr/20.....
do przetwarzania danych osobowych**

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. nr 10 poz. 926 z późn. zm.) odwołuję z dniem upoważnienie do przetwarzania danych osobowych wystawione dla Pani/Pana

.....
(podpis Administratora Bezpieczeństwa Informacji)

.....
(pieczęć Szkoły)

Kołobrzeg, dnia r.

**REJESTR OSÓB UPOWAŻNIONYCH
DO PRZETWARZANIA DANYCH OSOBOWYCH**

Nr upoważnienia	Imię i nazwisko	Identyfikator użytkownika*	Zakres upoważnienia do przetwarzania danych osobowych	Data nadania uprawnień i podpis ABI	Data odebrania uprawnień i podpis ABI	Uwagi

* Wypełnia się tylko dla osób upoważnionych do przetwarzania danych osobowych, które zostały dopuszczone do przetwarzania danych osobowych w systemie informatycznym

OŚWIADCZENIE
o zachowaniu poufności i zapoznaniu się z przepisami

Ja niżej podpisany(a) oświadczam, iż
zobowiązuję się do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia, do
których mam lub będę miał(a) dostęp w związku z wykonywaniem:

Rodzaj zadań *)

zadań i obowiązków służbowych wynikających z umowy o pracę	
zadań wynikających z umowy cywilno-prawnej	
zadań wynikających z umowy - w związku z praktyką studencką	

*) właściwe zaznaczyć X

zarówno w trakcie wykonywania umowy, jak i po jej ustaniu.

Zobowiązuję się przestrzegać polityki, instrukcji i procedur, obowiązujących w **Zespole Szkół
Ekonomiczno – Hotelarskich w Kołobrzegu** ul. Łopuskiego 13 – zwanego dalej ZSE-H a dotyczących
ochrony danych osobowych.

W szczególności oświadczam, że bez upoważnienia nie będę wykorzystywał(a) danych osobowych ze
zbiorów znajdujących się w ZSE-H.

Oświadczam, że zostałem(am) poinformowany(a) o obowiązujących w ZSE-H zasadach, dotyczących
przetwarzania danych osobowych, określonych w „**Polityce Bezpieczeństwa Informacji**”

Oświadczam, że zostałem(am) zapoznany(a) z przepisami Ustawy o ochronie danych osobowych (tekst
jednolity: Dz. U. 2014r, poz. 1182) oraz Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z
dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków
technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące
do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024 ze zm.).

Oświadczam, że zostałem(am) poinformowany o grożącej, stosownie do przepisów rozdziału 8 ustawy
o ochronie danych osobowych, odpowiedzialności karnej. Niezależnie od odpowiedzialności
przewidzianej w wymienionych przepisach, mam świadomość, że naruszenie zasad ochrony danych
osobowych, obowiązujących w Szkole może zostać uznane za ciężkie naruszenie podstawowych
obowiązków pracowniczych i skutkować odpowiedzialnością dyscyplinarną.

Kołobrzeg dnia. r.

miejsce i data złożenia oświadczenia

czytelny podpis osoby składającej oświadczenie

.....
(pieczęć Szkoły)

Kołobrzeg, dnia r.

.....
(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 Zespole Szkół Ekonomiczno – Hotelarskich im. E. Gierczak w Kołobrzegu, 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 Zespole Szkół Ekonomiczno – Hotelarskich im. E. Gierczak w Kołobrzegu 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.

.....
(Administratora Bezpieczeństwa Informacji)

Tabela form naruszeń danych osobowych

Nr (kod) naruszeń	Formy naruszeń	Sposób postępowania
A	Forma naruszenia ochrony danych osobowych przez pracownika zatrudnionego przy przetwarzaniu danych	
A.1	W zakresie wiedzy:	
A.1.1	Ujawnianie sposobu działania aplikacji i systemu jej zabezpieczeń osobom niepowołanym	Natychmiast przerwać rozmowę lub inną czynność prowadzącą do ujawnienia informacji. Sporządzić raport z opisem, jaka informacja została ujawniona, powiadomić ABl.
A.1.2	Ujawnianie informacji o sprzęcie i pozostałej infrastrukturze informatycznej	Natychmiast przerwać rozmowę lub inną czynność prowadzącą do ujawnienia informacji. Sporządzić raport z opisem, jaka informacja została ujawniona, powiadomić ABl.
A.1.3	Dopuszczanie i stwarzanie warunków, aby ktokolwiek taką wiedzę mógł pozyskać np. z obserwacji lub dokumentacji.	Natychmiast przerwać rozmowę lub inną czynność prowadzącą do ujawnienia informacji. Sporządzić raport z opisem, jaka informacja została ujawniona, powiadomić ABl.
A.2	W zakresie sprzętu i oprogramowania	
A.2.1	Opuszczenie stanowiska pracy i pozostawienie aktywnej aplikacji umożliwiającej dostęp do bazy danych osobowych.	Niezwłocznie zakończyć działanie aplikacji. Sporządzić raport
A.2.2	Dopuszczenie do korzystania z aplikacji umożliwiającej dostęp do bazy danych osobowych przez jakiegokolwiek inne osoby niż osoba, której identyfikator został przydzielony.	Wezwać osobę bezprawnie korzystającą z aplikacji do opuszczenia stanowiska przy komputerze. Pouczyć osobę, która dopuściła do takiej sytuacji. Sporządzić raport.
A.2.3	Pozostawienie w jakimkolwiek niezabezpieczonym, a w szczególności w miejscu widocznym, zapisanego hasła dostępu do bazy danych osobowych i sieci	Natychmiast zabezpieczyć notatkę z hasłami w sposób uniemożliwiający odczytanie. Niezwłocznie powiadomić ABl. Sporządzić raport.
A. 2.4	Dopuszczenie do użytkowania sprzętu komputerowego i oprogramowania umożliwiającego dostęp do bazy danych osobowych przez osoby nie będące pracownikami.	Wezwać osobę nieuprawnioną do opuszczenia stanowiska. Ustalić jakie czynności zostały przez osoby nieuprawnione wykonane. Przerwać działające programy. Niezwłocznie powiadomić administratora bezpieczeństwa informacji. Sporządzić raport.
A.2.5	Samodzielne instalowanie jakiegokolwiek oprogramowania.	Pouczyć osobę popełniającą wymienioną czynność, aby jej zaniechała. Wezwać ASI w celu odinstalowania programów. Sporządzić raport
A.2.6	Modyfikowanie parametrów systemu i aplikacji	Wezwać osobę popełniającą wymienioną czynność, aby jej zaniechała. Sporządzić raport.
A.2.7	Odczytywanie nośników danych przed sprawdzeniem ich programem antywirusowym.	Pouczyć osobę popełniającą wymienioną czynność, aby zaczęła stosować się do wymogów bezpieczeństwa pracy. Wezwać służby informatyczne w celu wykonania kontroli antywirusowej. Sporządzić raport.
A.3	W zakresie dokumentów i obrazów zawierających dane osobowe	
A.3.1	Pozostawienie dokumentów w otwartych pomieszczeniach bez nadzoru	Zabezpieczyć dokumenty. Sporządzić raport.
A.3.2	Przechowywanie dokumentów zabezpieczonych w niedostatecznym	Powiadomić przełożonych. Spowodować poprawienie zabezpieczeń sporządzić raport

	stopniu przed dostępem osób niepowołanych.	
A.3.3	Wyrzucanie dokumentów w stopniu zniszczenia umożliwiającym ich odczytanie.	Zabezpieczyć niewłaściwie zniszczone dokumenty. Powiadomić przełożonych. Sporządzić raport.
A.3.4	Dopuszczanie do kopiowania dokumentów i utraty kontroli nad kopią	Zaprzestać kopiowania. Odzyskać i zabezpieczyć wykonaną kopię. Powiadomić przełożonych. Sporządzić raport.
A.3.5	Dopuszczanie, aby inne osoby odczytywały zawartość ekranu monitora, na którym wyświetlane są dane osobowe.	Wezwać nieuprawnioną osobę odczytującą dane do zaprzestania czynności, wyłączyć monitor. Jeżeli ujawnione zostały ważne dane - sporządzić raport
A.3.6	Sporządzanie kopii danych na nośnikach danych w sytuacjach nie przewidzianych procedurą	Spowodować zaprzestanie kopiowania. Odzyskać i zabezpieczyć wykonaną kopię. Powiadomić ABI. Sporządzić raport.
A.3.7	Utrata kontroli nad kopią danych osobowych.	Podjąć próbę odzyskania kopii. Powiadomić ABI. Sporządzić raport
A.4	W zakresie pomieszczeń i infrastruktury służących do przetwarzania danych osobowych	
A.4.1	Opuszczanie i pozostawianie bez dozoru nie zamkniętego pomieszczenia, w którym zlokalizowany jest sprzęt komputerowy używany do przetwarzania danych osobowych, co stwarza ryzyko dokonania na sprzęcie lub oprogramowaniu modyfikacji zagrażających bezpieczeństwu danych osobowych.	Zabezpieczyć (zamknąć) pomieszczenie. Powiadomić przełożonych . Sporządzić raport.
A.4.2	Wpuszczanie do pomieszczeń osób nieznanych i dopuszczanie do ich kontaktu ze sprzętem komputerowym.	Wezwać osoby bezprawnie przebywające w pomieszczeniach do ich opuszczenia, próbować ustalić ich tożsamość. Powiadomić przełożonych i administratora bezpieczeństwa informacji. Sporządzić raport.
A.4.3	Dopuszczanie, aby osoby spoza służb informatycznych i telekomunikacyjnych podłączały jakiegokolwiek urządzenia do sieci komputerowej, demontowały elementy obudów gniazd i torów kablowych lub dokonywały jakiegokolwiek manipulacji.	Wezwać osoby dokonujące zakazanych czynności do ich zaprzestania. Postarać się ustalić ich tożsamość. Powiadomić ASI i ABI. Sporządzić raport.
A.5	W zakresie pomieszczeń w których znajdują się komputery centralne i urządzenia sieci.	
A.5.1	Dopuszczenie lub ignorowanie faktu, że osoby spoza służb informatycznych i telekomunikacyjnych dokonują jakiegokolwiek manipulacji przy urządzeniach lub okablowaniu sieci komputerowej w miejscach publicznych (hole, korytarze, itp.).	Wezwać osoby dokonujące zakazanych czynności do ich zaprzestania i ew. opuszczenia pomieszczeń. Postarać się ustalić ich tożsamość. Powiadomić ASI i ABI. Sporządzić raport
A.5.2	Dopuszczanie do znalezienia się w pomieszczeniach komputerów centralnych	Wezwać osoby dokonujące zakazanych czynności do ich zaprzestania i opuszczenia lub węzłów sieci komputerowej osób spoza służb informatycznych i telekomunikacyjnych lub ignorowania takiego faktu. chronionych pomieszczeń. Postarać się ustalić ich tożsamość. Powiadomić ASI i ABI. Sporządzić raport
B	Zjawiska świadczące o możliwości naruszenia ochrony danych osobowych.	
B.1	Ślady manipulacji przy układach sieci komputerowej lub komputerach.	Powiadomić niezwłocznie ABI oraz ASI. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji. Sporządzić raport
B.2	Obecność nowych kabli o nieznanym przeznaczeniu i pochodzeniu.	Powiadomić niezwłocznie ASI. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji. Sporządzić raport.

B.3	Niezapowiedziane zmiany w wyglądzie lub zachowaniu aplikacji służącej do przetwarzania danych osobowych.	Powiadomić niezwłocznie ASI. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji. Sporządzić raport.
B.4	Nieoczekiwane, nie dające się wyjaśnić, zmiany zawartości bazy danych	Powiadomić niezwłocznie ASI. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji. Sporządzić raport
B.5	Obecność nowych programów w komputerze lub inne zmiany w konfiguracji oprogramowania.	Powiadomić niezwłocznie ASI. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji. Sporządzić raport.
B.6	Ślady włamania do pomieszczeń, w których przetwarzane są dane osobowe.	Postępować zgodnie z właściwymi przepisami. Powiadomić niezwłocznie administratora bezpieczeństwa informacji. Sporządzić raport.
C	Formy naruszenia ochrony danych osobowych przez obsługę informatyczną w kontaktach z użytkownikiem	
C.1	Próba uzyskania hasła uprawniającego do dostępu do danych osobowych w ramach pomocy technicznej.	Powiadomić ABI. Sporządzić raport.
C.2	Próba nieuzasadnionego przeglądania (modyfikowania) w ramach pomocy technicznej danych osobowych za pomocą aplikacji w bazie danych identyfikatorem i hasłem użytkownika.	Powiadomić ABI. Sporządzić raport.

Raport o naruszeniu danych osobowych

Sporządzający raport

Imię i nazwisko

Stanowisko (funkcja)

Kod formy naruszenia danych (wg tabeli)

1. Miejsce , dokładny czas i data naruszenia ochrony danych osobowych (piętro godzina ,
nr pokoju , itp.)

.....
.....

2. Osoba powodująca naruszenie (która swoim działaniem lub zaniechaniem przyczyniła się
do naruszenia ochrony danych osobowych)

.....
.....

3. Osoby , które uczestniczyły w zdarzeniu związanym z naruszeniem ochrony danych
osobowych

.....
.....

4. Informacja o danych , które zostały lub mogły zostać ujawnione

.....
.....

5. Zabezpieczone materiały lub inne dowody związane z wydarzeniem

.....
.....

6. Krótki opis wydarzenia związanego z naruszeniem ochrony danych osobowych (przebieg
zdarzenia , opis zachowania uczestników , podjęte działania)

.....
.....

.....
data i podpis osoby sporządzającej raport