

POLITYKA BEZPIECZEŃSTWA INFORMACJI

Biskupiec 2012

**Polityka Bezpieczeństwa Informacji
w zakresie danych osobowych w
Urzędzie Gminy
Gminnym Ośrodku Pomocy Społecznej
Gminnym Zespole Obsługi Szkół
Gminnym Ośrodku Kultury
I Gminnej Bibliotece Samorządowej w Biskupcu.**

1. Wstęp i podstawowe pojęcia

§ 1

Podstawa prawna:

- Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2002/101/926 – tekst jednolity z późniejszymi zmianami),
- Ustawa z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. 1999/11/95)
- Rozporządzenie z dnia 29 kwietnia 2004 r. Ministra Spraw Wewnętrznych i Administracji (Dz. U. 2004/100/1024).

§ 2

Kierownictwa Urzędu Gminy Biskupiec zwanego dalej Urzędem, Gminnego Ośrodka Pomocy Społecznej zwanego dalej GOPS, Gminnego Zespołu Obsługi Szkół zwanego dalej GZOS, Gminnego Ośrodka Kultury zwanego dalej GOK i Gminnej Bibliotece Samorządowej w Biskupcu zwanej dalej Biblioteką świadome wagi problemów związanych z ochroną prawa do prywatności, w tym w szczególności prawa osób fizycznych powierzających Urzędowi, GOPS, GZOS, GOK i Bibliotece swoje dane osobowe, do właściwej i skutecznej ochrony tych danych deklarują zamiar:

1. Podejmowania wszystkich działań niezbędnych dla ochrony praw i usprawiedliwionych interesów jednostki, związanych z bezpieczeństwem danych osobowych,
2. Stałego podnoszenia świadomości oraz kwalifikacji osób przetwarzających dane osobowe w Urzędzie, GOPS, GZOS, GOK i Bibliotece w zakresie problematyki bezpieczeństwa tych danych, w tym propagowania świadomości wartości powierzonych Urzędowi, GOPS, GZOS, GOK i Bibliotece danych osobowych, jako czynnika wpływającego na jakość i ciągłość działalności oraz wiarygodność Urzędu, GOPS, GZOS, GOK i Biblioteki.
3. Traktowania obowiązków osób zatrudnionych przy przetwarzaniu danych osobowych jako należących do kategorii podstawowych obowiązków pracowniczych oraz stanowczego egzekwowania ich wykonania przez zatrudnione osoby,
4. Doskonalenia i rozwijania nowoczesnych metod zabezpieczenia danych przed zagrożeniami związanymi z ich przetwarzaniem, szczególnie w zakresie dotyczącym dynamicznego rozwoju metod i technik przetwarzania tych danych w systemach informatycznych oraz sieciach telekomunikacyjnych.

§ 3

Realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych, Urząd, GOPS, GZOS, GOK i Biblioteka dokładają szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności zapewnia, aby dane te były:

1. Przetwarzane zgodnie z prawem,
2. Zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami,
3. Merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane,
4. Przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.

§ 4

Definicje określeń użytych w dokumencie:

1. **Administrator Danych Osobowych (ADO)** – Wójt Gminy Biskupiec,
2. **Administrator Bezpieczeństwa Informacji** - osoba wyznaczona przez ADO, odpowiedzialna za bezpieczeństwo danych osobowych przetwarzanych w systemach informatycznych, zwana dalej ABI.
3. **Administrator Systemów Informatycznych** - osoba wyznaczona przez ADO, odpowiedzialna za sprawność i konserwację oraz wdrażanie technicznych zabezpieczeń systemów informatycznych przetwarzających zbiory danych osobowych, zwany dalej ASI.
4. **użytkownik systemu** - osoba posiadająca upoważnienie wydane przez Administratora lub uprawnioną przez niego osobę i dopuszczona jako użytkownik do przetwarzania danych osobowych w systemie informatycznym danej komórki organizacyjnej w zakresie wskazanym w upoważnieniu, zwana dalej użytkownikiem.
5. **zbiór danych osobowych** - każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie;
6. **dane osobowe** - wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
7. **przetwarzanie danych** – 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;
8. **system informatyczny** - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych;
9. **system tradycyjny** - zespół procedur organizacyjnych, związanych z mechanicznym przetwarzaniem informacji i wyposażenia, i środków trwałych w celu przetwarzania danych osobowych na papierze;
10. **usuwanie danych** - rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą

2. Wykaz obszarów, w których przetwarzane są dane osobowe:

§ 5

Do przetwarzania danych osobowych dochodzi lub może dochodzić we wszystkich pomieszczeniach administracyjnych wyposażonych w kartoteki, rejestry i inne formy papierowe oraz w służbowy komputer osobisty, które znajdują się w budynkach określonych zgodnie z poniższym zestawieniem:

Oddział	Nr pomieszczenia	Osoby pracujące w pomieszczeniu(stanowisko / liczba osób)	Część budynku	Lokalizacja budynku
Pomoc Społeczna i Zapomogi	1	Specjalista pracownik socjalny/ 4	Parter – Gminny Ośrodek Pomocy Społecznej	Biskupiec ul. Rynek 1 , 13-340 Biskupiec
Świadczenia Rodzinne i Fundusz Alimentacyjny	2	-Kierownik GOPS -inspektor ds. świadczeń rodzinnych/ 1 -referent/ 1 -koordynator projektu/ 1	Parter – Gminny Ośrodek Pomocy Społecznej	Biskupiec ul. Rynek 1 , 13-340 Biskupiec
USC	4	- zastępca kierownika USC/ 1	Piętro I – Urząd Gminy Biskupiec	Biskupiec ul. Rynek 1 , 13-340 Biskupiec
Budownictwo i Ochrona Środowiska	7	- inspektor ds. budownictwa wiejskiego, gospodarki komunalnej i mieszkaniowej, inwestycji i mienia komunalnego / 1 -młodszy referent ds. planowania przestrzennego i ochrony środowiska / 1	Piętro I – Urząd Gminy Biskupiec	Biskupiec ul. Rynek 1 , 13-340 Biskupiec
Ewidencja Ludności, Meldunki	8	- inspektor ds. obywatelskich, z – ca kierownika USC /1	Piętro I – Urząd Gminy Biskupiec	Biskupiec ul. Rynek 1 , 13-340 Biskupiec

Podatki	9	-inspektor ds. opłat i podatków/ 1 -inspektor ds. windykacji należności	Piętro I – Urząd Gminy Biskupiec	Biskupiec ul. Rynek 1 , 13-340 Biskupiec
Księgowość	10	-inspektor ds. księgowości budżetowej/ 3	Piętro I – Urząd Gminy Biskupiec	Biskupiec ul. Rynek 1 , 13-340 Biskupiec
Kadry, Działalność Gospodarcza	11	- inspektor ds. działalności gospodarczej/ 1 - inspektor ds. organizacyjno – kadrowych i BHP/ 1	Piętro I – Urząd Gminy Biskupiec	Biskupiec ul. Rynek 1 , 13-340 Biskupiec
Skarbnik	12	- Skarbnik Gminy Biskupiec/ 1	Piętro I – Urząd Gminy Biskupiec	Biskupiec ul. Rynek 1 , 13-340 Biskupiec
Sekretariat, Wójt	13	- Wójt Gminy Biskupiec/1 -Sekretarz Gminy /1 - inspektor ds. obsługi Rady Gminy i OSP /1	Piętro I – Urząd Gminy Biskupiec	Biskupiec ul. Rynek 1 , 13-340 Biskupiec
Magazyn, Serwerownia	14	-----	Piętro II – Urząd Gminy Biskupiec	Biskupiec ul. Rynek 1 , 13-340 Biskupiec
Archiwum Urzędu	15	-----	Piętro II – Urząd Gminy Biskupiec	Biskupiec ul. Rynek 1 , 13-340 Biskupiec
Archiwum GZOS	17	-----	Piętro II – Gminny Zespół Obsługi Szkół	Biskupiec ul. Rynek 1 , 13-340 Biskupiec
Archiwum Urzędu	18	-----	Piętro II – Urząd Gminy Biskupiec	Biskupiec ul. Rynek 1 , 13-340 Biskupiec
Fundusze Europejskie	19	- inspektor ds. funduszy unijnych /1	Piętro II – Urząd Gminy Biskupiec	Biskupiec ul. Rynek 1 , 13-340 Biskupiec

Rolnictwo, Leśnictwo	20	- inspektor ds. rolnictwa, gospodarki wodnej, inwestycji, obrony cywilnej, i dróg gminnych /1 - samodzielny referent ds. leśnictwa /1	Piętro II – Urząd Gminy Biskupiec	Biskupiec ul. Rynek 1 , 13-340 Biskupiec
Kierownik Gminnego Zespołu Obsługi Szkół	21	- Kierownik GZOS/ 1	Piętro II – Gminny Zespół Obsługi Szkół	Biskupiec ul. Rynek 1 , 13-340 Biskupiec
Gminny Zespół Obsługi Szkół	22	- główna księgowa /1 - starszy inspektor /2 - pracownik administracji /1	Piętro II – Gminny Zespół Obsługi Szkół	Biskupiec ul. Rynek 1 , 13-340 Biskupiec
Gminny Ośrodek Kultury	-----	-Dyrektor GOK /1	Gminny Ośrodek Kultury w Biskupcu	Biskupiec ul. Rynek 4, 13-340 Biskupiec
Gminna Biblioteka Samorządowa	-----	-Dyrektor Biblioteki /1 -Bibliotekarz /1	Gminny Ośrodek Kultury w Biskupcu	Biskupiec ul. Rynek 4, 13-340 Biskupiec

3. Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania danych osobowych i strukturą danych w zbiorze:

§ 6

1) Gminny Zespół Obsługi Szkół:

Zbiór danych osobowych	Program informatyczny służący do przetwarzania zbioru danych	Struktura danych w zbiorze
Baza pracowników	Radix Kadry+	id / pesel/ nip/ nazwisko/ imię/ drugie imię/ nazwisko rodowe/ imię ojca/ imię matki / nazwisko rodowe matki/ data urodzenia/ miejsce urodzenia/ data zgłoszenia/ data zmiany/ płeć/ stan cywilny/ adres[ulica, numer domu, numer lokalu, miejscowość, kod pocztowy, województwo, powiat, gmina, poczta, kod terytorialny, uwagi, kraj] / urząd skarbowy/ rodzaj dokumentu tożsamości/ numer i seria dokumentu tożsamości/ wystawca dokumentu tożsamości/ data wystawienia dokumentu tożsamości / dane o zatrudnieniu/ dane do ZUS/ informacje o rodzinie / wynagrodzenie, nr konta/ nazwa banku.
	Radix Płace+	pesel/ nip/ nazwisko/ imię/ drugie imię/ nazwisko rodowe/ imię ojca/ imię matki / nazwisko rodowe matki/ data urodzenia/ miejsce urodzenia/ data zgłoszenia/ data zmiany/ płeć/ stan cywilny/ adres[ulica, numer domu, numer lokalu, miejscowość, kod pocztowy, poczta, uwagi, kraj] / urząd skarbowy/ rodzaj dokumentu tożsamości/ numer i seria dokumentu tożsamości/ wystawca dokumentu tożsamości/ data wystawienia dokumentu tożsamości / dane o zatrudnieniu/ dane do ZUS/ informacje o rodzinie / wynagrodzenie, nr konta/ nazwa banku.
	Płatnik	nazwisko/ imię/ płeć/ PESEL/ NIP/ seria i nr dokumentu tożsamości/

		rodzaj dokumentu tożsamości/ data urodzenia/ status ubezpieczonego/ kod NFZ/ nazwa NFZ/ adres [miejscowość, ulica, nr domu, nr lokalu, kod pocztowy]/ telefon/ kod ubezpieczenia/ data ubezpieczenia/ kod wyrejestrowania/ podstawa wymiaru składki na ubezpieczenie emerytalne i rentowe/ podstawa wymiaru składki na ubezpieczenie chorobowe, wypadkowe i zdrowotne/ kwota składki na ubezpieczenie emerytalne rentowe, chorobowe, zdrowotne.
	System Finansowo – Księgowy Radix FKB+	dane wykazu kont [numer konta, nazwa konta, rodzaj/typ, Bo Wn, Bo Ma, plan, data] / dane do sprawozdań finansowych[miesiąc, rodzaj sprawozdania, rodzaj wykazu] / dane do dowodów księgowych[pozycja, znak, konto, kwota Wn, kwota Ma, opis operacji] / dane planu kont[konto, nazwa, rodzaj] / dane do planów finansowych[data, konto, zmiana Wn, zmiana Ma, kwota Wn, kwota Ma] / dane sprawozdań finansowych[sprawozdanie, symbol, nazwa]
	Bank BS	nazwisko / imię / adres / nr rachunku / zleceniodawca / kwota wynagrodzenia
Baza Kontrahentów	Przelewy COM	nazwa kontrahenta / nr konta / skrót / kod pocztowy / miasto
Baza Uczniów	SIO	Imię i nazwisko ucznia, imiona rodziców, PESEL, adres zamieszkania, dane szkoły do której uczęszcza

2) Gminny Ośrodek Pomocy Społecznej:

Zbiór danych osobowych	Program informatyczny służący do przetwarzania zbioru danych	Struktura danych w zbiorze
Baza ludności	Radix Świadczenia Rodzinne EZAR	Imię/ nazwisko/ data urodzenia/ płeć/ NIP/ PESEL/ stan cywilny/ numer i seria dowodu osobistego/ numer paszportu/ obywatelstwo/ dane do NFZ/ nazwa banku/ numer konta/ dane adresowe[miejscowość, ulica, nr domu, nr lokalu, kod pocztowy, poczta] / nr telefonu.
	Radix WIP+	PESEL/ imię/ nazwisko/ data urodzenia/ imię ojca/ imię matki/ dane adresowe[miejscowość, nr domu, nr lokalu, kod pocztowy, poczta]
	Radix FA+ (Fundusz Alimentacyjny)	Status/ numer konta/ nazwa konta/ data założenia/ data likwidacji/ pozycja
	Radix NDM+ (Dodatki Mieszkaniowe)	Imię/ nazwisko/ data urodzenia/ płeć/ NIP/ PESEL/ stan cywilny/ numer i seria dowodu osobistego/ numer paszportu/ obywatelstwo/ nazwa banku/ numer konta/ dane adresowe[miejscowość, ulica, nr domu, nr lokalu, kod pocztowy, poczta] / nr telefonu.

	POMOST (Pomoc Społeczna)	Dane rodziny[nr rodziny, nr teczki, nazwa rodziny, data rejestracji]/ Wyplaty[nr listy, data utworzenia, data wypłaty, status, sposób realizacji]/ Dane osobowe[nazwisko, imię, nazwisko rodowe, imiona rodziców, nazwisko rodowe matki, data urodzenia, płeć, PESEL, rodzaj dokumentu tożsamości, numer dok. toż., seria dok. toż., obywatelstwo] dane adresowe[miejscowość, ulica, nr domu, nr lokalu, kod pocztowy, poczta].
	Płatnik	nazwisko/ imię/ płeć/ PESEL/ NIP/ seria i nr dokumentu tożsamości/ rodzaj dokumentu tożsamości/ data urodzenia/ status ubezpieczonego/ kod NFZ/ nazwa NFZ/ adres [miejscowość, ulica, nr domu, nr lokalu, kod pocztowy]/ telefon/ kod ubezpieczenia/ data ubezpieczenia/ kod wyrejestrowania/ podstawa wymiaru składki na ubezpieczenie emerytalne i rentowe/ podstawa wymiaru składki na ubezpieczenie chorobowe, wypadkowe i zdrowotne/ kwota składki na ubezpieczenie emerytalne rentowe, chorobowe, zdrowotne.

3) Urząd Gminy Biskupiec:

Baza ludności	Puma (Ewidencja ludności)	Imię/ nazwisko/ nazwisko rodowe/ data urodzenia/ miejsce urodzenia/ data zgonu/ płeć/ imiona rodziców/ nazwisko rodowe matki/ PESEL/ rodzaj dokumentu tożsamości/ numer dok. toż./ seria dok. toż./ data wydania dokumentu tożsamości/ data unieważnienia dokumentu tożsamości/ obywatelstwo/ adres zamieszkania[miejscowość, ulica, nr domu, nr lokalu, kod pocztowy, poczta]/ kolor oczu/ rysopis/ uprawnienia wyborcze/ wykształcenie/ adres pobytu czasowego/ nr książeczki wojskowej/ stopień wojskowy/ nr aktu zgonu/ nr
---------------	----------------------------------	--

		<p>aktu urodzenia/ akty małżeństwa[nazwisko, imię, nazwisko rodowe, nazwisko z poprzedniego małżeństwa/ imiona rodziców, data urodzenia, miejsce urodzenia, akta urodzenia, data i nr USC / archiwalne dane osobowe (nazwisko, imię, nazwisko rodowe, nazwisko z poprzedniego małżeństwa) / adres zamieszkania lub pobytu stałego oraz data zameldowania/ archiwalne adresy zamieszkania lub pobytu stałego oraz data zameldowania/ adres czasowy lub okres pobytu czasowego/ archiwalne adresy czasowe lub okresy pobytu czasowego/ dokument tożsamości(rodzaj dokumentu, seria i numer dowodu, wystawca dokumentu)/ PESEL/ stan cywilny(imię i nazwisko współmałżonka, nazwisko rodowe i nazwisko z poprzedniego małżeństwa, data zawarcia małżeństwa, data wydania i wydający dokument tożsamości,)/ archiwalny stan cywilny(imię i nazwisko współmałżonka, nazwisko rodowe i nazwisko z poprzedniego małżeństwa)/ data wydania i wydający dokument tożsamości/ imiona i nazwiska rodowe/ narodowość/ obywatelstwo(data zmiany, podstawa prawna)/ adnotacje o rozwodzie.</p>
	<p>ESO USC</p>	<p>Akt małżeństwa[nazwisko, imiona, nazwisko rodowe, stan cywilny, data urodzenia, miejsce urodzenia, miejsce zamieszkania, data i miejsce zawarcia małżeństwa, dane dotyczące rodziców(nazwisko, imiona, nazwisko rodowe), nazwisko noszone po zawarciu małżeństwa(mężczyzna, kobieta, dzieci), świadkowie(nazwisko, imię)]/ / Akt urodzenia[nazwisko, imiona, płeć, data urodzenia, miejsce urodzenia, dane dotyczące rodziców(nazwisko, imiona, nazwisko rodowe, data urodzenia, miejsce urodzenia, miejsce zamieszkania), dane dotyczące osoby (zakładu) zgłaszającego urodzenie(nazwisko i imię(nazwa zakładu), miejsce zamieszkania(siedziba zakładu)/ Akt</p>

		Zgonu[nazwisko, imiona, nazwisko rodowe, stan cywilny, data urodzenia, ostatnie miejsce zamieszkania, dane dotyczące daty i miejsca zgonu(data zgonu, godzina zgonu, miejsce zgonu, data znalezienia zwłok, godzina znalezienia zwłok, miejsce znalezienia zwłok), dane dotyczące małżonka osoby zmarłej(nazwisko, imiona, nazwisko rodowe), dane dotyczące rodziców osoby zmarłej(imiona, nazwisko rodowe), dane dotyczące osoby(zakładu) zgłaszającej zgon(nazwisko i imię(nazwa zakładu), miejsce zamieszkania(siedziba zakładu))].
Baza ludności	EWOpis	Nazwisko/ imię/ imię ojca/ imię matki/ NIP/ PESEL/ dane dokumentu tożsamości/ dane adresowe[miejscowość, ulica, nr domu, nr lokalu, kod pocztowy, poczta]/ dane współmałżonka.
	CEiDG	Imię/ nazwisko/ nazwa działalności/ skrócona nazwa działalności/ data rozpoczęcia/ data likwidacji/ data zawieszenia/ data wznowienia/ adres zamieszkania/ adres wykonywania/ dodatkowy adres wykonywania/ dane kontaktowe/ zakres działalności (PKD)/ NIP/ REGON/ PESEL/ data zgłoszenia/ data wpisu/ nr ewidencyjny/ kraj pochodzenia.
	Radix WIP+	PESEL/ imię/ nazwisko/ data urodzenia/ imię ojca/ imię matki/ dane adresowe[miejscowość, nr domu, nr lokalu, kod pocztowy, poczta]
	Radix Pogrun+	Imię/ nazwisko/ data urodzenia/ imiona rodziców/ nazwisko rodowe matki/ PESEL/NIP/ regon/ kraj/ województwo/ powiat gmina/ adres zamieszkania[miejscowość, ulica, nr domu, nr lokalu, kod pocztowy, poczta].

Baza pracowników	Platnik	<p>nazwisko/ imię/ płeć/ PESEL/ NIP/ seria i nr dokumentu tożsamości/ rodzaj dokumentu tożsamości/ data urodzenia/ status ubezpieczonego/ kod NFZ/ nazwa NFZ/ adres</p> <p>[miejsowość, ulica, nr domu, nr lokalu, kod pocztowy]/ telefon/ kod ubezpieczenia/ data ubezpieczenia/ kod wyrejestrowania/ podstawa wymiaru składki na ubezpieczenie emerytalne i rentowe/ podstawa wymiaru składki na ubezpieczenie chorobowe, wypadkowe i zdrowotne/ kwota składki na ubezpieczenie emerytalne rentowe, chorobowe, zdrowotne.</p>
	Radix Kadry+	<p>Id/ pesel/ nip/ nazwisko/ imię/ drugie imię/ nazwisko rodowe/ imię ojca/ imię matki / nazwisko rodowe matki/ data urodzenia/ miejsce urodzenia/ data zgłoszenia/ data zmiany/ płeć/ stan cywilny/ adres[ulica, numer domu, numer lokalu, miejscowość, kod pocztowy, województwo, powiat, gmina, poczta, kod terytorialny, uwagi, kraj] / urząd skarbowy/ rodzaj dokumentu tożsamości/ numer i seria dokumentu tożsamości/ wystawca dokumentu tożsamości/ data wystawienia dokumentu tożsamości / dane o zatrudnieniu/ dane do ZUS/ informacje o rodzinie / wynagrodzenie/ dane książeczki wojskowej.</p>
	Radix Place+	<p>pesel/ nip/ nazwisko/ imię/ drugie imię/ nazwisko rodowe/ imię ojca/ imię matki / nazwisko rodowe matki/ data urodzenia/ miejsce urodzenia/ płeć/ stan cywilny/ adres[ulica, numer domu, numer lokalu, miejscowość, kod pocztowy, poczta, uwagi, kraj] / urząd skarbowy/ rodzaj dokumentu tożsamości/ numer i seria dokumentu tożsamości/ wystawca dokumentu tożsamości/ data wystawienia dokumentu tożsamości / dane o zatrudnieniu/ dane do ZUS/ informacje o rodzinie / wynagrodzenie, nr konta/ nazwa banku.</p>

4. Zbiory danych osobowych przetwarzanych tradycyjnie

§7

Zbiór danych osobowych	Lokalizacja zbioru danych osobowych (nr pomieszczenia)
Zestawienie wysyłanych i odbieranych przesyłek pocztowych	11
Dokumentacja pracownicza	11
Dokumentacja dotycząca spraw BHP	11
Ewidencja wyjazdów służbowych	11
Dokumenty CEiDG	11
Dokumentacja pracownicza	10
Zbiór naliczeń podatkowych	9
Zbiór wpłat podatkowych	9
Oświadczenia majątkowe radnych gminnych	13
Oświadczenia majątkowe	13
Decyzje zezwalające na wycinkę drzew	20
Rejestr osób przeznaczonych do pełnienia służby w formacjach obrony cywilnej	20
Ewidencja ludności	8
Rejestr osób posiadających kwalifikację wojskową	8
Rejestr osób posiadających obowiązek stawienia się do kwalifikacji wojskowej	8
Rejestr osób zobowiązanych do świadczeń rzeczowych i osobistych	8
Rejestr kurierów	8
Księgi stanu cywilnego (urodzeń, małżeństw, zgonów), akta zbiorowe do tych ksiąg	4
Rejestr dowodów osobistych	4
Świadczenia Rodzinne	2
Zaliczka alimentacyjna	2
Dodatki mieszkaniowe	2
Zbiór wysyłanych i odbieranych przesyłek pocztowych	2
Rejestr skarg i wniosków	2
Świadczenia pomocy społecznej	1
Dokumentacja pracownicza	22
Dokumentacja pracownicza nauczycieli i pracowników placówek oświatowych	22
Nadzór nad realizacją obowiązku szkolnego i obowiązku nauki	22
Arkusze organizacyjne szkół	22
Ewidencja nauczycieli ubiegających się o awans zawodowy na stopień nauczyciela mianowanego	22
Decyzje o warunkach zabudowy i zagospodarowania terenu	7
Ewidencja zbiorników bezodpływowych	7
Ewidencja przydomowych oczyszczalni ścieków	7
Ewidencja najemców komunalnych lokali mieszkalnych	7
Ewidencja osób ubiegających się o przydział lokalu komunalnego	7
Decyzje i postępowania o podziale i rozgraniczeniu nieruchomości	7
Decyzje przekształcenia wieczystego użytkowania na własność	7
Sprzedaż lokali komunalnych	7
Decyzje o ustaleniu inwestycji celu publicznego	7
Ewidencja wyrobów zawierających azbest	7

Decyzje ustalające jednorazową opłatę z tytułu wzrostu wartości zbywalnej nieruchomości	7
Numery porządkowe nieruchomości	7
Karty czytelników biblioteki (nazwisko, imię, rok urodzenia, adres, data zapisu)	Gminna Biblioteka Samorządowa w Biskupcu
Rejestr czytelników biblioteki (nazwisko, imię, data przerejestrowania, znak statystyczny)	Gminna Biblioteka Samorządowa w Biskupcu
Karty zapisu na czytelnika biblioteki (nazwisko, imię, data urodzenia, imię ojca, PESEL, zawód/uczeń, nr dokumentu tożsamości)	Gminna Biblioteka Samorządowa w Biskupcu
Rejestr osób korzystających z Internetu na terenie biblioteki (nazwisko, imię, data korzystania)	Gminna Biblioteka Samorządowa w Biskupcu

5. Sposób przepływu danych między poszczególnymi systemami

§8

KADRY -> PŁACE

Z programu **Radix Kadry+** do programu **Radix Place+** przekazywane są dane dotyczące danych osobowych, wynagrodzenia, płac zasadniczych i dodatków do płac pracowników.

Sposób przekazywania danych: manualny.

PŁACE -> PŁATNIK

Z programu **Radix Place+** do programu **Płatnik** przekazywane są dane dotyczące wynagrodzenia pracowników.

Sposób przekazywania danych: manualny.

KADRY -> PŁATNIK

Z programu **Radix Kadry+** do programu **Płatnik** przekazywane są dane osobowe i dane adresowe pracowników.

Sposób przekazywania danych: manualny.

PŁACE -> BANK BS BRODNICA

Z programu **Radix Place+** do **Bank BS Brodnica** przekazywane są dane dotyczące należnych kwot przelewanych na konto pracowników.

Sposób przekazywania danych: manualny.

POGRUN -> WIP

Z programu **Radix Pogrun+** do **Radix WIP** przekazywane są dane osobowe i dane dotyczące podatków.

Sposób przekazywania danych: manualny.

EWOPIS -> EWMAPA

Z programu **EWOpis** do **EWMapa** przekazywane są dane dotyczące opisu map.

Sposób przekazywania danych: automatyczny

WIP -> FA

Z programu **Radix WIP** do **Radix FA+** przekazywane są dane dotyczące dłużników alimentacyjnych.

Sposób przekazywania danych: manualny.

6. Określenie środków technicznych i organizacyjnych zapewniających bezpieczeństwo w przetwarzaniu danych

§9

Realizując Politykę Bezpieczeństwa Informacji Kierownictwo Urzędu, GOPS, GZOS, GOK i Biblioteki zapewnia ich:

- 1) **Poufność** – informacja nie jest udostępniana lub ujawniana nieautoryzowanym osobom, podmiotom lub procesom.
- 2) **Integralność** – dane nie zostają zmienione lub zniszczone w sposób nieautoryzowany.
- 3) **Dostępność** – dyspozycję do wykorzystania na żądanie, w założonym czasie, przez autoryzowany podmiot.
- 4) **Rozliczalność** – przypisanie działań danego podmiotu w sposób jednoznaczny tylko temu podmiotowi.
- 5) **Autentyczność** – zapewnienie, że tożsamość podmiotu lub zasobu jest taka, jak deklarowana (autentyczność dotyczy użytkowników, procesów, systemów i informacji).

§10

Polityka Bezpieczeństwa Informacji w Urzędzie, GOPS, GZOS, GOK i Bibliotece ma na celu zredukowanie możliwości wystąpienia negatywnych konsekwencji naruszeń w tym zakresie, tzn.:

- 1) Naruszeń danych o osobach rozumianych, jako ich dobro prywatne powierzone Urzędowi, GOPS, GZOS, GOK i Bibliotece.
- 2) Naruszeń przepisów prawa oraz innych regulacji.
- 3) Utraty lub obniżenia reputacji Urzędu, GOPS, GZOS, GOK lub Biblioteki mogącej mieć wpływ na ich wartość.
- 4) Strat finansowych w wyniku nałożonych kar lub utraty wiarygodności.
- 5) Zakłóceń czynności urzędowych spowodowanych nieprawidłowym działaniem systemów informatycznych lub prowadzeniem kontroli zewnętrznych na terenie Urzędu, GOPS, GZOS, GOK i Biblioteki.

A) Kompetencje i odpowiedzialność w zarządzaniu bezpieczeństwem danych osobowych

§11

Administrator Danych Osobowych (ADO)

1. Administratorem danych osobowych w Urzędzie Gminy Biskupiec jest Wójt Gminy Biskupiec.
2. Administrator powołuje Administratora Bezpieczeństwa Informacji (ABI), który w jego imieniu wykonuje określone zadania.

§12

Administrator Bezpieczeństwa Informacji (ABI)

1. Egzekwuje zgodne z prawem przetwarzanie danych osobowych w Urzędzie, GOPS, GZOS, GOK i Bibliotece w imieniu ADO.
2. Udziela upoważnień do przetwarzania danych osobowych określając ich zakres oraz termin ważności.
3. Prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych.
4. Prowadzi dokumentację opisującą sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zabezpieczenia danych osobowych – niniejsza polityka .
5. Ewidencjonuje oświadczenia osób upoważnionych do przetwarzania danych osobowych o zaznajomieniu się z zasadami zachowania ich bezpieczeństwa.

6. Przygotowuje projekty umów powierzania przetwarzania danych osobowych innemu podmiotowi
7. Udziela wyjaśnień i interpretuje zgodność stosowanych rozwiązań w zakresie ochrony danych osobowych z przepisami prawa.
8. Obsługuje kontrolę oraz współpracę z podmiotami zewnętrznymi uprawnionymi do dostępu do danych osobowych przetwarzanych w Urzędzie, GOPS, GZOS, GOK i Bibliotece.
9. Bierze udział w podnoszeniu świadomości oraz kwalifikacji osób przetwarzających dane osobowe w Urzędzie, GOPS, GZOS, GOK i Bibliotece w zakresie problematyki bezpieczeństwa tych danych, w tym zapewnia odpowiedni poziom przeszkolenia pracowników w zakresie ochrony danych osobowych.
10. Wydaje zalecenia dla pracowników przetwarzających dane (PPD) w zakresie podwyższenia standardów zabezpieczeń danych osobowych.
11. Kontroluje procesy udostępniania danych osobowych.
12. Współpracuje z Administratorem Systemu Informatycznego w zakresie nadzoru i kontroli nad bezpieczeństwem systemu informatycznego, w którym przetwarzane są dane osobowe.
13. Przeprowadza kontrolę stanu zabezpieczeń fizycznych i technicznych obszaru przetwarzania danych.
14. Podejmuje działania zgodne z obowiązującymi w Urzędzie, GOPS, GZOS i Bibliotece procedurami w sytuacji naruszenia ochrony danych osobowych.

§13

Administrator Systemu Informatycznego (ASI)

1. Zarządza bezpieczeństwem przetwarzania danych osobowych w systemie informatycznym zgodnie z wymogami prawa i wskazówkami ABI.
2. Doskonali i rozwija metody zabezpieczenia danych przed zagrożeniami związanymi z ich przetwarzaniem, szczególnie w zakresie dotyczącym dynamicznego rozwoju metod i technik przetwarzania tych danych w systemach informatycznych oraz sieciach telekomunikacyjnych.
3. Przydziela identyfikatory użytkownikom systemu informatycznego oraz zaznaja im ich z procedurami ustalania i zmiany haseł dostępu.
4. Nadzoruje prace związane z rozwojem, modyfikacją, serwisowaniem i konserwacją systemu informatycznego.
5. Zapewnia bezpieczeństwo wewnętrznego i zewnętrznego obiegu informacji w sieci i zabezpieczenie łączy zewnętrznych.
6. Prowadzi nadzór nad wykonywaniem kopii awaryjnych, ich przechowywaniem oraz okresowym sprawdzaniem pod kątem ich dalszej przydatności do odtworzenia danych w przypadku awarii systemu.
7. Prowadzi nadzór nad archiwizacją zbiorów danych oraz zabezpiecza elektroniczne nośniki informacji zawierających dane osobowe.
8. Zapewnia bezawaryjny system zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych osobowych w Urzędzie, GOPS, GZOS, GOK i Bibliotece.

§14

Pracownik przetwarzający dane (PPD)

1. Chroni prawo do prywatności osób fizycznych powierzających Urzędowi, GOPS, GZOS, GOK i Bibliotece swoje dane osobowe poprzez skuteczną ochronę tych danych, w zgodzie z przepisami prawa oraz zasadami Polityki Bezpieczeństwa Informacji oraz Instrukcji Zarządzania Systemem Informatycznym obowiązujących w Urzędzie, GOPS, GZOS, GOK i Bibliotece.

B) Zasady udzielania dostępu do danych osobowych

§15

Dostęp do danych osobowych może mieć wyłącznie osoba zaznajomiona z zasadami ich ochrony zawartymi w Polityce Bezpieczeństwa Informacji i Instrukcji Zarządzania Systemem Informatycznym. Za zaznajomienie osoby z tymi zasadami odpowiedzialny jest ABI. Osoba zaznajomiona z zasadami ochrony danych osobowych obowiązujących w Urzędzie, GOPS, GZOS, GOK i Bibliotece potwierdza to w pisemnym **oświadczeniu** zgodnie ze wzorem w *załączniku nr 1*, stanowiącym integralną część niniejszego dokumentu.

§16

Dostęp do danych osobowych może mieć wyłącznie osoba posiadająca pisemne oraz imienne **upoważnienie** wydane przez ABI, zgodnie ze wzorem w *załączniku nr 2*, stanowiącym integralną część niniejszego dokumentu.

§17

ABI może wyznaczać uprawnionych do przetwarzania danych osobowych pracowników Urzędu, GOPS, GZOS, GOK i Biblioteki do nadzoru nad upoważnionymi pracownikami podmiotów zewnętrznych lub innymi osobami przetwarzającymi dane osobowe w Urzędzie, GOPS, GZOS, GOK i Bibliotece w ramach prowadzonej działalności.

§18

Upoważnienia dla pracowników Urzędu, GOPS, GZOS, GOK i Biblioteki wydawane są na pisemny wniosek ich przełożonego.

§19

Upoważnienie do dostępu do systemu informatycznego dla pracowników podmiotów zewnętrznych wykonujących prace zlecone (np. konserwacje) wydawane są na wniosek ASI.

C) Bezpieczeństwo w przetwarzaniu danych osobowych w formie tradycyjnej

§20

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 przetwarzane zbiory danych osobowych musi być poprzedzone przeniesieniem zbioru danych lub jego części do odpowiednio zabezpieczonego miejsca jego przechowywania oraz, przy planowanej dłuższej nieobecności, wiązać się z zamknięciem drzwi pomieszczenia na klucz.

Klucze do pomieszczeń wydawane są jedynie pracownikom upoważnionym do przetwarzania danych osobowych w zakresie zgodnym z kategorią danych.

Korzystanie ze zbiorów danych przez osoby niezatrudnione w Urzędzie, GOPS, GZOS, GOK czy Bibliotece powinno odbywać się po zweryfikowaniu upoważnienia udzielonego tej osobie lub skonsultowane z ABI w przypadku przedstawicieli instytucji upoważnionych do przetwarzania tych danych na podstawie ogólnie obowiązujących przepisów.

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 czasu ich przydatności są niszczone przy użyciu niszczarek.

D) Bezpieczeństwo w przetwarzaniu danych osobowych w systemach informatycznych

§21

Zasady bezpiecznego użytkowania systemu informatycznego zawarte są w załączniku nr 3: „Instrukcja Zarządzania Systemem Informatycznym”, która jest integralną częścią dokumentacji Urzędu. GOPS, GZOS, GOK i Biblioteki w zakresie ochrony danych osobowych, obowiązkową do zapoznania się i stosowania przez wszystkich użytkowników systemu informatycznego.

7. Analiza ryzyka związanego z przetwarzaniem danych osobowych

Zagrożenia:

§22

Forma przetwarzania danych	Przykładowe zagrożenia
Dane przetwarzane w sposób tradycyjny	<ul style="list-style-type: none">– oszustwo, kradzież, sabotaż,– zaniedbania pracowników (udostępnienie danych osobom nieupoważnionym, niedyskrecja)– obecność nieupoważnionych osób w obszarze przetwarzania danych,– podsłuchy, podglądy,– ataki terrorystyczne,– brak rejestrowania udostępniania danych,– niewłaściwe miejsce przetwarzania danych,– zdarzenia losowe (powódź, pożar).
Dane przetwarzane w systemie informatycznym	<ul style="list-style-type: none">– dostanie się do systemu złośliwego oprogramowania,– niewłaściwa administracja systemu,– kradzież haseł i identyfikatorów,– zdarzenia losowe (powódź, pożar),– obecność nieupoważnionych osób w obszarze przetwarzania danych,– zaniedbania pracowników (udostępnienie danych osobom nieupoważnionym, niedyskrecja),– naprawy systemu informatycznego, sprzętu, i sieci przez osoby nieuprawnione,– przypadkowe bądź celowe zmiany/ uszkodzenia w aplikacjach informatycznych,– przypadkowe bądź celowe wprowadzanie zmian do chronionych danych osobowych,– niekontrolowane podłączenie zewnętrznych nośników informacji do komputera.

Zapobieganie:

§23

Forma przetwarzania danych	Przykładowe stosowane środki zapobiegawcze
Dane przetwarzane w sposób tradycyjny	<ul style="list-style-type: none">- - przechowywanie danych w pomieszczeniach i szafach zamkniętych na klucz,- - zastosowanie monitoringu obserwującego wejście do budynku,- - przetwarzanie danych wyłącznie przez osoby posiadające upoważnienie wydane przez ABI,- - zapoznanie pracowników z zasadami przetwarzania danych osobowych oraz obsługą sprzętu służącego do ich przetwarzania.
Dane przetwarzane w systemie informatycznym	<ul style="list-style-type: none">- - zastosowanie programów antywirusowych i innych narzędzi chroniących system informatyczny przed atakiem złośliwego oprogramowania,- - systematyczne tworzenie kopii zapasowych,- - przechowywanie nośników danych w dobrze zabezpieczonych pomieszczeniach i szafach,- - zabezpieczenie pomieszczenia serwerowni,- - właściwa budowa hasła do systemu,- - przydzielanie każdemu użytkownikowi indywidualnego unikalnego identyfikatora i hasła,- - kontrola dostępu do systemów,

8. Odpowiedzialność karna

§24

Przetwarzanie danych osobowych niezgodnie z prawem, 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, bądź może zostać uznane za ciężkie naruszenie podstawowych obowiązków pracowniczych i skutkować odpowiedzialnością dyscyplinarną.

WÓJT

Tomaszowski

Wzór oświadczenia o zachowaniu poufności i zapoznaniu się z przepisami.

**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 Urzędzie Gminy, Gminnym Ośrodku Pomocy Społecznej i Gminnym Zespole Obsługi Szkół w Biskupcu, a dotyczących ochrony danych osobowych. W szczególności oświadczam, że bez upoważnienia nie będę wykorzystywał(a) danych osobowych ze zbiorów znajdujących się w Urzędzie, GOPS i GZOS. Oświadczam, że zostałem(am) poinformowany(a) o obowiązujących w Urzędzie, GOPS i GZOS zasadach, dotyczących przetwarzania danych osobowych, określonych w „Polityce Bezpieczeństwa Informacji”

Oświadczam, że zostałem(am) zapoznany(a) z przepisami Ustawy o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 ze zm.) 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 Urzędzie, GOPS i GZOS może zostać uznane za ciężkie naruszenie podstawowych obowiązków pracowniczych i skutkować odpowiedzialnością dyscyplinarną.

..... dn. r.

miejsce i data złożenia oświadczenia

.....
czytelny podpis osoby składającej oświadczenie

Wzór upoważnienia do przetwarzania danych osobowych.

**UPOWAŻNIENIE NR / 2013
do przetwarzania danych osobowych**

Działając na podstawie uprawnień nadanych mi przez Urząd Gminy, Gminny Ośrodek Pomocy Społecznej, Gminny Zespół Obsługi Szkół, Gminny Ośrodek Kultury i Gminną Bibliotekę Samorządową w Biskupcu, w sprawie ochrony danych osobowych, upoważniam

Panią / Pana:

Do przetwarzania danych osobowych w systemach informatycznych/ nieinformatycznych funkcjonujących w Urzędzie Gminy, Gminnym Ośrodku Pomocy Społecznej, Gminnym Zespole Obsługi Szkół, Gminnym Ośrodku Kultury i Gminnej Bibliotece Samorządowej w Biskupcu służących do przetwarzania danych osobowych zawartych w zbiorze centralnym / rozproszonym noszącym nazwę

.....
.....

Wyżej wymieniona osoba została zapoznana z obecnie obowiązującymi przepisami dotyczącymi ochrony danych osobowych i dopuszczona jest do ich przetwarzania jedynie w zakresie określonym w obowiązkach służbowych i zgodnie z Ustawą z dnia 29.08.1997r o ochronie danych osobowych (tekst jednolity Dz. U z roku 2002 nr 101 poz.926) i wydanych do niej przepisach wykonawczych oraz w Zarządzeniu Wójta Gminy Biskupiec Nr 80/2012 w sprawie ochrony danych osobowych.

Wymieniona osoba została wpisana do ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych w Urzędzie Gminy w Biskupcu.

.....
podpis osoby wystawiającej upoważnienie

.....
data i czytelny podpis osoby upoważnionej

INSTRUKCJA POSTĘPOWANIA W SYTUACJI NARUSZENIA DANYCH OSOBOWYCH

ROZDZIAŁ I Informacje ogólne

§1

Celem instrukcji jest określenie sposobu działania, gdy:

- a. stwierdzono naruszenie zabezpieczenia systemu informatycznego w obszarze danych osobowych.
- b. stan urządzenia, zawartość zbioru danych osobowych, ujawnienie metody pracy, sposób działania programu lub jakość komunikacji w sieci komputerowej mogą wskazywać na naruszenie bezpieczeństwa danych osobowych.

§2

Instrukcja określa zasady postępowania wszystkich osób zatrudnionych przy przetwarzaniu danych osobowych w systemach informatycznych / nieinformatycznych zgodnie z tabelą naruszeń.

§3

Naruszeniem zabezpieczenia systemu informatycznego, przetwarzającego dane osobowe 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:

- a. nieautoryzowany dostęp do danych,
- b. nieautoryzowane modyfikacje lub zniszczenie danych,
- c. udostępnienie danych nieautoryzowanym podmiotom,
- d. nielegalne ujawnienie danych,
- e. pozyskiwanie danych z nielegalnych źródeł.

ROZDZIAŁ II

Postępowanie w przypadku naruszenia zabezpieczenia systemu informatycznego

§4

W przypadku stwierdzenia naruszenia zabezpieczenia systemu informatycznego lub zaistnienia sytuacji, które mogą wskazywać na naruszenie zabezpieczenia danych osobowych, każdy pracownik zatrudniony przy przetwarzaniu danych osobowych w Urzędzie Gminy Biskupiec, Gminnym Ośrodku Pomocy Społecznej, Gminnym Zespole Obsługi Szkół, Gminnym Ośrodku Kultury i Gminnej Bibliotece Samorządowej w Biskupcu **jest zobowiązany przerwać przetwarzanie danych osobowych i niezwłocznie powiadomić o tym fakcie Administratora Bezpieczeństwa Informacji (lub osobę przez niego upoważnioną), a następnie postępować stosownie do podjętej przez niego decyzji.**

Zgłoszenie naruszenia ochrony danych osobowych powinno zawierać:

- a. opisanie symptomów naruszenia ochrony danych osobowych,
- b. określenie sytuacji i czasu, w jakim stwierdzono naruszenie ochrony danych osobowych,
- c. określenie wszelkich istotnych informacji mogących wskazywać na przyczynę naruszenia,

- d. określenie znanych danej osobie sposobów zabezpieczenia systemu oraz wszelkich kroków podjętych po ujawnieniu zdarzenia.

§5

Administrator bezpieczeństwa Informacji lub inna upoważniona przez niego osoba podejmuje wszelkie działania mające na celu:

- a. minimalizację negatywnych skutków zdarzenia,
- b. wyjaśnienie okoliczności zdarzenia,
- c. zabezpieczenia dowodów zdarzenia,
- d. umożliwienie dalszego bezpiecznego przetwarzania danych.

§6

W celu realizacji zadań niniejszej instrukcji ABI lub inna upoważniona przez niego osoba, ma prawo do podejmowania wszelkich działań dopuszczonych przez prawo, a w szczególności:

- a. żądania wyjaśnień od pracowników,
- b. korzystania z pomocy konsultantów,
- c. nakazanie przerwania pracy, zwłaszcza w zakresie przetwarzania danych osobowych.

§7

Polecenia ABI wydawane w czasie realizacji wynikających z niniejszej instrukcji są priorytetowe i powinny być wykonywane w pierwszej kolejności, zapewniając ochronę danych osobowych.

§8

Odmowa udzielenia wyjaśnień lub współpracy z ABI traktowana będzie, jako **naruszenie obowiązków pracowniczych**.

§9

ABI po zażegnaniu sytuacji nadzwyczajnej opracowuje raport końcowy (*w załączniku nr 1*), w którym przedstawia przyczyny i skutki zdarzenia oraz wnioski, w tym kadrowe, ograniczające możliwość wystąpienia zdarzenia w przyszłości.

ROZDZIAŁ III

Sankcje

§10

Nieprzestrzeganie zasad określonych w niniejszej instrukcji stanowi naruszenie obowiązków pracowniczych i może być przyczyną odpowiedzialności dyscyplinarnej określonej w Kodeksie Pracy.

§11

Jeżeli skutkiem działania określonego w §10 jest ujawnienie informacji osobie nieupoważnionej, sprawca może zostać pociągnięty do odpowiedzialności karnej wynikającej z przepisów Kodeksu Karnego.

§12

Jeżeli skutkiem działania określonego w §10 jest szkoda, sprawca ponosi odpowiedzialność materialną na warunkach określonych w Kodeksie Pracy oraz Prawa Cywilnego.

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

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM, W KTÓRYM PRZETWARZANE SĄ DANE OSOBOWE

I. Wstęp

Za poprawność realizacji zasad zarządzania systemem informatycznym odpowiada Administrator Systemu Informatycznego.

Celem Instrukcji Zarządzania Systemem Informatycznym jest zapewnienie bezpieczeństwa danych osobowych przetwarzanych w Urzędzie Gminy, Gminnym Ośrodku Pomocy Społecznej, Gminnym Zespole Obsługi Szkół, Gminnym Ośrodku Kultury i Gminnej Bibliotece Samorządowej w Biskupcu oraz minimalizowanie incydentów mogących zagrozić bezpieczeństwu systemu.

II. Nadawanie i rejestrowanie uprawnień do przetwarzania danych osobowych w systemie informatycznym

1. Każdy użytkownik systemu informatycznego przed przystąpieniem do przetwarzania danych osobowych musi zapoznać się z:
 - a. polityką bezpieczeństwa informacji w Urzędzie, GOPS, GZOS, GOK i Bibliotece
 - b. niniejszym dokumentem
2. Każdy użytkownik systemu informatycznego potwierdza zapoznanie się z powyższymi dokumentami własnoręcznym podpisem na **Oświadczeniu o zachowaniu poufności i zapoznaniu się z przepisami**, oraz posiada **Upoważnienie do przetwarzania danych osobowych** (załączniki 1 i 2 w PBI) wydane przez ABI.
3. Tworzenie kont użytkowników, nadawanie im uprawnień oraz ich modyfikacje realizuje Administrator Systemu Informatycznego.
4. Usuwanie kont stosowanie jest jedynie w uzasadnionych przypadkach, standardowo, przy ustaniu potrzeby utrzymywania konta danego użytkownika ulega ono dezaktywacji w celu zachowania historii jego aktywności.
5. Osoby które zostały uprawnione do przetwarzania danych osobowych są zobowiązane do zachowania tajemnicy w zakresie tych danych oraz sposobu ich zabezpieczenia, obowiązek ten istnieje również po ustaniu stosunku pracy, co jest równoważne z cofnięciem uprawnień do przetwarzania danych osobowych.
6. Po zakończeniu zatrudnienia danego użytkownika ABI uaktualnia ewidencję pracowników upoważnionych do przetwarzania danych osobowych i przekazuje informację do ASI w celu uaktualnienia rejestru użytkowników.

III. Metody i środki uwierzytelniania użytkowników systemu informatycznego

1. Przyznanie użytkownikowi dostępu do systemu informatycznego polega na zalogowaniu się indywidualnym identyfikatorem i hasłem.
2. Hasło przydziela i przekazuje użytkownikowi w formie ustnej Administrator Systemu Informatycznego.
3. Użytkownik po otrzymaniu hasła jest zobowiązany do jego niezwłocznej zmiany zgodnie z wymogami stopnia złożoności adekwatnymi do poziomu zabezpieczenia danego systemu o którym informuje go ASI. Standardowo hasło powinno składać się z 8 znaków i zawierać wielkie i małe litery, cyfry oraz znaki specjalne.
4. Hasło nie może być zmieniane, zapisywane lub przechowywane w miejscu dostępnym dla osób do tego uprawnionych.
5. W przypadku zagubienia hasła użytkownik musi skontaktować się z ASI w celu uzyskania nowego hasła.

6. Standardowa częstotliwość zmiany hasła to 1 miesiąc, użytkownik o potrzebie zmiany hasła jest informowany przez ASI.

IV. Zasady bezpieczeństwa podczas pracy w systemie informatycznym

1. Kroki podejmowane w celu uruchomienia systemu informatycznego:
 - 1.1. zalogowanie się do systemu operacyjnego, poprzez wpisanie indywidualnego identyfikatora i hasła.
 - 1.2. uruchomienie programu przetwarzającego dane osobowe przez użytkownika autoryzowane jest poprzez nadane uprawnienia.
 - 1.3. zalogowanie do niektórych programów i systemów wymaga dodatkowego wprowadzenia unikalnego identyfikatora i hasła.
2. W sytuacji tymczasowego zaprzestania pracy na skutek opuszczenia stanowiska należy uniemożliwić osobom postronnym korzystanie z systemu informatycznego, np. poprzez zablokowanie systemu operacyjnego klawiszami: ctrl + alt + delete i wybór opcji „Zablokuj”, poprzez całkowite wylogowanie się z systemu lub zamknięcie na klucz drzwi do opuszczonego pomieszczenia, w którym znajduje się komputer z uruchomionym systemem.
3. W sytuacji, gdy wgląd w wyświetlane na monitorze dane może mieć osoba nieuprawniona, należy tymczasowo zmienić widok wyświetlany na monitorze, obrócić monitor lub przykryć ekran laptopa.
4. Przed wyłączeniem komputera, należy zamknąć programy przetwarzające dane osobowe oraz wylogować się z systemu operacyjnego.
5. W sytuacji podejrzenia naruszenia bezpieczeństwa systemu, braku możliwości zalogowania się na konto przypisane do użytkownika lub stwierdzenia fizycznej ingerencji w przetwarzane dane bądź użytkowane narzędzia programowe lub sprzętowe należy niezwłocznie powiadomić ASI.
6. Przykładowe elementy, które mogą wskazywać na naruszenie zabezpieczeń systemu informatycznego:
 - 6.1. nietypowy stan stacji roboczej (np. brak zasilania, problemy z uruchomieniem, naruszona obudowa) .
 - 6.2. różnice w funkcjonowaniu systemu (np. komunikaty o błędach, nieprawidłowości w wykonywanych operacjach, brak dostępu do programów bądź funkcji).
 - 6.3. różnice w zawartości zbioru danych osobowych(brak lub nadmiar danych).

V. Tworzenie kopii danych w systemie informatycznym

Rodzaj danych	Częstotliwość tworzenia kopii	Okres przechowywania	Metoda kopiowania	Rodzaj nośnika	Metoda likwidacji danych na nośniku
Wszystkie bazy danych	Codziennie	2 lata	Kopia całościowa	Dyski twarde, płyty dvd, QNAP NAS	Bezpieczne kasowanie i nadpisywanie

VI. Tworzenie kopii programów służących do przetwarzania danych osobowych

Rodzaj programu	Częstotliwość tworzenia kopii	Okres przechowywania	Metoda kopiowania	Rodzaj nośnika	Metoda likwidacji danych na nośniku
Wszystkie programy w których przetwarzane są dane osobowe	Raz w miesiącu lub każdorazowo przed aktualizacją	nieograniczony	Kopia całościowa	Server i QNAP NAS	Bezpieczne kasowanie

VII. Przechowywanie elektronicznych nośników informacji zawierających dane osobowe

1. Płyty CD, DVD , Dyski Twarde, zawierające dane osobowe, kopie danych, kopie zapasowe, są przechowywane w pomieszczeniu zabezpieczonym przed dostępem osób nieupoważnionych w szafie pancernej zamkniętej na klucz.
2. W przypadku likwidacji stacji roboczej, dyski twarde, które zawierają dane osobowe są uszkodzane w sposób uniemożliwiający odczyt tych danych.
3. Nadzór nad archiwizacją danych, kopiami zapasowymi pełni Administrator Systemu Informatycznego.
4. Nadzór na prawidłowości zabezpieczenia elektronicznych nośników informacji zawierających dane osobowe wdrażanych przez ASI prowadzi ABI.

VIII. Zabezpieczenie systemu informatycznego przed działalnością niepożądanego oprogramowania.

1. Na każdym komputerze i serwerze w Urzędzie, GOPS, GZOS, GOK i Bibliotece zainstalowane jest licencjonowane oprogramowanie antywirusowe, włączona jest również zaporę Firewall, zadaniem tych narzędzi jest przeciwdziałanie złośliwemu oprogramowaniu.
2. Obszary systemu informatycznego narażone na ingerencję złośliwego oprogramowania, to całość oprogramowania funkcjonującego w Urzędzie, GOPS, GZOS, GOK i Bibliotece.
3. Możliwe źródła przedostania się złośliwego oprogramowania to:
 - Internet,
 - nieautoryzowane nośniki danych.
4. Działania podejmowane w kierunku zminimalizowania możliwości zainstalowania się szkodliwego oprogramowania do systemu to m. in. :
 - nadzór zewnętrznych nośników danych wkładanych do komputera (nieużywanie nieautoryzowanych nośników),
 - ograniczenie korzystania z uprawnień administracyjnych(jedynie w uzasadnionych przypadkach),
 - nadzór nad aktualizacjami oprogramowania antywirusowego.
5. W przypadku wystąpienia na monitorze komputera komunikatu o wykryciu wirusa lub podobnych nieprawidłowościach należy niezwłocznie poinformować o tym ASI. Do czasu weryfikacji stopnia zagrożenia i/lub jego zniwelowania należy wstrzymać się od dalszej pracy na komputerze.

IX. Rejestracja zdarzeń udostępniania danych osobowych

1. Każda osoba fizyczna, której dane przetwarzane są w Urzędzie, GOPS, GZOS, GOK i Bibliotece ma prawo zwrócić się z wnioskiem o udzielenie informacji związanych z przetwarzaniem tych danych, prawo do kontroli swoich danych osobowych, 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 .

X. Przeglądy i konserwacje systemów oraz nośników informacji służących do przetwarzania danych

1. Przeglądy i konserwacje systemu informatycznego są prowadzone na bieżąco przez ASI .
2. W przypadku stwierdzenia uszkodzenia urządzenia, dyski i inne informatyczne nośniki danych zawierające dane osobowe, przed ich przekazaniem w celu naprawy innemu podmiotowi, pozbawiane są zawartości.