Projekt

ZARZĄDZENIE NR .....
WÓJTA GMINY ŚNIADOWO

z dnia ..... 2020 r.

w sprawie wdrożenia środków technicznych i organizacyjnych przetwarzania danych osobowych w Urzędzie Gminy Śniadowo

Na podstawie art.24 ust.1 i 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119 s.1) zarządzam, co następuje:

§ 1. Wdrażam „Politykę bezpieczeństwa danych osobowych" stanowiącą Załącznik nr 1 do niniejszego zarządzenia.

§ 2. Wdrażam „Politykę bezpieczeństwa informacji" stanowiącą Załącznik nr 2 do niniejszego zarządzenia.

§ 3. Wyznaczam Pana Michała Kamińskiego - informatyka na Administratora Systemów Informatycznych.

§ 4. Upoważnienia do przetwarzania danych osobowych nadane przez Wójta na podstawie dotychczas obowiązujących przepisów, zachowują swoją moc do czasu nadania nowych upoważnień.

§ 5. Wykonanie zarządzenia powierzam Inspektorowi Ochrony Danych.

§ 6. Traci moc Zarządzenie Nr 77.2015 Wójta Gminy Śniadowo z dnia 3 grudnia 2015 r. w sprawie wprowadzenia dokumentacji opisującej sposób przetwarzania danych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzania danych osobowych w Urzędzie Gminy Śniadowo.

§ 7. Zarządzenie wchodzi w życie z dniem podpisania.

Załącznik Nr 1 do zarządzenia Nr .....
Wójta Gminy Śniadowo
z dnia ..... 2020 r.

POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

§ 1

Przedmiot

W celu ochrony podstawowych praw i wolności osób fizycznych, w szczególności prawa do ochrony danych osobowych, w związku przetwarzaniem danych osobowych, URZĄD GMINY ŚNIADOWO wdraża dokument o nazwie **„Polityka bezpieczeństwa danych osobowych”.**

§ 2

Cel

Podstawowym celem przygotowania i wdrożenia „Polityki bezpieczeństwa danych osobowych” w Urzędzie Gminy Śniadowo jest zapewnienie zgodności działania z obowiązującymi przepisami prawa w zakresie ochrony danych osobowych, w tym w szczególności z:

1. Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119, s. 1);
2. Ustawą z dnia 10 maja 2018 roku o ochronie danych osobowych (Dz.U. 2019 r. poz. 1781).

§ 3

Zakres polityki bezpieczeństwa danych osobowych

1. Polityka bezpieczeństwa danych osobowych w Urzędzie Gminy Śniadowo określa zasady przetwarzania danych osobowych oraz środki techniczne i organizacyjne zastosowane do przetwarzania danych osobowych, a także jest elementem systemu zarządzania bezpieczeństwem informacji.
2. Polityka dotyczy danych osobowych osób fizycznych przetwarzanych niezależnie

od formy ich przetwarzania (zbiory tradycyjne, systemy informatyczne).

3. Polityka ma zastosowanie wobec wszystkich komórek organizacyjnych, samodzielnych stanowisk pracy i wszystkich procesów przebiegających w ramach przetwarzania danych osobowych.
4. Polityka zapewnia przetwarzanie danych osobowych zgodne z przepisami oraz ich ochronę przed udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów określających zasady postępowania przy przetwarzaniu danych osobowych oraz przed uszkodzeniem, zniszczeniem lub nieupoważnioną zmianą.
5. Ze względu na nieustannie zmieniające się okoliczności przetwarzania danych osobowych, niniejsza polityka jest dokumentem dynamicznie zmieniającym się w czasie. W celu utrzymania aktualności i ciągłości Polityki Bezpieczeństwa Danych Osobowych, dokumenty stanowiące integralną część Polityki będą aktualizowane na bieżąco i nie będą wymagały zmiany Zarządzenia w tym zakresie.

§ 4

Zastosowane skróty i definicje oznaczają

1. **Polityka** - oznacza niniejszą Politykę bezpieczeństwa danych osobowych, o ile co innego nie wynika wyraźnie z kontekstu.
2. **RODO -** oznacza rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119, s. 1).
3. **Ustawa** – ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. 2019, poz. 1781).
4. **Administrator** – oznacza Wójta Gminy Śniadowo, ul. Ostrołęcka 11, 18-411 Śniadowo.
5. **IOD** – oznacza Inspektora Ochrony Danych wyznaczanego przez Administratora.
6. **Administrator Systemów Informatycznych (ASI)** – oznacza informatyka, (pracownika) wyznaczanego przez Administratora, który odpowiedzialny jest za funkcjonowanie i zabezpieczenie systemów informatycznych oraz stosowanie środków technicznych i organizacyjnych ochrony stosowanych w tych systemach;
7. **Dane osobowe** - oznaczają informacje o zidentyfikowanej lub możliwej do

zidentyfikowania osobie fizycznej ("osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;

8. **Dane szczególne** - oznaczają dane wymienione w art. 9 ust. 1 RODO, tj. dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej.
9. **Zbiór danych** - oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;
10. **Przetwarzanie** - oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie,wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;
11. **Podmiot przetwarzający** - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;
12. **Rejestr -** oznacza Rejestr Czynności Przetwarzania Danych Osobowych.
13. **Urząd** – oznacza Urząd Gminy Śniadowo.
14. **Organ nadzorczy** – Urząd Ochrony Danych Osobowych.
15. **Odbiorca danych osobowych** - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z

prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania.

§ 5

Polityka zawiera

1. Wykaz budynków, pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe, określony w **zał. Nr 1** do Polityki;
2. Rejestr Czynności Przetwarzania Danych Osobowych, określony w **zał. Nr 2** do Polityki.
3. Obowiązki informacyjne, zasady zawierania umów powierzenia przetwarzanych danych a także przekazywanie danych dla odbiorców.

§ 6

Odpowiedzialnymi za przetwarzanie danych osobowych w Urzędzie są:

1.Administrator;

2.Inspektor Ochrony Danych;

3.Administrator Systemów Informatycznych;

4.Kierownicy Referatów;

5.Pracownicy bądź inne osoby mające upoważnienie Administratora do przetwarzania danych osobowych.

§ 7

Obowiązki i zadania osób odpowiedzialnych za przetwarzanie danych osobowych:

1. **Administrator** jest odpowiedzialny za wdrożenie środków technicznych i organizacyjnych związanych z przetwarzaniem danych osobowych oraz odpowiednich polityk ochrony danych.
2. **Inspektor Ochrony Danych**:
   a) informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;
   b) monitorowanie przestrzegania niniejszego rozporządzenia, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu

uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;

c) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35 RODO;
d) współpraca z organem nadzorczym;
e) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 RODO, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.

3. **Administrator Systemów Informatycznych**:
   a) nadzór nad nadawaniem uprawnień do przetwarzania danych osobowych w systemach informatycznych;
   b) prowadzenie i aktualizacja rejestru nadanych uprawnień do przetwarzania danych w systemach informatycznych;
   c) nadzór nad stosowaniem środków zapewniających bezpieczeństwo przetwarzania danych osobowych w systemach informatycznych, a w szczególności przeciwdziałających dostępowi osób niepowołanych do tych systemów
   d) podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń;
   e) identyfikacja i analiza zagrożeń oraz ocena ryzyka, na które może być narażone przetwarzanie danych osobowych w systemach informatycznych;
   f) wykonywanie kopii zapasowych systemów oraz sprawowanie nadzoru nad ich przechowywaniem,
   g) podejmowanie innych czynności w zakresie zabezpieczenia przetwarzania danych w systemach informatycznych.
4. **Kierownicy referatów:**
   a) nadzór nad przestrzeganiem zasad przetwarzania danych przez poszczególnych pracowników,
   b) występowanie z wnioskami do Administratora o nadanie upoważnień do przetwarzania danych dla pracowników referatu;
   c) współpraca z Inspektorem Ochrony Danych w zakresie obowiązków wynikających z ochrony danych osobowych.
5. **Pracownicy:**
   a) przestrzeganie przepisów dotyczących ochrony danych osobowych zgodnie z ustawą, RODO, Polityką oraz innymi procedurami;

b) zachowanie poufności przetwarzanych danych osobowych;

c) naruszenie obowiązku ochrony danych osobowych, a w szczególności obowiązku zachowania danych osobowych w tajemnicy skutkuje poniesieniem odpowiedzialności cywilnej, karnej na podstawie przepisów Ustawy oraz RODO i stanowi ciężkie naruszenie obowiązków pracowniczych i może być podstawą rozwiązania stosunku pracy zgodnie z ustawą - Kodeks Pracy.

§ 8

Zasady ochrony danych osobowych w Urzędzie

1. **Legalność** – przetwarza się dane w oparciu o podstawę prawną i zgodnie z prawem,
2. **Rzetelność** – przetwarza się dane rzetelnie i uczciwie,
3. **Przejrzystość** – przetwarza się dane w sposób przejrzysty i transparentny,
4. **Minimalizacja** – dane przetwarza są adekwatnie i stosownie, w konkretnych celach i nie „na zapas”,
5. **Bezpieczeństwo** − zapewnia się odpowiedni poziom bezpieczeństwa danych podejmując stale działania w tym zakresie.
6. **Ograniczenie przetwarzania** – dane przetwarza są przez okres nie dłuższy, niż jest to niezbędne,
7. **Integralność i poufność** – zapewnia się odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem,
8. **Rozliczalność** – dokumentuje się to, w jaki sposób spełnia obowiązki, aby w każdej chwili móc wykazać ich przestrzeganie.

§ 9

System ochrony danych

System ochrony danych osobowych w Urzędzie składa się z następujących elementów:

1. **Inwentaryzacja danych –** dokonuje się identyfikacji zasobów danych osobowych, w szczególności zbiorów danych;
    a) **Dane szczególne -** identyfikuje się przypadki, w których przetwarza się lub może przetwarzać dane szczególne oraz zapewnia zgodność ich przetwarzania z RODO.
    b) **Dane niezidentyfikowane –** identyfikuje się przypadki, w których przetwarza lub może przetwarzać dane niezidentyfikowane i zapewnia realizację praw osób, których dotyczą dane niezidentyfikowane.
2. **Rejestr -** Administrator opracowuje, prowadzi i utrzymuje Rejestr Czynności Przetwarzania Danych Osobowych.
    a) Rejestr stanowi formę dokumentowania czynności przetwarzania danych, pełni rolę mapy przetwarzania danych i jest jednym z kluczowych

elementów umożliwiających realizację fundamentalnej zasady, na której opiera się cały system ochrony danych osobowych, czyli zasady rozliczalności.

b) Administrator prowadzi Rejestr Czynności Przetwarzania Danych Osobowych, w którym inwentaryzuje i monitoruje sposób, w jaki wykorzystuje dane osobowe.

c) W Rejestrze, dla każdego zbioru danych odnotowuje się: dane Administratora, dane Inspektora danych Osobowych, zbiory danych (czynności przetwarzania), cel przetwarzania, opis kategorii osób, opis kategorii danych, opis kategorii odbiorców danych, informację o przekazaniu danych poza EU/EOG; ogólny opis technicznych i organizacyjnych środków bezpieczeństwa.

3. **Obsługa praw jednostki** - Administrator spełnia obowiązki informacyjne względem osób, których dane przetwarza, oraz zapewnia obsługę ich praw, realizując otrzymane w tym zakresie żądania, w szczególności:
   a) **obowiązki informacyjne –** przekazuje osobom, prawem wymagane informacje przy zbieraniu danych i w innych sytuacjach, poprzez zamieszczenie ogólnej klauzuli informacyjnej na stronie BIP oraz tablicy ogłoszeń Urzędu Gminy, a także poprzez przekazanie osobom, których dane dotyczą klauzuli informacyjnej przez pracowników wynikającej z celu i podstawy przetwarzania zgodnie z **zał. Nr 3** do niniejszej Polityki;
   b) **obsługa żądań -** zapewnia odpowiednie działania, aby żądania osób były realizowane w terminach i w sposób wymagany przez RODO.
   c) **zawiadamianie o naruszeniach** – jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, zawiadamia bez zbędnej zwłoki osobę, której dane dotyczą.
4. **Bezpieczeństwo –** Administrator zapewnia odpowiedni poziom bezpieczeństwa danych, w tym:
   a) przeprowadza analizę ryzyka przetwarzania danych osobowych,
   b) dostosowuje środki ochrony danych do ustalonego ryzyka;
5. **Podmiot przetwarzający:**
   a) W Urzędzie identyfikuje się podmioty przetwarzające dane osobowe na rzecz Administratora i zawiera się z nimi odpowiednie umowy powierzenia w tym zakresie;
   b) Administrator prowadzi rejestr zawartych umów powierzenia z podmiotami przetwarzającymi zgodnie ze wzorem określonym w **zał. Nr 4** do niniejszej Polityki.
6. **Odbiorca danych:**
   Administrator na bieżąco monitoruje, czy istnieją przesłanki przekazania danych do państw trzecich lub do organizacji międzynarodowych w celu zapewnienia zgodnych z prawem warunków takiego przekazywania, jeśli ma ono miejsce.
7. **Przetwarzanie transgraniczne** – w Urzędzie nie prowadzi się przetwarzania

transgranicznego w rozumieniu RODO.

§ 10

Podstawy przetwarzania

1. Podstawą przetwarzania danych osobowych w Urzędzie jest: wypełnienie obowiązku prawnego, przetwarzanie w celu zawarcia umowy, ochrona żywotnych interesów osoby, realizacja zadania w interesie publicznym lub w ramach sprawowania władzy publicznej, zgodnie z art.6 RODO.
2. W przypadku przetwarzania danych osobowych na podstawie zgody osoby, której dane dotyczą (art.6 ust.1 RODO), Administrator wskazuje podstawę przetwarzania w sposób jasny i zrozumiały, wskazując jednocześnie obowiązki informacyjne określone w art.13 RODO.
3. W Urzędzie Gminy Śniadowo przetwarzane mogą być szczególne kategorie danych osobowych zgodnie z art. 9 ust. 2 RODO.

§ 11

Odpowiedzialność za naruszenie ochrony danych osobowych

1. **Odpowiedzialność cywilna:**

1) Każda osoba, która poniosła szkodę majątkową lub niemajątkową w wyniku naruszenia jego praw i wolności, w szczególności danych osobowych, ma prawo uzyskać od Administratora lub podmiotu przetwarzającego odszkodowanie za poniesioną szkodę.
2) W sprawach o roszczenia z tytułu naruszenia przepisów o ochronie danych osobowych, o których mowa w art.79 i 82 RODO, jest właściwy sąd okręgowy.

2. **Odpowiedzialność administracyjna:**

1) Za nieprzestrzeganie przepisów RODO Prezes UODO może nałożyć na Administratora w drodze decyzji administracyjnej karę pieniężną w wysokości do 100.000 zł;
2) Administracyjne kary pieniężne Prezes UODO nakłada na podstawie i na warunkach określonych w art.83 RODO.

3. **Odpowiedzialność karna:**

1) Kto przetwarza dane osobowe, choć ich przetwarzanie nie jest dopuszczalne albo do których przetwarzania nie jest uprawniony, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.
2) Jeżeli czyn określony w pkt 1) dotyczy danych szczególnych, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 3.
3) Kto udaremnia lub utrudnia kontrolującemu prowadzenie kontroli przestrzegania

przepisów o ochronie danych osobowych, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

Załącznik Nr 1
do Polityki bezpieczeństwa
danych osobowych

Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe

Lp.	Dokładny adres	Dział użytkujący pomieszczenie	Nr pokoju lub pomieszczenia	Rodzaj zastosowanego zabezpieczenia pomieszczenia	Uwagi
1.	Urząd Gminy w Śniadowie 18-411 Śniadowo, ul. Ostrołęcka 11 Budynek A	Referat Finansowo-Budżetowy	Pokoje: Nr 1, 2, 3	Budynek zabezpieczony systemem alarmowym. Pokoje zamykane na klucz.	
2.	Urząd Gminy w Śniadowie 18-411 Śniadowo, ul. Ostrołęcka 11 Budynek A	Referat Organizacyjny	Pokoje: Nr 5, 6, 9, 10	Budynek zabezpieczony systemem alarmowym. Pokoje zamykane na klucz.	
3.	Urząd Gminy w Śniadowie 18-411 Śniadowo, ul. Ostrołęcka 11 Budynek A	Referat Organizacyjny	Serwerownia	Budynek zabezpieczony systemem alarmowym. Pomieszczenie zamykane na klucz.	
4.	Urząd Gminy w Śniadowie 18-411 Śniadowo, ul. Ostrołęcka 11 Budynek B	Referat Organizacyjny	Archiwum	Pomieszczenie zamykane na klucz	
5.	Urząd Gminy w Śniadowie 18-411 Śniadowo, ul. Ostrołęcka 11 Budynek B	Referat Rozwoju Gospodarczego	Pokoje: Nr 11 i 13	Pokoje zamykane na klucz.	

Data i podpis Administratora:

….....

Załącznik Nr 2
do Polityki bezpieczeństwa
danych osobowych

REJESTR CZYNNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH URZĘDU GMINY ŚNIADOWO

ADMINISTRATOR:

Wójt Gminy Śniadowo

ul. Ostrołęcka 11, 18-411 Śniadowo

Tel. 86 3090800

NIP: 718-20-23-707

E-mail: sekretariat@sniadowo.pl

www.sniadowo.pl

INSPEKTOR OCHRONY DANYCH:

Urząd Gminy Śniadowo

ul. Ostrołęcka 11, 18-411 Śniadowo

L.p	Nazwa czynności przetwarzania	Cel Przetwarzania/ Podstawa prawna	Opis kategorii osób oraz kategorie danych osobowych	Kategorie odbiorców	Przekazanie danych osobowych	-	Po zakończeniu kadencji sołtysa
					-	-	Zgodnie z jednolitym rzeczowym wykazem akt organów gminy
						-	Zgodnie z jednolitym rzeczowym wykazem akt organów gminy
						-	Zgodnie z jednolitym rzeczowym wykazem akt organów gminy
						-	Po zakończeniu umowy

Opis technicznych i organizacyjnych środków bezpieczeństwa

Lp.	Środki bezpieczeństwa	Ogólny opis środków bezpieczeństwa
1.	**Środki techniczne**	1. Administrator zapewnia środki ochrony adekwatne do stwierdzonego poziomu ryzyka. 2. Została opracowana i wdrożona polityka kluczy. 3. Przetwarzanie danych dokonywane jest w warunkach zabezpieczających je przed dostępem osób nieupoważnionych w 2-ch budynkach A i B. Budynek główny (A) zabezpieczony jest systemem alarmowym. Budynek główny (A) oraz pomieszczenia w budynku A i B są zamykane na klucz. 4. Wejścia do budynku głównego są monitorowane za pomocą monitoringu wizyjnego. 5. Wewnętrzna sieć informatyczna zabezpieczona jest zaporą firewall. 6. Wszystkie stacje komputerowe zabezpieczone są programem antywirusowym. 7. Budynek A i budynek B posiada dodatkowe źródło zasilania w energię elektryczną w postaci agregatu prądotwórczego. 8. W budynku A i B zapewniona jest zgodnie z instrukcją ppoż. odpowiednia ilość legalizowanych gaśnic. 9. Stanowiska komputerowe podtrzymywane są dodatkowym źródłem zasilania w postaci zasilacza UPS.
2.	**Środki organizacyjne**	1. Administrator wyznaczył Inspektora Danych Osobowych. 2. Została opracowana i wdrożona dokumentacja dotycząca ochrony danych osobowych. 3. Do przetwarzania danych osobowych zostały dopuszczone wyłącznie osoby posiadające stosowne upoważnienie (prowadzona jest ewidencja upoważnień). 4. Osoby dopuszczone do przetwarzania danych osobowych zostały zapoznane z zasadami ochrony danych i zobowiązały się do zachowania poufności. 5. Administrator zapewnia coroczne szkolenie wewnętrzne dla pracowników w zakresie ochrony danych osobowych. 6. Administrator dokonuje oceny ryzyka przetwarzanych danych osobowych. 7. Administrator stosuje pisemne umowy powierzenia przetwarzanych danych z podmiotami przetwarzającymi..

Data i podpis Administratora:

…….

Załącznik nr 3
do Polityki bezpieczeństwa
danych osobowych

Ogólna klauzula informacyjna

Zgodnie z art. 13 ust. 1−2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119, s. 1) – zwanym dalej RODO – ustala się niniejszą klauzulę:

I. Administrator danych osobowych

Wójt Gminy Śniadowo, ul. Ostrołęcka 11, 18-411 Śniadowo

II. Inspektor Ochrony Danych

Urząd Gminy Śniadowo, ul. Ostrołęcka 11, 18-411 Śniadowo

III. Cele i podstawy przetwarzania

1. Celem przetwarzania danych jest realizacja zadań własnych gminy zgodnie z art. 7 ustawy z dnia 8 marca 1990 roku o samorządzie gminnym (Dz.U. 2019, poz.506 ze zm.), a także innych zadań wynikających z ustaw szczególnych.
2. Podstawą przetwarzania jest art. 6 ust.1 RODO, w szczególności:

a) zgoda osoby, której dane dotyczą (podstawa z art. 6 ust. 1 lit. a RODO):

b) jest to niezbędne w celu zawarcia bądź wykonania umowy (podstawa z art. 6 ust. 1 lit. b RODO);

c) jest to niezbędne do wypełnienia obowiązku prawnego (podstawa z art. 6 ust. 1 lit. c RODO);

d) jest to niezbędne do ochrony Pana/Pani żywotnych interesów lub żywotnych interesów innej osoby (podstawa z art. 6 ust. 1 lit. d RODO);

e) jest to niezbędne do wykonania zadania, które Administrator realizuje w interesie publicznym lub w ramach powierzonej władzy publicznej (podstawa z art. 6 ust. 1 lit. e RODO);

IV. Okres przechowywania danych

Zebrane dane będą przechowywane do chwili realizacji zadania zgodnie z celem i podstawą przetwarzania, określonym w pkt. III, na podstawie Rozporządzenia Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych (Dz.U. 2011, Nr 14, poz.67).

V. Odbiorcy danych

Pani/Pana dane osobowe mogą zostać udostępnione podmiotom, z którymi Administrator ma zawarte umowy powierzenia przetwarzania danych osobowych

oraz innym podmiotom upoważnionym na podstawie odpowiednich przepisów prawa. Administrator nie zamierza przekazywać Pana/Pani danych osobowych do państwa trzeciego lub organizacji międzynarodowej.

VI. Prawa osób, których dane dotyczą:

Zgodnie z RODO, przysługuje Panu/Pani:

a) prawo dostępu do swoich danych oraz otrzymania ich kopii;

b) prawo do sprostowania (poprawiania) swoich danych;

c) prawo do usunięcia danych, ograniczenia przetwarzania danych;

d) prawo do wniesienia sprzeciwu wobec przetwarzania danych;

e) prawo do przenoszenia danych;

f) prawo do wniesienia skargi do organu nadzorczego.

VII. Informacja o wymogu/dobrowolności podania danych

1. Podanie przez Pana/Panią danych jest obowiązkiem wynikającym z przepisów prawa, a konsekwencją niepodania danych osobowych będzie brak możliwości realizacji usługi/zadania.
2. W przypadku umowy podanie danych ma charakter dobrowolny, ale jest konieczne w celu jej zawarcia.
3. Pani/Pana dane nie będą przetwarzane w sposób zautomatyzowany, w tym również w formie profilowania

Załącznik Nr 4
do Polityki bezpieczeństwa
danych osobowych

Rejestr zawartych umów powierzenia

Lp.	Dane Administratora	Dane podmiotu przetwarzającego	Przedmiot i czas trwania umowy	Charakter i cel przetwarzania	Rodzaj danych osobowych	Kategorie osób
1.						
2.						
3.						
4.						
5.						
6.						

Data i podpis Administratora:

.....

Załącznik Nr 2 do zarządzenia Nr .....

Wójta Gminy Śniadowo

z dnia ..... 2020 r.

POLITYKA BEZPIECZEŃSTWA INFORMACJI

§ 1. Postanowienia ogólne

1. Polityka bezpieczeństwa informacji zwana dalej „PBI" określa zestaw efektywnych i udokumentowanych procedur, regulaminów zawierających zasady i sposoby postępowania mających na celu zapewnienia odpowiedniego poziomu bezpieczeństwa informacji.

2. PBI jest elementem systemu zarządzania bezpieczeństwem informacji zapewniającym poufność, dostępność i integralność informacji.

3. PBI jest dokumentem dynamicznie zmieniającym się w czasie. W celu utrzymania aktualności i ciągłości Polityki Bezpieczeństwa Informacji, dokumenty stanowiące jej integralną część będą aktualizowane na bieżąco i nie będą wymagały zmiany Zarządzenia w tym zakresie.

4. PBI została opracowana na podstawie:

1) Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119, s. 1);
2) Ustawy z dnia 10 maja 2018 roku o ochronie danych osobowych (Dz.U.2019, poz.1781).
3) Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. 2017, poz. 2247).

5. Zastosowane skróty i definicje oznaczają:

1) **Ustawa** - ustawa z dnia maja 2018 r. o ochronie danych osobowych (Dz. U. 2019, poz. 1781),
2) **Rozporządzenie** - Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119, s. 1);
3) **KRI** – Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. 2017, poz.2247).
4) **Administrator -Wójt** Gminy Śniadowo, ul. Ostrołęcka 11, 18-411 Śniadowo.
5) **Inspektor Ochrony Danych (IOD)** – pracownik bądź inna osoba wyznaczona przez Administratora (Wójta),
6) **Użytkownik systemu** - osoba upoważniona do przetwarzania danych osobowych w systemie informatycznym. Użytkownikiem może być osoba zatrudniona w urzędzie na podstawie stosunku pracy, osoba wykonująca pracę na podstawie umowy zlecenia lub innej, umowy cywilno-prawnej, osoba odbywająca staż w urzędzie,
7) **Identyfikator użytkownika** - ciąg znaków jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym,
8) **Administrator Systemu Informatycznego (ASI)** - informatyk (pracownik) wyznaczony przez Administratora (Wójta), który odpowiedzialny jest za funkcjonowanie i zabezpieczenie systemów informatycznych oraz stosowanie środków technicznych i organizacyjnych ochrony stosowanych w tych systemach;

9) **Sieć lokalna** - należy przez to rozumieć połączenie komputerów pracujących w urzędzie w celu wymiany danych (informacji) dla własnych potrzeb, przy wykorzystaniu urządzeń telekomunikacyjnych,

10) **System informatyczny** - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,

11) **Przetwarzanie** - oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;

12) **Zabezpieczenie danych w systemie informatycznym** - wdrożenie i wykorzystywanie stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich utratą,

13) **Komórka organizacyjna** - referaty, samodzielne stanowiska pracy,

14) **UODO – Urząd Ochrony Danych Osobowych.**

§ 2. Nadawanie upoważnień do przetwarzania danych oraz ich rejestrowanie w systemie informatycznym

1. Przed przystąpieniem do pracy przy przetwarzaniu danych, każdy użytkownik powinien zostać zapoznany przez kierownika komórki organizacyjnej lub IOD z przepisami dotyczącymi ochrony danych osobowych.
2. Wydanie upoważnienia oraz rejestracja użytkownika w systemie informatycznym przetwarzającym dane następuje na wniosek kierownika komórki organizacyjnej.
3. Procedury nadawania i odwoływania upoważnień dla użytkowników do przetwarzania danych osobowych realizowane są wg następujących zasad:

1) Kierownik komórki organizacyjnej składa do Administratora pisemny wniosek o wydanie upoważnienia do przetwarzania danych osobowych, którego wzór stanowi **Zał. Nr 1** do PBI. Wniosek obejmuje także nadanie uprawnień w systemie informatycznym;

2) użytkownik składa pisemne oświadczenie o zachowaniu w tajemnicy zasad przetwarzania danych oraz sposobów ich zabezpieczania, obejmujący także okres po ustaniu stosunku pracy lub innej formy zatrudnienia bądź odwołaniu upoważnienia. Wzór oświadczenia stanowi **Zał. Nr 2** do PBI;

3) wzór upoważnienia do przetwarzania danych osobowych stanowi **Zał. Nr 3** do PBI.

4. Upoważnienia nadane przez Administratora zachowują swoją ważność do chwili ich wygaśnięcia bądź odwołania.
5. Administrator prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych według wzoru stanowiącego **Zał. Nr 4** do PBI.
6. Przyznanie uprawnień do przetwarzania danych osobowych w systemie polega na wprowadzeniu do systemu identyfikatora, hasła oraz ustanowienia zakresu dostępnych danych i operacji dla każdego użytkownika.
7. Za przydzielenie i wygenerowanie hasła użytkownikowi, który po raz pierwszy korzysta z systemu, odpowiada ASI.
8. Identyfikator użytkownika nie może być zmieniany, a po wyrejestrowaniu użytkownika z systemu nie może być przydzielony innej osobie.
9. Kierownik komórki organizacyjnej (przełożony) użytkownika zobowiązany jest pisemnie informować ASI o każdej zmianie dotyczącej użytkowników mającej wpływ na zakres posiadanych uprawnień do przetwarzania danych.
10. W przypadku dłuższej nieobecności w pracy użytkownika, kierownik komórki organizacyjnej występuje do ASI o czasowe zablokowanie konta użytkownika.

11. Wyrejestrowanie użytkownika z systemu następuje z dniem wygaśnięcia upoważnienia bądź jego odwołania. Wyrejestrowania dokonuje ASI po uzyskaniu informacji od Administratora bądź kierownika komórki organizacyjnej użytkownika.

§ 3. Stosowane metody i środki uwierzytelniania oraz procedury związane z ich zarządzaniem i uwierzytelnianiem

1. System, w którym przetwarza się dane osobowe wyposażony jest w mechanizmy uwierzytelnienia użytkownika oraz kontroli dostępu użytkowników. Jednym z elementów umożliwiającym dostęp do systemu jest hasło, które pełni rolę weryfikowania tożsamości użytkownika.
2. Hasło dostępu składa się z ciągu literowo-cyfrowego i nie może kojarzyć się bezpośrednio z użytkownikiem.
3. Hasło dostępu zapisywane jest na ekranie monitora w formie niejawnej i znane jest tylko użytkownikowi.
4. Hasło nadane przez użytkownika musi składać się z co najmniej z 8 znaków oraz zawierać małe i wielkie litery oraz cyfry lub znaki specjalne.
5. Użytkownik sam ustala hasło dostępu i w przypadku podejrzenia lub stwierdzenia jego ujawnienia niezwłocznie je zmienia. Jeżeli system nie wymusza zmiany hasła, użytkownik ma obowiązek zmieniać je nie rzadziej niż co 30 dni.
6. Hasła dostępu do baz danych są różne od haseł uwierzytelniających użytkowników w systemie.
7. Identyfikator użytkownika składa się z ciągu znaków literowych, cyfrowych lub innych jednoznacznie identyfikujących w systemie osobę upoważnioną do przetwarzania danych osobowych.
8. Identyfikator użytkownikowi przyznaje Administrator.
9. Identyfikator podlega wpisowi do " Ewidencji osób upoważnionych do przetwarzania danych osobowych" i po jego wyrejestrowaniu nie może być przydzielony innej osobie.
10. Podczas przetwarzania danych osobowych w systemie posługiwanie się identyfikatorem innej osoby jest zabronione.
11. Użytkownik ponosi odpowiedzialność za czynności wykonywane w systemie przy użyciu identyfikatora i hasła.
12. Osobą odpowiedzialną za prawidłowe funkcjonowanie w systemie mechanizmów uwierzytelniających jest ASI.
13. ASI deponuje u Administratora tzw. „bezpieczną kopertę” z hasłami do systemów informatycznych.
14. Otwarcie „bezpiecznej koperty” przez Administratora może nastąpić w przypadku zaistnienia sytuacji nadzwyczajnej uniemożliwiającej funkcjonowanie systemów informatycznych.

§ 4. Praca w systemie informatycznym oraz zapewnienie ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem bądź uszkodzeniem

1. Użytkownik, rozpoczynając pracę na komputerze, loguje się do systemu informatycznego.
2. Dostęp do danych osobowych możliwy jest jedynie po dokonaniu uwierzytelnienia użytkownika.
3. W przypadku zablokowania dostępu do systemu, odblokowania dostępu do zbioru danych może dokonać ASI.
4. W przypadku braku aktywności użytkownika na komputerze przez czas dłuższy niż 10 minut następuje automatyczne włączenie wygaszacza ekranu.
5. Monitory stanowisk komputerowych, na których przetwarzane są dane osobowe, znajdujące się w pomieszczeniach, gdzie przebywają osoby, które nie posiadają upoważnień do przetwarzania danych, należy ustawić w taki sposób, aby uniemożliwić tym osobom wgląd w dane.
6. Przebywanie osób nieuprawnionych w pomieszczeniach znajdujących się na obszarze, w którym są przetwarzane dane osobowe, jest dopuszczalne tylko w obecności osoby upoważnionej.

7. Dostęp do serwerowni posiada ASI, który obowiązany jest ewidencjonować przebywanie w pomieszczeniu (ewidencja wejść i wyjść).
8. Pomieszczenia, w których przetwarzane są dane osobowe, należy zamykać na czas nieobecności osób upoważnionych, w sposób uniemożliwiający dostęp do nich osobom nieupoważnionym.
9. Przed opuszczeniem stanowiska pracy użytkownik jest obowiązany wylogować się z systemu informatycznego lub wywołać blokowany hasłem wygaszacz ekranu.
10. Kończąc pracę użytkownik jest zobowiązany wylogować się z systemu, a następnie wyłączyć sprzęt komputerowy i listwę zasilającą,
11. Wszelką dokumentację oraz nośniki magnetyczne i optyczne, na których znajdują się dane osobowe, przechowuje się szafach zamykanych na klucz.
12. Zabrania się udostępniania innym osobom haseł oraz podpisu elektronicznego w celu nieuprawnionego dostępu do systemu informatycznego.
13. Zastosowane środki ochrony fizycznej Urzędu oraz ochronę pomieszczeń przed nieuprawnionym dostępem określa Polityka kluczy zawarta w **Zał. Nr 5** do niniejszej PBI.

§ 5. Zapewnienie odpowiedniego poziomu bezpieczeństwa w systemach informatycznych

1. Za aktualizację oprogramowania na poszczególnych stanowiskach komputerowych odpowiedzialny jest ASI.
2. Zabrania się użytkownikom samodzielnego instalowania programów, aplikacji na stanowiskach komputerowych bez zgody ASI.
3. Za bezpieczeństwo plików systemowych odpowiada ASI. Użytkownicy nie mogą posiadać uprawnień administratora systemów informatycznych.
4. Dane przetwarzane w systemie informatycznym podlegają zabezpieczeniu, poprzez tworzenie kopii zapasowych.
5. Za tworzenie kopii zapasowych zbiorów danych osobowych odpowiedzialny jest ASI.
6. Kopie zapasowe danych przetwarzanych w systemach informatycznych wykonywane są codziennie w sposób automatyczny po zakończeniu pracy Urzędu i zapisywane są na serwerze znajdującym się w serwerowni.
7. Wykonane kopie zapasowe zgrywane są na dysk zewnętrzny co najmniej raz w tygodniu i przechowywane poza obszarem przetwarzania w szafie zamykanej na klucz.
8. ASI okresowo nie rzadziej niż raz na pół roku przeprowadza sprawdzenie kopii zapasowych zbiorów danych pod kątem ich przydatności do odtworzenia.
9. W celu minimalizacji utraty danych na stanowiskach komputerowych przetwarzających dane osobowe należy stosować dodatkowe zabezpieczenie w postaci zasilacza UPS.

§ 6. Sposób i miejsce przechowywania elektronicznych nośników danych zawierających dane osobowe oraz kopii zapasowych

1. Użytkownicy nie mogą wynosić z terenu Urzędu nośników i wydruków z zapisanymi danymi osobowymi, bez zgody Administratora lub IOD.
2. Zabrania się używania prywatnych elektronicznych nośników.
3. Elektroniczne nośniki informacji zawierające dane oraz wydruki (dokumenty papierowe) przechowuje się wewnątrz obszaru przetwarzania danych, w meblach biurowych zamykanych na klucz.
4. Nośniki przenośne podlegają inwentaryzacji prowadzonej przez ASI.
5. Kopie zapasowe przechowuje się w szafach zamykanych na klucz w pomieszczeniach, które nie są stałym miejscem ich przetwarzania i zapewniają właściwą ochronę przed nieuprawnionym dostępem, modyfikacją uszkodzeniem lub zniszczeniem.

6. Usunięcie danych z systemu powinno być zrealizowane przy pomocy oprogramowania przeznaczonego do bezpiecznego usuwania danych z nośnika danych.
7. Dane osobowe w postaci elektronicznej należy usuwać z nośnika danych w sposób uniemożliwiający ich ponowne odtworzenie.
8. Nośniki danych podlegają komisyjnemu zniszczeniu, w przypadku wycofania z eksploatacji sprzętu komputerowego, na którym przetwarzane były dane osobowe oraz po przeniesieniu danych osobowych do zbiorów danych osobowych w systemie informatycznym z nośników, których ponowne wykorzystanie nie jest możliwe. Z przeprowadzonych czynności komisja sporządza protokół.
9. Przez zniszczenie nośników danych należy rozumieć ich trwałe i nieodwracalne zniszczenie fizyczne do stanu uniemożliwiającego ich rekonstrukcję i odzyskanie danych.
10. Niepotrzebne wydruki z systemu, które zawierają dane osobowe należy niszczyć w niszczarkach w sposób uniemożliwiający ich odtworzenie.

§ 7. Zasady gwarantujące bezpieczną pracę w systemach informatycznych i przy przetwarzaniu mobilnym oraz zasady postępowania z informacjami zapewniającymi minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji

1. Za ochronę antywirusową systemu informatycznego odpowiada ASI.
2. System antywirusowy zainstalowany jest na każdym komputerze.
3. W przypadku pojawienia się wirusa, użytkownik obowiązany jest zaprzestać wykonywania jakichkolwiek czynności w systemie i niezwłocznie powiadomić o tym fakcie ASI i IOD.
4. Niedozwolone jest wyłączanie, blokowanie i odinstalowywanie programów zabezpieczających komputer przed oprogramowaniem złośliwym oraz nieautoryzowanym dostępem (skaner antywirusowy, firewall).
5. Przy przesyłaniu danych osobowych pocztą elektroniczną użytkownicy powinni stosować zasady bezpieczeństwa zgodnie z regulaminem korzystania z poczty elektronicznej stanowiącym **Zał. Nr 6** do PBI.
6. Zasady korzystania z urządzeń mobilnych, na których przetwarzane są dane osobowe określa regulamin stanowiący **Zał. Nr 7** do niniejszej PBI.
7. Zasady korzystania przez użytkowników z Internetu określa regulamin stanowiący **Zał. Nr 8** do niniejszej PBI.
8. W celu minimalizacji utraty bądź nieuprawnionego dostępu do danych osobowych Administrator wprowadza politykę czystego biurka określoną w **Zał. Nr 9** do niniejszej PBI.
9.

§ 8. Wykonywanie przeglądów i konserwacji sprzętu i systemu informatycznego oraz inwentaryzacji sprzętu i oprogramowania

1. Wszelkie prace związane z przeglądami i konserwacją sprzętu oraz systemu informatycznego przetwarzającego dane osobowe wykonuje ASI.
2. ASI przeprowadza przeglądy i konserwację co najmniej raz w roku oraz odpowiada za ich dokumentowanie.
3. Nieprawidłowości w działaniu systemu informatycznego oraz oprogramowania są niezwłocznie usuwane przez ASI, a ich przyczyny analizowane.
4. Zmiana konfiguracji sprzętu komputerowego, na którym znajdują się dane osobowe lub zmiana jego lokalizacji, może być dokonywana za wiedzą i zgodą Administratora.
5. Administrator zapewnia utrzymywanie aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania danych osobowych.
6. Odpowiedzialnym za utrzymywanie aktualnej inwentaryzacji sprzętu i oprogramowania obejmującej, m.in. rodzaj i konfigurację jest ASI, który prowadzi szczegółową ewidencję w tym zakresie.

§ 9. Postępowanie w przypadku naruszenia ochrony danych osobowych

1. Każdy użytkownik, który stwierdza lub podejrzewa naruszenie ochrony danych w systemie informatycznym, zobowiązany jest niezwłocznie poinformować Administratora.
2. W przypadku naruszenia ochrony danych osobowych Administrator nie później niż w terminie 72 godz. od stwierdzenia naruszenia zgłasza je do UODO zgodnie ze wzorem określonym w **Zał. Nr 10** do PBI, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.
3. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.
4. Zawiadomienie osób fizycznych nie jest wymagane w przypadku wdrożenia przez Administratora odpowiednich środków technicznych i organizacyjnych dla ochrony danych osobowych, zastosowania środków eliminujących prawdopodobieństwo wysokiego ryzyka naruszenia praw i wolności osoby, której dane dotyczą, bądź wymagałoby ono niewspółmiernie dużego wysiłku.
5. W przypadkach określonych w ust.4 Administrator wydaje publiczny komunikat, który umieszcza na stronie internetowej i tablicy ogłoszeń Urzędu.
6. Administrator wdraża instrukcję postępowania w sytuacji wystąpienia incydentu naruszenia danych osobowych, stanowiącą **Zał. Nr 11** do PBI.
7. Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych w rejestrze naruszeń danych osobowych zgodnie ze wzorem stanowiącym **Zał. Nr 12** do PBI.

§ 10. Odpowiedzialność za naruszenie ochrony danych osobowych

1. Odpowiedzialność cywilna:
   1) Każda osoba, która poniosła szkodę majątkową lub niemajątkową w wyniku naruszenia jego praw i wolności, w szczególności danych osobowych, ma prawo uzyskać od Administratora lub podmiotu przetwarzającego odszkodowanie za poniesioną szkodę.
   2) W sprawach o roszczenia z tytułu naruszenia przepisów o ochronie danych osobowych, o których mowa w art.79 i 82 RODO, jest właściwy sąd okręgowy.
2. Odpowiedzialność administracyjna:
   1) Za nieprzestrzeganie przepisów RODO Prezes UODO może nałożyć na Administratora w drodze decyzji administracyjnej karę pieniężną w wysokości do 100.000 zł;
   2) Administracyjne kary pieniężne Prezes UODO nakłada na podstawie i na warunkach określonych w art.83 RODO.
3. Odpowiedzialność karna:
   1) Kto przetwarza dane osobowe, choć ich przetwarzanie nie jest dopuszczalne albo do których przetwarzania nie jest uprawniony, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.
   2) Jeżeli czyn określony w pkt 1) dotyczy danych szczególnych, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 3.
   3) Kto udaremnia lub utrudnia kontrolującemu prowadzenie kontroli przestrzegania przepisów o ochronie danych osobowych, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

Załącznik nr 1
do Polityki bezpieczeństwa informacji

WNIOSEK

O WYDANIE UPOWAŻNIENIA DO PRZETWARZANIA DANYCH OSOBOWYCH ORAZ NADANIE UPRAWNIEŃ W SYSTEMIE INFORMATYCZNYM

Imię nazwisko użytkownika	**Komórka organizacyjna**
Przetwarzanie danych osobowych zgodnie z zakresem czynności na stanowisku: **Nadanie uprawnień użytkownika w systemie informatycznym: TAK /~~NIE~~ *** **Zakres uprawnień:** zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, modyfikowanie, pobieranie, wykorzystywanie, przeglądanie, udostępnianie.	
Data wystawienia:	**Popis kierownika komórki organizacyjnej użytkownika systemu:** **……..**
Podpis Kierownika Urzędu **……..**	

*** - niepotrzebne skreślić**

Załącznik nr 2
do Polityki bezpieczeństwa informacji

Śniadowo,dn.....

….....

….....
Imię i Nazwisko pracownika

….....

….....
adres

OŚWIADCZENIE

Oświadczam, iż w związku z wykonywanymi obowiązkami służbowymi, przetwarzam lub mam dostęp do zbiorów, dokumentów, zestawień, kartotek lub systemów informatycznych zawierających dane osobowe i w związku z tym:

1. Stwierdzam własnoręcznym podpisem, iż znana mi jest treść przepisów:

a) ustawy z dnia 10 maja 2018 r. r. o ochronie danych osobowych (Dz. U. 2019, poz.1781),
b) rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) – RODO, (Dz.Urz. UE L 119, s. 1);
c) zarządzenia Nr 7.2020 Wójta Gminy Śniadowo z dnia 13 stycznia 2020 roku w sprawie w sprawie wdrożenia środków technicznych i organizacyjnych przetwarzania danych osobowych w Urzędzie Gminy Śniadowo

2. Zobowiązuję się nie ujawniać wiadomości, z którymi zapoznałem/zapoznałam* się z racji wykonywanej pracy w Urzędzie, a w szczególności nie będę:

a) ujawniać danych osobowych zawartych w bazach danych i systemach informatycznych,
b) ujawniać szczegółów technologicznych używanych w Urzędzie systemów oraz oprogramowań,
c) udostępniać osobom nieupoważnionym danych osobowych, niezależnie od formy ich przetwarzania,
d) kopiować lub przetwarzać danych w sposób inny niż dopuszczony obowiązującymi przepisami.

3. Oświadczam, że zostałem (am) poinformowany o grożącej, stosownie do w/w przepisów Ustawy o ochronie danych osobowych oraz Rozporządzenia RODO, odpowiedzialności karnej i cywilnej. Niezależnie od odpowiedzialności przewidzianej w wymienionych przepisach, mam świadomość, że naruszenie zasad ochrony danych osobowych, obowiązujących w Urzędzie może zostać uznane za ciężkie naruszenie podstawowych obowiązków pracowniczych i skutkować odpowiedzialnością dyscyplinarną zgodnie z ustawą – Kodeks pracy.

….....

podpis

Załącznik nr 3
do Polityki bezpieczeństwa informacji

Śniadowo, dnia ……

UPOWAŻNIENIE NR ……
do przetwarzania danych osobowych

Na podstawie art. 29 i art.32 ust.4 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119, s. 1) − **upoważniam Panią / Pana:**

……
Imię i nazwisko

……
Stanowisko

do przetwarzania danych osobowych

w Urzędzie Gminy Śniadowo w zakresie niezbędnym do wykonywania zadań określonych w zakresie czynności związanych z wykonywaniem obowiązków na zajmowanym stanowisku, polegającym na: zbieraniu, utrwalaniu, organizowaniu, przechowywaniu, adaptowaniu lub modyfikacji, pobieraniu, przeglądaniu lub innego rodzaju udostępnianiu, dopasowywaniu lub łączeniu, ograniczaniu, usuwaniu lub niszczeniu.

Przedmiotowe upoważnienie obejmuje przetwarzanie danych w formie tradycyjnej i elektronicznej.

Upoważnienie jest ważne na czas zatrudnienia w Urzędzie Gminy Śniadowo.

…….....……
pieczęć i podpis osoby nadającej upoważnienie

Zobowiązuję się, przy przetwarzaniu danych osobowych do szczególnej dbałości o zachowanie poufności tych danych, ich integralności i dostępności.
Zobowiązuję się do zachowania w tajemnicy treści przetwarzanych danych osobowych, do których uzyskałam dostęp oraz sposobów ich zabezpieczania, zarówno w okresie trwania umowy jak i po jej ustaniu.

…….....……

data i podpis osoby upoważnionej

Załącznik nr 4
do Polityki bezpieczeństwa informacji

Ewidencja osób upoważnionych do przetwarzania danych osobowych

Lp.	Imię i nazwisko	Data nadania upoważnienia	Data ustania upoważnienia	**Identyfikator** (jeżeli dane są przetwarzane w systemie informatycznym)

Data i podpis Administratora:

.....

Załącznik Nr 5
do Polityki Bezpieczeństwa Informacji

Polityka kluczy

1. Zastosowane środki ochrony fizycznej pomieszczeń:

UG Śniadowo zlokalizowany jest w 2-ch budynkach:

- Budynek A – znajdują się w nim Referaty: Organizacyjny oraz Finansowo-Budżetowy zabezpieczony i chroniony jest systemem alarmowym i zamykany na klucz. Otwieranie i zamykanie budynku oraz uruchamianie i wyłączanie alarmu dokonuje sprzątaczka bądź inna osoba wyznaczona przez Administratora.
- Budynek B – znajduje się tam Referat Rozwoju Gospodarczego oraz archiwum. Pomieszczenia (pokoje) otwierane i zamykane są na klucz przez pracujących w nich pracowników.

2. Instrukcja wydawania kluczy:

1) Klucze do pomieszczeń znajdujących się w budynku A i B znajdują się w szafce w pokoju nr 5 w Referacie Organizacyjnym. Przed rozpoczęciem pracy pracownicy pobierają, a po jej zakończeniu pozostawiają klucze w pokoju nr 5.
2) Pokój nr 5 codziennie otwiera pracownik ds. organizacyjnych i kadr bądź sprzątaczka.
3) Dostęp do pokoju nr 5 posiada sprzątaczka, która nie ma dostępu do baz danych.
4) Dokumenty zawierające dane osobowe przechowywane są w szafach bądź biurkach zamykanych na klucz.
5) Po zakończeniu pracy zabronione jest pozostawianie kluczy w szafach i biurkach.
6) Bazy danych w systemie elektronicznym przechowywane są na komputerach zabezpieczonych hasłem.

Załącznik Nr 6
do Polityki Bezpieczeństwa Informacji

Regulamin korzystania z poczty elektronicznej

1. W przypadku przesyłania danych osobowych poza Urząd należy stosować odpowiednie metody zabezpieczające przed nieupoważnionym dostępem do danych osobowych.
2. Hasło należy przesłać w odrębnej wiadomości elektronicznej lub inną metodą.
3. Zaleca się, aby użytkownik podczas przesyłania danych osobowych pocztą elektroniczną zawarł w treści prośbę o potwierdzenie otrzymania i zapoznania się z informacją przez adresata.
4. Nie należy otwierać załączników w mailach nadesłanych przez nieznanego nadawcę lub podejrzanych załączników nadanych przez znanego nadawcę. W przypadku wątpliwości, należy konsultować się z ASI.
5. Użytkownicy nie powinni rozsyłać wiadomości zawierających załączniki o rozmiarze przekraczającym maksymalną wielkość wskazaną przez ASI.
6. Użytkownicy powinni okresowo kasować niepotrzebne wiadomości.
7. Podczas wysyłania maili do wielu adresatów jednocześnie, należy użyć metody „Ukryte do wiadomości – UDW”.
8. Poczta elektroniczna jest przeznaczona wyłącznie do wykonywania obowiązków służbowych.
9. Przy korzystaniu z poczty elektronicznej użytkownicy mają obowiązek przestrzegać prawa własności i prawa autorskiego.

Załącznik Nr 7
do Polityki Bezpieczeństwa Informacji

Regulamin korzystania z urządzeń mobilnych

1. W przypadku przechowywania na urządzeniu mobilnym danych osobowych lub informacji chronionych użytkownik zobowiązany jest do ich zabezpieczenia przed dostępem osób nieupoważnionych.
2. Na urządzeniach mobilnych przeznaczonych do zewnętrznych prezentacji multimedialnych nie powinny znajdować się dane osobowe i informacje chronione.
3. W przypadku kradzieży lub zgubienia urządzenia mobilnego, użytkownik powinien natychmiast powiadomić o tym IOD oraz ASI.
4. Użytkownik zobowiązany jest do zabezpieczenia urządzenia w czasie transportu.
5. Po zakończeniu pracy urządzenia mobilne zaleca się umieszczać w zamykanych szafkach. Pozostawianie laptopów, tabletów i smartfonów bez nadzoru jest zabronione.
6. Użytkownik urządzenia mobilnego jest zobowiązany do regularnego powiadamiania ASI o konieczności tworzenia kopii bezpieczeństwa danych.
7. Pracując na urządzeniu mobilnym w miejscach publicznych, użytkownik zobowiązany jest chronić wyświetlane na ekranie informacje przed wglądem osób nieupoważnionych.
8. Zabrania się używania prywatnych urządzeń mobilnych do celów służbowych.

Załącznik Nr 8
do Polityki Bezpieczeństwa Informacji

Regulamin korzystania z internetu

1. Użytkownik zobowiązany jest do korzystania z Internetu przede wszystkim w celach służbowych.
2. Zabrania się zgrywania na dysk komputera oraz uruchamia programów oraz plików pobranych z niewiadomego źródła. Pliki takie powinny być ściągane tylko za każdorazową zgodą ASI tylko w uzasadnionych przypadkach.
3. Użytkownik ponosi odpowiedzialność za szkody spowodowane przez oprogramowanie instalowane z Internetu.
4. Zabrania się wchodzenia na strony, na których prezentowane są informacje o charakterze przestępczym, hakerskim, pornograficznym lub innym zakazanym przez prawo.
5. Nie należy w przeglądarkach internetowych włączać opcji zapamiętywania haseł.
6. W przypadku korzystania z szyfrowanego połączenia przez przeglądarkę, należy zwracać uwagę na pojawienie się odpowiedniej ikony (kłódka) oraz adresu www rozpoczynającego się frazą”https:\\”.
7. Należy zachować szczególną ostrożność w przypadku żądania lub prośby podania kodów, numerów PIN, numerów kart płatniczych przez Internet.
8. Przy korzystaniu z Internetu, użytkownicy mają obowiązek przestrzegać prawa własności i prawa autorskiego.

Załącznik Nr 9
do Polityki Bezpieczeństwa Informacji

POLITYKA CZYSTEGO BIURKA

1. Niniejsza polityka czystego biurka obowiązuje wszystkich pracowników zatrudnionych w Urzędzie.
2. Za pracownika uważa się każdą osobę zatrudnioną na podstawie umowy o pracę, powołania, wyboru, a także na innej podstawie niż stosunek pracy.
3. Każdy pracownik zobowiązany jest do przechowywania na biurku tylko tych dokumentów, które są pracownikowi niezbędne w danym momencie pracy do wykonania bieżących zadań.
4. Opuszczając stanowisko pracy bądź po jej zakończonej pracownik zobowiązany jest odłożyć wszystkie dokumenty zawierające dane osobowe do zamykanej na klucz szafy bądź biurka.
5. Po zakończonej pracy na biurku mogą znajdować się jedynie telefon i przybory biurowe, takie jak: zszywacz, dziurkacz, długopis, itp.
6. Pracownik zobowiązany jest do niszczenia dokumentów niepotrzebnych w taki sposób, aby nie było możliwe odtworzenie zawartych w nich informacji, np. w niszczarce.

Załącznik Nr 10
do Polityki bezpieczeństwa informacji

Zgłoszenie naruszenia ochrony danych osobowych organowi nadzorczemu

Data naruszenia ……..…….. Data zgłoszenia ……..……

Nazwa administratora:

…….…….

Dane inspektora ochrony danych …….

Opis charakteru naruszenia ochrony danych osobowych, w tym kategorie i przybliżona ilość osób, których dane dotyczą		
Możliwe konsekwencje naruszenia ochrony danych osobowych		
Środki naprawcze	zastosowane	
	proponowane	

……
(podpis Administratora)

Załącznik Nr 11
do Polityki bezpieczeństwa informacji

Instrukcja postępowania w sytuacji wystąpienia incydentu naruszenia danych osobowych

1. **Instrukcja określa tryb postępowania w przypadku, gdy:**
   1) Stwierdzono wystąpienie incydentu,
   2) Istnieje podejrzenie wystąpienia incydentu.

2. **Typowe zagrożenia:**
   1) niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów,
   2) niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą lub utratą danych,
   3) nieprzestrzeganie zasad ochrony informacji przez pracowników (np. niestosowanie zasady czystego biurka/ekranu, ochrony haseł; niezamykanie pomieszczeń, szaf biurek.

3. **Typowe incydenty:**
   1) zdarzenia losowe zewnętrzne (np.: pożar obiektu/pomieszczenia, zalanie wodą, utrata łączności),
   2) zdarzenia losowe wewnętrzne (np.: awarie serwera, komputerów, oprogramowania, pomyłki informatyków, użytkowników, utrata/zagubienie danych),
   3) umyślne incydenty (np.: włamanie do systemu lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów).

4. **Plan ciągłości działania:**
   1) Każda osoba przetwarzająca dane, która stwierdzi lub podejrzewa naruszenie zabezpieczenia ochrony danych osobowych lub informacji, niezwłocznie powiadamia o tym Administratora oraz IOD ASI.
   2) Administrator podejmuje decyzje o sposobie postępowania w celu powstrzymania lub ograniczenia incydentu. Korzysta przy tym ze wsparcia IOD i ASI.
   3) W przypadku incydentu dotyczącego systemu informatycznego do czasu przybycia ASI na miejsce naruszenia lub ujawnienia naruszenia ochrony danych, należy:

a) niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego naruszenia;
b) rozważyć wstrzymanie bieżącej pracy na komputerze w celu zabezpieczenia miejsca zdarzenia;
c) zaniechać, o ile to możliwe, dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić jego udokumentowanie i analizę;
d) udokumentować wstępnie zaistniałe naruszenie;
e) nie opuszczać, bez uzasadnionej potrzeby, miejsca zdarzenia do czasu przybycia IOD lub ASI.

4) Po przybyciu na miejsce naruszenia lub ujawnienia naruszenia ochrony danych osobowych ASI:
a) zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metody dalszego postępowania;
b) dokonuje zabezpieczenia systemu informatycznego przed dalszym rozprzestrzenianiem się skutków naruszenia;
c) podejmuje odpowiednie kroki w celu powstrzymania lub ograniczenia dostępu osoby niepowołanej, zminimalizowania szkód i zabezpieczenia przed usunięciem śladów lub naruszenia;
5) Po wyczerpaniu niezbędnych środków doraźnych, ASI zasięga opinii Administratora lub IOD i proponuje działania mające na celu usunięcie naruszenia i jego skutków oraz ustosunkowuje się do kwestii ewentualnego odtworzenia danych z kopii zapasowej i terminu wznowienia przetwarzania danych.
6) ASI zobowiązany jest do usunięcia incydentu naruszenia danych osobowych i uruchomienia systemów informatycznych po zaakceptowaniu środków zapobiegawczych przez Administratora.
7) Po przywróceniu prawidłowego funkcjonowania systemu informatycznego, ASI przeprowadza szczegółową analizę w celu określenia przyczyn naruszenia ochrony danych osobowych lub podejrzenia takiego naruszenia oraz podejmuje kroki mające na celu wyeliminowanie podobnych zdarzeń w przyszłości.
8) IOD przeprowadza postępowanie wyjaśniające dotyczące wystąpienia bądź podejrzenia wystąpienia incydentu naruszenia ochrony danych, zgłasza naruszenie do UODO i rejestruje naruszenie w prowadzonym przez Administratora rejestrze naruszeń danych osobowych.

Załącznik Nr 12
do Polityki bezpieczeństwa informacji

Rejestr naruszeń danych osobowych

Lp.	Okoliczności/ opis naruszenia	Data i godzina stwierdzenia naruszenia/podejrzenia naruszenia	Kategoria osób i danych, których naruszenie dotyczy	Opis skutków, konsekwencji naruszenia	Podjęte działania zaradcze	Czy zachodzi obowiązek poinformowania UODO lub osób, których dotyczy naruszenie

Data i podpis Administratora:

….....