Polityka ochrony danych osobowych
w Urzędzie Gminy Żarnów

Rozdział 1
Postanowienia ogólne

§ 1.

Celem Polityki ochrony danych w Urzędzie Gminy Żarnów, zwanym dalej „Organizacją", jest uzyskanie optymalnego i zgodnego z wymogami obowiązujących aktów prawnych sposobu przetwarzania informacji zawierających dane, w tym również dane osobowe.

§ 2.

Polityka ochrony danych osobowych została opracowana w oparciu o wymagania zawarte w:

1. Rozporządzeniu 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 /Dz. Urz. UE.L nr 119, str.1/;
2. Ustawie z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 24 maja 2018 r., poz. 1000);
3. Rozporządzeniu 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. z 2017 r., poz. 2247);
4. ustawie z dnia 9 lutego 2018 r. o ochronie informacji niejawnych (tj. Dz. U. z 2018r., poz. 412);
5. § 3. i § 4. Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych, oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. Nr 100, poz. 1024).

§ 3.

Ochrona danych realizowana jest poprzez zabezpieczenia fizyczne, organizacyjne, oprogramowanie systemowe, aplikacje oraz użytkowników proporcjonalne i adekwatne do ryzyka naruszenia bezpieczeństwa danych przetwarzanych w ramach prowadzonej działalności.

§ 4.

1. Utrzymanie w Organizacji ochrony danych, w tym danych osobowych, rozumiane jest jako zapewnienie ich poufności, integralności, rozliczalności oraz dostępności na odpowiednim poziomie. Miarą bezpieczeństwa jest akceptowalna wielkość ryzyka związanego z ochroną danych.
2. Zastosowane zabezpieczenia mają służyć osiągnięciu powyższych celów i zapewnić:
    1. **poufność danych** – rozumianą jako właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom;
    2. **integralność danych** – rozumianą jako właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
    3. **rozliczalność danych** – rozumianą jako właściwość zapewniającą, że działania osoby mogą być przypisane w sposób jednoznaczny tylko tej osobie;

4. **integralność systemu** – rozumianą jako nienaruszalność systemu, niemożność jakiejkolwiek manipulacji, zarówno zamierzonej, jak i przypadkowej;
5. **dostępność informacji** – rozumianą jako zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią zasobów wtedy, gdy jest to potrzebne;
6. **zarządzanie ryzykiem**– rozumiane jako proces identyfikowania, kontrolowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa, które może dotyczyć systemów informacyjnych służących do przetwarzania danych.

§ 5.

1. Administratorem jest Urząd Gminy Żarnów reprezentowany przez Wójta Gminy.
2. Administrator powołał Inspektora Ochrony Danych (IOD), zgodnie z art. 37 RODO, z którym można skontaktować się pod numerem telefonu 44-75-77-055 w godzinach pracy Urzędu Gminy w Żarnowie lub pod adresem email: iod@zarnow.eu.Zadania IOD zawarte są w art. 39 RODO.

Rozdział 2
Definicje

§ 6.

Przez użyte w Polityce ochrony danych osobowych określenia należy rozumieć:

1. **Administrator Danych** – zwany dalej Administratorem lub AD, jest osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych, w tym danych osobowych;
2. **Inspektor Ochrony Danych (IOD)** – osoba wyznaczona przez Administratora, nadzorująca przestrzeganie zasad i wymogów ochrony danych określonych w RODO i przepisach krajowych;
3. **ustawa** – ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 24 maja 2018 r., poz. 1000);
4. **RODO** – Rozporządzenie 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 (Dz. Urz. UE.L nr 119/1);
5. **dane** – wszelkie informacje, w tym również dane osobowe, przetwarzane w Organizacji w sposób tradycyjny, jak również za pomocą systemu informatycznego;
6. **dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;
7. **zbiór danych osobowych** – uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów;
8. **przetwarzanie danych** – operacja lub zestaw operacji wykonywanych na danych w sposób zautomatyzowany lub niezautomatyzowany, takich jak zbieranie, utrwalanie, przechowywanie, opracowywanie, łączenie, przesyłanie, zmienianie, udostępnianie, usuwanie i niszczenie itd.
9. **system informatyczny** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych;

10. **system tradycyjny** – zespół procedur organizacyjnych, związanych z mechanicznym przetwarzaniem informacji oraz wyposażenie i środki trwałe wykorzystywane w celu przetwarzania danych na papierze;
11. **system zarządzania bazą danych,** zwany dalej **systemem** – oprogramowanie służące do zarządzania bazą danych (moduły programowe) przetwarzające dane zawarte w jednym lub wielu zbiorach;
12. **zabezpieczenie danych w systemie informatycznym (ASI)** – osoba lub osoby, upoważnione przez Administratora do administrowania i zarządzania systemem informatycznym;
13. **Administrator systemu informatycznego (ASI)** – osoba lub osoby, upoważnione przez Administratora do administrowania i zarządzania systemem informatycznym;
14. **odbiorca** – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, któremu ujawnia się dane osobowe w oparciu m. in. o umowę powierzenia,
15. **strona trzecia** – osoba fizyczna lub prawna, organ publiczny , jednostka lub podmiot inny niż osoba, której dane dotyczą , które z upoważnienia Administratora mogą przetwarzać dane osobowe;
16. **identyfikator użytkownika (login)** – ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych w systemie informatycznym;
17. **hasło** – ciąg znaków literowych, cyfrowych lub innych, przypisany do identyfikatora użytkownika, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.

Rozdział 3
Zakres stosowania

§ 7.

1. W Organizacji przetwarzane są dane zebrane w zbiorach danych, ale również dane bez wyraźnego usystematyzowania.
2. Informacje te są przetwarzane zarówno w postaci dokumentacji tradycyjnej, jak i elektronicznej.
3. Polityka ochrony danych zawiera uregulowania dotyczące wprowadzonych zabezpieczeń technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych.
4. Innymi dokumentami w Organizacji regulującymi ochronę danych, w tym również osobowych, są:

    1. instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych,
    2. ewidencja osób upoważnionych do przetwarzania danych osobowych,
    3. rejestr zbiorów danych osobowych,
    4. procedura postępowania w sytuacji naruszenia ochrony danych osobowych.

§ 8.

Politykę ochrony danych stosuje się w szczególności do:

1. danych przetwarzanych w systemach informatycznych, wymienionych w ewidencji osób upoważnionych do przetwarzania danych – załącznik nr 3,

2. wszystkich informacji dotyczących danych pracowników Administratora, mieszkańców Gminy Żarnów,
3. odbiorców danych, którym przekazano dane osobowe do przetwarzania w oparciu o umowy powierzenia, którymi są m.in. obsługa BHP.
4. informacji dotyczących zabezpieczenia danych, w tym w szczególności nazw kont i haseł w systemach służących do przetwarzania danych,
5. rejestru osób, którym Administrator nadał upoważnienia do przetwarzania danych – załącznik nr 5,
6. innych dokumentów zawierających dane.

§ 9.

1. Zakresy ochrony danych określone przez Politykę ochrony danych oraz inne z nią związane dokumenty mają zastosowanie do:

    1. wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów oraz tych w formie tradycyjnej, w których przetwarzane są dane osobowe podlegające ochronie,
    2. wszystkich lokalizacji – budynków i pomieszczeń w których są lub będą przetwarzane informacje podlegające ochronie,
    3. wszystkich pracowników, zleceniobiorców, stażystów, praktykantów i innych osób mających dostęp do informacji podlegających ochronie.

2. Do stosowania zasad określonych przez Politykę ochrony danych osobowych oraz inne z nią związane dokumenty zobowiązani są wszystkie wymienione wyżej grupy osób oraz inne osoby mające dostęp do danych podlegających ochronie.

Rozdział 4
Wykaz zbiorów danych, w tym danych osobowych

§ 10.

1. Dane gromadzone są w zbiorach:

    1. Wnioski o udostępnienie informacji publicznej
    2. Elektroniczny obieg dokumentów system DOKUS
    3. Oświadczenia Radnych o stanie majątkowym
    4. Petycje oraz dokumentacja z Sesji i Komisji Rady Gminy
    5. Ewidencja gruntów i budynków
    6. Ewidencja decyzji o podziale nieruchomości
    7. Ewidencja decyzji o rozgraniczeniach nieruchomości
    8. Ewidencja sprzedaży mienia komunalnego
    9. Ewidencja nabycia mienia komunalnego
    10. Ewidencja osób zatrudnionych
    11. Ewidencja osób składających wniosek o przyznanie stypendium sportowego za osiągnięcia sportowe
    12. Ewidencja zgłoszeń do ubezpieczenia społecznego pracowników i zleceniobiorców
    13. Ewidencja zgłoszeń do ubezpieczenia zdrowotnego członków rodziny pracowników jednostki

14. Podatek od środków transportowych
15. Urząd Stanu Cywilnego - akta stanu cywilnego i akta zbiorowe rejestracji stanu cywilnego
16. Rejestr decyzji o świadczenia osobiste i rzeczowe na rzecz obrony
17. Rejestr osób podlegających stawiennictwu do kwalifikacji wojskowej
18. Ewidencja ludności i dowodów osobistych
19. Rejestr wniosków o przyznanie stypendiów szkolnych
20. Wnioski o dofinansowanie kształcenia młodocianego pracownika
21. Rejestr szkód łowieckich
22. Ewidencja skazanych wykonujących prace na rzecz kary ograniczenia wolności
23. Rejestr zezwoleń na wycięcie drzew i krzewów
24. Decyzje o środowiskowych uwarunkowaniach
25. Ewidencja gospodarowania odpadami na terenie gminy
26. Rejestr decyzji na zajęcie pasa drogowego i uzgodnień drogowych
27. Ewidencja umów najmu lokali użytkowych lub dzierżawy mienia gminnego
28. Karty Gospodarstw Rolnych dotyczące KRUS
29. Podatki: rolny, leśny, od nieruchomości – nakazy
30. Księgowość zobowiązań podatkowych i niepodatkowych
31. Ewidencja osób ubiegających się o zwrot akcyzy paliwowej
32. Ewidencja pozwoleń na sprzedaż napojów alkoholowych
33. KASA+
34. Rejestr i decyzje o warunkach zabudowy i zagospodarowaniu terenu
35. Ewidencja wypisów i wyrysów z miejscowego planu zagospodarowania przestrzennego
36. Ewidencja decyzji o lokalizacji inwestycji celu publicznego
37. Ewidencja wniosków o nadanie numeru porządkowego nieruchomości
38. Ewidencja osób otrzymujących dofinansowanie do zmiany ogrzewania
39. Ewidencja osób otrzymujących dofinansowanie na usuwanie azbestu
40. Ewidencja uczestników zamówień publicznych
41. Oświadczenia o stanie majątkowym: wójta, zastępcy wójta, sekretarza gminy, skarbnika gminy, kierowników jednostek organizacyjnych gminy
42. Ewidencja wniosków do Gminnej Komisji Rozwiązywania Problemów Alkoholowych
43. Rejestr mężczyzn objętych rejestracją wojskową z terenu Gminy Żarnów
44. Rejestr kobiet objętych rejestracją wojskową z terenu Gminy Żarnów
45. Ewidencja wniosków do Centralnej Ewidencji i Informacji o Działalności Gospodarczej
46. Rejestr VAT
47. Upoważnienia
48. Rejestr umów dzierżaw - osób fizycznych
49. Ewidencja zwolnień lekarskich pracowników Urzędu
50. Ewidencja zaświadczeń o wielkości gospodarstwa
51. Ewidencja umorzeń podatkowych
52. Rejestr warunków technicznych za podłączenie do sieci wodociągowej i kanalizacyjnej
53. Prowadzenie spraw związanych z PPK
54. Prowadzenie spraw związanych z PKZP

55. WOW
56. Elektroniczny obieg dokumentów system PROTON
57. Deklaracje dotyczące emisyjności budynków
58. Ewidencja rozliczeń pracowników oraz zleceniobiorców, stypendystów, sołtysów i radnych z Urzędem Skarbowym (Pit 11, Pit R)

2. Szczegółowy wykaz Rejestru zbiorów danych osobowych zawiera załącznik nr 2.

Rozdział 5
Wykaz budynków, pomieszczeń, w których wykonywane są operacja przetwarzania danych

§12.

1. Dane, w tym dane osobowe, przetwarzane są w budynku, mieszczącym się w Żarnowie, przy ulicy Opoczyńska 5.

2. Obszar, w którym przetwarzane są dane za pomocą systemów oraz tradycyjnie, w których przechowuje się wszelkie nośniki informacji zawierające dane, jak również te podlegające zniszczeniu.

Rozdział 6
Środki organizacyjne i techniczne zabezpieczenia danych

§ 13.

1. **Zabezpieczenia organizacyjne:**
   - **1.** opracowano i wdrożono Politykę bezpieczeństwa przetwarzania danych,
   - **2.** sporządzono i wdrożono Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych w Organizacji,
   - **3.** stworzono procedurę postępowania w sytuacji naruszenia ochrony danych osobowych,
   - **4.** opracowano i bieżąco prowadzi się rejestr czynności przetwarzania,
   - **5.** opracowano i wdrożono instrukcję posługiwania się pocztą elektroniczną,
   - **6.** wyznaczono Inspektora Ochrony Danych,
   - **7.** do przetwarzania danych zostały dopuszczone wyłącznie osoby posiadające upoważnienia nadane przez Administratora bądź osobę przez niego upoważnioną,
   - **8.** osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych oraz w zakresie zabezpieczeń Systemu Informatycznego,
   - **9.** osoby zatrudnione przy przetwarzaniu danych obowiązane zostały do zachowania ich w tajemnicy,
   - **10.** przetwarzanie danych dokonywane jest w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych,
   - **11.** przebywanie osób nieuprawnionych w pomieszczeniach, gdzie przetwarzane są dane jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu danych oraz w warunkach zapewniających bezpieczeństwo danych,
   - **12.** dokumenty i nośniki informacji zawierające dane, które podlegają zniszczeniu, neutralizuje się za pomocą urządzeń do tego przeznaczonych lub dokonuje się takiej ich modyfikacji, która nie pozwoli na odtworzenie ich treści.

2. **Zabezpieczenia techniczne**
   1. wewnętrzną siecią komputerową zabezpieczoną poprzez odseparowanie od sieci publicznej za pomocą urządzeń UTM,
   2. stanowiska komputerowe wyposażono w indywidualną ochronę antywirusową,
   3. komputery zabezpieczono przed możliwością użytkowania przez osoby nieuprawnione do przetwarzania danych za pomocą indywidualnego identyfikatora użytkowania i cyklicznie wymuszanej zmiany hasła.

3. **Środki ochrony fizycznej:**
   1. obszar, na którym przetwarzane są dane, poza godzinami pracy, chroniony jest alarmem,
   2. urządzenia służące do przewarzania danych umieszczone są w zamykanych pomieszczeniach,
   3. dokumenty i nośniki informacji zawierające dane przechowywane są w zamykanych na klucz szafach.

Rozdział 7
Zadania Administratora lub Inspektora Ochrony Danych (IOD)

§ 14.

1. Obowiązki Administratora lub IOD zostały określone w załączniku do Zarządzenia Nr 24/2018 Wójta Gminy Żarnów z dnia 06.04.2018 r. w sprawie: powołania Administratora Bezpieczeństwa Informacji w Urzędzie Gminy w Żarnowie do, których należy przede wszystkim:
   1. sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania dla administratora,
   2. prowadzenie szkoleń dla pracowników Urzędu Gminy Żarnów z zakresu ochrony danych osobowych,
   3. prowadzenie rejestru zbiorów danych przetwarzanych przez administratora danych,
   4. wydawanie i anulowanie upoważnień do przetwarzania danych osobowych na podstawie pełnomocnictwa udzielonego przez ADO,
   5. prowadzenie postępowania wyjaśniającego w przypadku naruszenia ochrony danych osobowych,
   6. prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych.

Rozdział 8
Zadania Informatyka pełniącego obowiązki Administratora Systemu Informatycznego (ASI)

§ 15.

1. ASI odpowiedzialny jest za:
   1. bieżący monitoring i zapewnienie ciągłości działania Systemu Informatycznego oraz baz danych, instalacje i konfiguracje sprzętu sieciowego i serwerowego,
   2. instalacje i konfiguracje oprogramowania systemowego, sieciowego,

3. konfigurację i administrowanie oprogramowaniem systemowym, sieciowym oraz zabezpieczającym dane chronione przed nieupoważnionym dostępem,
4. nadzór nad zapewnieniem awaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych,
5. współpracę z dostawcami usług oraz sprzętu sieciowego i serwerowego oraz zapewnienie zapisów dotyczących ochrony danych,
6. zarządzanie kopiami awaryjnymi konfiguracji oprogramowania systemowego, sieciowego,
7. zarządzanie kopiami awaryjnymi danych osobowych oraz zasobów umożliwiających ich przetwarzanie,
8. przeciwdziałanie próbom naruszenia bezpieczeństwa informacji,
9. przyznawanie na wniosek Administratora lub IOD ściśle określonych praw dostępu do informacji w Systemach,
10. wnioskowanie do Administratora lub IOD w sprawie zmian lub usprawnienia procedur bezpieczeństwa i standardów zabezpieczeń,
11. zarządzanie licencjami, procedurami ich dotyczącymi,
12. prowadzenie profilaktyki antywirusowej.

2. Praca ASI jest nadzorowana pod względem przestrzegania RODO, ustawy o ochronie danych osobowych, oraz Polityki ochrony danych Organizacji przez Administratora lub IOD.

Rozdział 9
Sprawozdanie roczne z funkcjonowania systemu ochrony danych

§ 16.

1. Corocznie do dnia 31 stycznia kolejnego roku IOD przygotowuje sprawozdanie roczne z funkcjonowania systemu ochrony danych i przekazuje do Administratora.
2. Sprawozdanie przygotowywane jest w formie pisemnej.

Rozdział 10
Postanowienia końcowe

§ 17.

1. Każdy użytkownik przed dopuszczeniem do pracy z Systemem przetwarzającym dane lub zbiorami danych w formie tradycyjnej winien być poddany przeszkoleniu w zakresie ochrony danych.
2. Za przeprowadzenie szkolenia odpowiada Administrator, ASI lub IOD.
3. Zakres szkolenia powinien obejmować zaznajomienie użytkownika z przepisami RODO, ustawie o ochronie danych osobowych oraz wydanymi na jej podstawie aktami wykonawczymi oraz Polityką ochrony danych i innymi związanymi z nią dokumentami obowiązującymi u Administratora.

Załącznik nr 1
do Polityki ochrony danych osobowych
w Urzędzie Gminy w Żarnowie

Instrukcja Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Żarnów

Postanowienia ogólne

§ 1.

Podstawę prawną do opracowania i wdrożenia niniejszej instrukcji stanowią ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2018 r. poz. 1000 z późn. zm.) oraz Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. nr 100 poz. 1024). Instrukcja stanowi zestaw procedur opisujących zasady zapewnienia bezpieczeństwa danych osobowych w systemach i aplikacjach informatycznych.

Definicje

§ 2.

Ilekroć w niniejszym dokumencie jest mowa o:

1. **Urzędzie**– należy przez to rozumieć Urząd Gminy w Żarnowie.
2. **Administratorze Danych Osobowych (ADO)** – należy przez to rozumieć Wójta Gminy (zwany dalej Administratorem) decydującego o celach i środkach przetwarzania danych osobowych.
3. **Inspektor Ochrony Danych (IOD)** – osoba wyznaczona przez Administratora, nadzorująca przestrzeganie zasad i wymogów ochrony danych określonych w RODO i przepisach krajowych;
4. **Administrator Systemu Informatycznego (ASI)** – osoba upoważniona przez Administratora, odpowiedzialna za bezpieczeństwo danych osobowych przetwarzanych we wskazanych systemach informatycznych, nadzorująca pracę systemu informatycznego oraz wykonująca w nim czynności wymagające specjalnych uprawnień. ASI odpowiedzialny jest za sprawność, konserwację oraz wdrażanie technicznych zabezpieczeń systemu informatycznego do przetwarzania danych osobowych.
5. **Użytkownik systemu** – należy przez to rozumieć osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym urzędu.

Postanowienia ogólne

§ 3.

1. Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w urzędzie zwana dalej „Instrukcją" określa zasady, tryb postępowania i zalecenia Administratora Danych Osobowych, które muszą być stosowane przez osoby przez niego upoważnione do przetwarzania danych osobowych w systemach informatycznych.
2. Instrukcja została opracowana zgodnie z wymogami § 5 Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. nr 100 poz. 1024).
3. Podstawowymi celami zabezpieczeń systemów informatycznych służących do przetwarzania danych osobowych jest zapewnienie jak najwyższego poziomu bezpieczeństwa przetwarzanych danych osobowych w systemach informatycznych.
4. Za priorytet uznano zagwarantowanie zgromadzonym danym osobowym, przez cały okres ich przetwarzania w systemach, charakteru poufnego wraz z zachowaniem ich integralności i rozliczalności.

Obowiązki w zakresie ochrony danych osobowych

§ 4.

1. Do obowiązków osób zaangażowanych w przetwarzanie danych osobowych w systemach informatycznych należy:
   a. podejmowanie współpracy przy ustaleniu przyczyn naruszenia ochrony danych osobowych oraz usuwania skutków tych naruszeń, w tym zapobieganie ich ewentualnemu ponownemu wystąpieniu,
   b. przetwarzanie danych osobowych wyłącznie w celach określonych przez swoich przełożonych.
2. Do kompetencji osób zarządzających pracownikami należy w szczególności wystawianie dla bezpośrednio podległych pracowników wniosków o nadanie, zmianę lub cofnięcie uprawnień do systemów informatycznych, w których są przetwarzane dane osobowe.
3. Użytkownicy powinni podlegać okresowym szkoleniom, stosownie do potrzeb wynikających ze zmian w systemie informatycznym (wymiana sprzętu na nowszej generacji, zmiana oprogramowania) oraz w związku ze zmiana przepisów o ochronie danych osobowych lub zmiana wewnętrznych regulacji.

Poziom bezpieczeństwa

§ 5.

W Urzędzie Gminy w Żarnowie obowiązuje wysoki poziom bezpieczeństwa systemu informatycznego z uwagi na to, że jest on połączony z siecią publiczną (z Internetem).

Bezpieczna eksploatacja sprzętu i oprogramowania
§ 6.

Celem procedury jest określenie wymagań bezpieczeństwa dla sprzętu i oprogramowania eksploatowanego w Urzędzie Gminy w Żarnowie. Bezpieczna eksploatacja systemów informatycznych przetwarzających dane osobowe zostaje zapewniona poprzez przestrzeganie następujących zasad:

1. Użytkownikom zabrania się wprowadzania zmian do oprogramowania, sprzętu informatycznego poprzez jego samodzielne konfigurowanie i wyposażanie.
2. Użytkownikom zabrania się umożliwiania stronom trzecim uzyskiwania nieupoważnionego dostępu do systemów informatycznych.
3. Użytkownikom nie wolno instalować nowego lub aktualizować już zainstalowanego oprogramowania.
4. Użytkownikom nie wolno korzystać z systemów informatycznych dla celów innych niż związane z wykonywaniem obowiązków służbowych.
5. Użytkownikom nie wolno podejmować prób testowania, modyfikacji i naruszenia zabezpieczeń systemów informatycznych lub jakichkolwiek działań noszących takie znamiona.
6. Informacje przetwarzane przy użyciu współdzielonych aplikacji sieciowych na stacjach roboczych muszą być zapisane na dyskach serwera.
7. Wszystkie aplikacje sieciowe, współdzielone zasoby użytkowe muszą być ulokowane na przeznaczonych do tego celu serwerach.
8. Nieautoryzowane podłączenie własnego lub strony trzeciej urządzenia teleinformatycznego do systemu informatycznego jest zabronione.
9. Urządzenia aktywne obsługujące sieć lokalną urzędu chronią ja na poziomie warstwy łącza danych na ewentualność podłączenia obcych urządzeń.
10. Ekrany monitorów są wyposażone w wygaszacze zabezpieczone hasłem, które aktywują się automatycznie po upływie określonego czasu od ostatniego użycia komputera.
11. Programy zainstalowane na komputerach obsługujących przetwarzanie danych osobowych są użytkowane z zachowaniem praw autorskich i posiadają licencje.
12. Instalacji oprogramowania może dokonywać jedynie Administrator Systemu Informatycznego (ASI). W razie konieczności instalacji oprogramowania przez pracowników firm zewnętrznych czynność ta powinna być wykonywana za przyzwoleniem i w obecności pracownika komórki informatyzacji.
13. System Informatyczny wyposażony jest w mechanizmy oraz uwierzytelnienia użytkownika sprawujące kontrole dostępu do danych osobowych jedynie osób upoważnionych.
14. Użytkownikom nie wolno uruchamiać oprogramowania z innych źródeł (nośniki wymienne, Internet) bez zgody Administratora Systemu Informatycznego (ASI).
15. Komputer przenośny może być używany do przetwarzania danych osobowych po odpowiednim jego zabezpieczeniu.
16. Użytkownik korzystający z komputera przenośnego jest zobowiązany do zachowania szczególnej ostrożności podczas transportu komputera oraz nie może udostępniać komputera osobom nieupoważnionym.
17. Ekrany monitorów są ustawione w miarę możliwości w taki sposób, żeby uniemożliwić odczyt wyświetlanych informacji osobom nieupoważnionym.

Procedury korzystania z Internetu i poczty elektronicznej
§ 7.

1. Celem procedury jest uregulowanie zasad korzystania z Internetu i poczty elektronicznej, aby zagwarantować bezpieczeństwo danych osobowych przesyłanych przez media. Użytkownicy Internetu zobowiązani są do przestrzegania następujących zasad:
   a. zakazuje się ściągania przez użytkowników plików lub przeglądania zasobów informacyjnych o treści prawnie zabronionej, obscenicznej bądź pornograficznej,
   b. zaleca się, aby do wymiany korespondencji w czasie korzystania z systemu informatycznego urzędu wykorzystywać jedynie służbową pocztę elektroniczną,
   c. szczególne rygory należy stosować wobec ściągania z Internetu plików wykonywalnych. Użytkownik ponosi odpowiedzialność za szkody spowodowane przez oprogramowania ściągnięte z Internetu i przez niego używane,
   d. do korzystania z Internetu użytkownicy mogą wykorzystywać jedynie zaakceptowane przez Administratora Systemu Informatycznego (ASI) formy dostępu (dotyczy prób obchodzenia poustawianych obostrzeń oraz podłączania dodatkowych urządzeń komunikacyjnych).
2. Użytkownicy systemu poczty elektronicznej zobowiązani są do przestrzegania następujących zasad:
   a. przesyłanie informacji za pośrednictwem poczty elektronicznej winno odbywać się zgodnie z uprawnieniami adresatów do korzystania z określonego typu danych. W przypadku wątpliwości nadawca powinien sprawdzić, czy dana osoba ma uprawnienia do korzystania z dokumentów danego typu lub o określonej klauzuli poprzez skonsultowanie się z Administratorem Systemu Informatycznego (ASI),
   b. jeśli adresatem wiadomości zawierającej dane osobowe jest pracownik urzędu zaleca się doręczenia danych w formie elektronicznej w sposób wykorzystujący wewnętrzne mechanizmy przekazywania danych (dyski sieciowe, udostępnienia folder użytkownika docelowego),
   c. przesyłanie informacji poza obręb urzędu może odbywać się tylko przez osoby do tego upoważnione do adresatów upoważnionych do przesyłanych danych,
   d. w razie konieczności przesyłania danych osobowych dane te należy uprzednio odpowiednio zabezpieczyć wykorzystując mechanizmy kompresji z szyfrowaniem z tym zastrzeżeniem, że hasło musi zostać dostarczone do adresata drogą inną niż same dane (np. przez telefon). Złożoność hasła: na poziomie minimum 10 znaków w tym duża, mała litera, znak specjalny oraz cyfra,
   e. użytkownicy powinni zwrócić szczególna uwagę na poprawność adresu odbiorcy dokumentu,
   f. jeżeli istotne jest potwierdzenie otrzymania przez adresata przesyłki, użytkownik winien skorzystać, o ile jest to technicznie możliwe, z opcji systemu poczty elektronicznej informującej o dostarczeniu i otwarciu dokumentu. Dodatkowo zaleca się, aby użytkownik zawarł w treści dokumentu prośbę o potwierdzenie otrzymania i zapoznania się z informacją. Adresat zobowiązany jest w takiej sytuacji przesłać nadawcy potwierdzenie,
   g. informacje przesyłane za pośrednictwem poczty elektronicznej muszą być zgodne z prawem i z zasadami zawartymi w Polityce Bezpieczeństwa Danych Osobowych obowiązującej w Urzędzie Gminy w Żarnowie,

h. użytkownicy nie powinni otwierać przesyłek od nieznanych sobie osób, których tytuł nie sugeruje związku z wypełnianymi przez nich obowiązkami służbowymi. W przypadku otrzymania takiej przesyłki, użytkownik powinien ją zniszczyć lub skontaktować się z Administratorem Systemu Informatycznego (ASI),

i. użytkownicy nie powinni uruchamiać wykonywalnych załączników (pliki. exe) dołączonych do wiadomości przesyłanych pocztą elektroniczną. W takim przypadku użytkownik powinien poinformować o zdarzeniu Inspektora Ochrony Danych (IOD), który winien sprawdzić, czy załącznik stanowi zagrożenie dla przetwarzanych w systemie informatycznym informacji,

j. użytkownicy nie powinni rozsyłać za pośrednictwem poczty elektronicznej informacji o zagrożeniach dla systemu informatycznego „łańcuszków szczęścia",

k. użytkownicy nie powinni rozsyłać, wiadomości zawierających załączniki o dużym rozmiarze (powyżej 10 MB) do większej liczby adresatów. W razie konieczności przesłania większych załączników winni skontaktować się z Informatykiem,

l. użytkownicy powinni okresowo kasować niepotrzebne wiadomości pocztowe.

Procedura nadawania uprawnień do przetwarzania danych osobowych

§ 8.

Celem procedury jest zapewnienie użytkownikom odpowiednich uprawnień do przetwarzania danych osobowych, aby redukować zagrożenie nieuprawnionego dostępu do danych osobowych i utraty poufności.

1. Każdy użytkownik systemu przed przystąpieniem do przetwarzania danych osobowych musi zapoznać się z:
   - **a.** ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2018, poz. 1000 z późn. zm.);
   - **b.** polityką ochrony danych osobowych w Urzędzie Gminy w Żarnowie;
   - **c.** niniejszym dokumentem.
2. Zapoznanie się z powyższymi informacjami pracownik potwierdza własnoręcznym podpisem na oświadczeniu, którego wzór stanowi załącznik.
3. Administrator Systemu Informatycznego przyznaje uprawnienia w zakresie dostępu do systemu informatycznego na podstawie pisemnego zlecenia złożonego przez bezpośredniego przełożonego pracownika, którego zlecenie dotyczy.
4. Zlecenie to podlega zatwierdzeniu przez IOD, na podstawie którego wydane zostaje upoważnienie do przetwarzania danych osobowych – wzór upoważnienia stanowi załącznik nr 4. Upoważnienia do przetwarzania danych osobowych wydaje ADO.
5. Przyznanie uprawnień w zakresie dostępu do systemu informatycznego polega na wprowadzeniu do systemu dla każdego użytkownika unikalnego identyfikatora, hasła oraz zakresu dostępnych danych i operacji.
6. Hasło ustawione podczas przyznawania uprawnień przez Administratora Systemu Informatycznego (ASI) należy zmienić na indywidualne podczas pierwszego logowania się w systemie.
7. Pracownik ma prawo do wykonywania tylko tych czynności, do których został upoważniony.

8. Pracownik ponosi odpowiedzialność za wszystkie operacje wykonane przy użyciu jego identyfikatora i hasła dostępu.
9. Odbieranie uprawnień pracownikowi następuje na pisemny wniosek przełożonego, któremu pracownik podlega z podaniem daty oraz przyczyny odebrania uprawnień.
10. Identyfikator osoby, która utraciła uprawnienia do dostępu do danych osobowych należy bezzwłocznie wyrejestrować z systemu informatycznego, w którym są one przetwarzane oraz unieważnić jej hasło.
11. Administrator Systemu Informatycznego (ASI) zobowiązany jest do prowadzenia i ochrony rejestru użytkowników i ich uprawnień w systemie informatycznym.

Metody i środki uwierzytelniające
§ 9.

Celem procedury jest zapewnienie, że do systemów informatycznych przetwarzających dane osobowe mają dostęp jedynie osoby do tego upoważnione.

Identyfikatory i hasła są sposobem zagwarantowania rozliczalności, poufności i integralności danych osobowych przetwarzanych w systemach informatycznych.

Służą do weryfikowania tożsamości użytkownika, uzyskania dostępu do określonych zasobów, kont uprzywilejowanych lub uruchomienia określonej funkcjonalności.

1. Wszystkie konta dostępowe (identyfikatory) do systemów informatycznych powinny być chronione hasłem lub innym bezpiecznym, zaakceptowanym przez Administrator Systemu Informatycznego (ASI) sposobem uwierzytelniania.
2. Identyfikator oraz nadane uprawnienia powinny umożliwiać wykonywanie czynności wyłącznie zgodnych z zakresem powierzonych obowiązków.
3. Identyfikator użytkownika powinien być niepowtarzalny, a po wyrejestrowaniu się z systemu informatycznego nie powinien być przydzielany innej osobie.
4. Identyfikator, który utracił ważność nie może być ponownie przydzielony innemu użytkownikowi.
5. Hasło początkowe, które jest przydzielane przez Administratora Systemu Informatycznego (ASI), powinno umożliwiać użytkownikowi zarejestrowanie się w systemie tylko jeden raz i powinno być natychmiast zmienione przez użytkownika. Mając na uwadze zagwarantowanie wysokiego poziomu bezpieczeństwa przetwarzania danych osobowych oraz zagwarantowania użytkownikom pełnej rozliczalności wykonywanych przez nich operacji w systemach informatycznych, wszyscy użytkownicy przy uwierzytelnianiu do systemów informatycznych powinni stosować się do poniższych zasad:
   a. pierwsze hasło dla użytkownika ustala, przydziela ASI przy wprowadzaniu identyfikatora użytkownika do systemu,
   b. użytkownik systemu niezwłocznie ustala swoje, znane tylko jemu hasło, po nadaniu hasła przez ASI,
   c. użytkownik systemu w trakcie pracy w aplikacji może zmienić swoje hasło dostępu,
   d. hasła nie mogą być powszechnie używanymi słowami. W szczególności nie należy wykorzystywać: dat, imion, nazwisk, inicjałów, numerów rejestracyjnych samochodów, numerów telefonów,
   e. hasło nie może być ujawnione nawet po utracie przez nie ważności,

f. hasła mają charakter poufny – są znane tylko jego właścicielowi,
g. zabronione jest zapisywanie haseł w sposób jawny oraz przekazywanie ich innym osobom,
h. hasło winno składać się z co najmniej 8 znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne,
i. hasła administratora do poszczególnych programów/systemów powinny być spisane oraz umieszczone w zamkniętej kopercie w miejscu uniemożliwiającym dostęp do nich osobom nieupoważnionym, chroniącym przed utratą lub zniszczeniem oraz gwarantującym ich odczytanie upoważnionemu użytkownikowi, a także kierownikowi urzędu,
j. zarejestrowane hasła administratora, oprócz treści hasła winny posiadać adnotację o dacie ich wprowadzenia do systemu,
k. w przypadku utraty uprawnień przez osobę administrującą systemem należy niezwłocznie zmienić hasła, do których miała dostęp.

Wymogi dotyczące zmiany haseł
§ 10.

1. Użytkownik jest zobowiązany zmieniać hasło, w którego posiadaniu się znajduje:
   a. okresowo, zgodnie z wymaganiami dla danego systemu informatycznego (przed upływem terminu ważności hasła).
   b. w przypadku ujawnienia lub podejrzenia ujawnienia hasła.
2. W przypadku braku dostępu do konta chronionego hasłem, w którego posiadaniu się znajduje, użytkownik zobowiązany jest wystąpić o zmianę hasła do ASI, w sytuacji:
   a. zapomnienia/zgubienia hasła,
   b. wygaśnięcia ważności hasła,
   c. zablokowania konta spowodowanego nieprawidłowym wprowadzeniem hasła,
   d. braku uprawnień/interfejsu umożliwiających samodzielną zmianę hasła.
3. Zmiana haseł użytkowników powinna być wymuszana przez system co 30 dni, w przypadku braku wymuszenia przez system, użytkownik sam jest zobowiązany do zmiany hasła co 30 dni.

Procedura rozpoczęcia, zawieszenia i zakończenia pracy
§ 11.

Celem procedury jest zabezpieczenie danych osobowych przed nieuprawnionym dostępem i utratą poufności w sytuacji, gdy użytkownik rozpoczyna, przerywa lub kończy pracę w systemie informatycznym przetwarzającym dane osobowe.

1. Rozpoczynając prace na komputerze użytkownik loguje się do systemu informatycznego.
2. Dostęp do danych osobowych możliwy jest jedynie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia użytkownika.
3. Jeśli system to umożliwia, po przekroczeniu 5 prób logowania system blokuje dostęp do systemu informatycznego na poziomie danego użytkownika.
4. ASI ustala przyczyny zablokowania systemu oraz w zależności od zaistniałej sytuacji podejmuje odpowiednie działania. O zaistniałym incydencie powiadamia Inspektora Ochrony Danych (IOD).

5. Przed opuszczeniem stanowiska pracy, użytkownik obowiązany jest:
   a. wylogować się z systemu informatycznego, lub
   b. wywołać blokowany hasłem wygaszacz ekranu.
6. Kończąc pracę należy:
   a. wylogować się z systemu informatycznego, a następnie wyłączyć sprzęt komputerowy,
   b. zabezpieczyć stanowisko pracy, w szczególności wszelką dokumentację oraz nośniki magnetyczne i optyczne, na których znajdują się dane osobowe.

Procedura tworzenia kopii zapasowych
§ 12.

Tworzenie kopii bezpieczeństwa danych osobowych z programów.

1. Kopie zapasowe danych z programów przetwarzających dane osobowe wykonywane są na koniec każdego dnia roboczego z wykorzystaniem odpowiednio skonfigurowanych zasobów sieciowych urzędu.
2. Kopie zapasowe na macierz dyskową wykonuje się w cyklu dziennym oraz miesięcznym.
3. Zapis kopii zapasowych na macierzy dyskowej dokonuje się w sposób rotacyjny, zapewniający zachowanie kopii miesięcznych z okresu minimum 3 miesięcy, po tym okresie kopia jest usuwana.
4. W wypadku użycia nośnika zewnętrznego kopie zapasowe są odpowiednio oznakowane.
5. Poza macierzą dyskową miesięczne kopie bezpieczeństwa przechowywane są na serwerach plików odpowiednio do tego celu zabezpieczonych.
6. ASI sprawuje nadzór nad wykonywaniem kopii zapasowych oraz weryfikuje ich poprawność.

Sposób, miejsce i okres przechowywania elektronicznych nośników informacji i wydruków.
§ 13.

Procedura określa sposób postępowania z nośnikami, na których znajdują się dane osobowe, celem zabezpieczenia ich przed niszczeniem, kradzieżą, dostępem osób nieupoważnionych.

1. Dane osobowe mogą być przechowywane:
   a. na serwerach zlokalizowanych w obszarach wyznaczonych do przetwarzania danych osobowych,
   b. na wymiennych nośnikach elektronicznych.
2. Po wykorzystaniu dane osobowe w postaci elektronicznej należy niezwłocznie usunąć z nośnika elektronicznego w sposób uniemożliwiający ich ponowne odtworzenie.
3. Wykorzystanie wymiennych nośników elektronicznych (CD/DVD, pamięć USB, wymienna karta pamięci, dyskietka) powinno być ściśle kontrolowane i dozwolone wyłącznie dla upoważnionych użytkowników.
4. Wymienne nośniki elektroniczne, o ile nie są użytkowane, powinny być przechowywane w zamykanych szafach.

5. Nośniki zawierające kopie zapasowe powinny być przechowywane w innym pomieszczeniu niż to, w którym umieszczony jest serwer przetwarzający dane osobowe.
6. Kopie zapasowe powinny być przechowywane w odpowiednio zabezpieczonej, ognioodpornej szafie, do której dostęp mogą mieć wyłącznie osoby upoważnione.
7. Nośniki magnetyczne i optyczne z danymi osobowymi powinny być:
   a. oznaczone i przechowywane w zamykanych szafach lub sejfach,
   b. przechowywane maksymalnie przez okres wskazany dla danego rodzaju danych osobowych przez Administratora Danych Osobowych (ADO).
8. Pracownicy nie mogą wynosić na zewnątrz urzędu wymiennych elektronicznych nośników informacji z zapisanymi danymi osobowymi bez zgody IOD.
9. Dane osobowe w postaci elektronicznej należy usuwać z nośnika informacji w sposób uniemożliwiający ich ponowne odtworzenie, nie później niż po upływie tygodnia, po wykorzystaniu tych danych, chyba, że z odrębnych przepisów wynika obowiązek ich przechowywania.
10. Uszkodzone nośniki komputerowe, zawierające dane osobowe, są fizycznie niszczone przy udziale komisji powołanej przez Administratora Danych Osobowych (ADO), który sporządza protokół z wykonywanych czynności.
11. Nośnik danych są przechowywane w sposób uniemożliwiający dostęp do nich osób nieupoważnionych, jak również zabezpieczający je przed zagrożeniami środowiskowymi (zalanie, pożar).
12. Zaleca się, aby informacje wewnętrzne znajdujące się na nośnikach przenośnych, wynoszonych poza teren placówki, były szyfrowane.
13. Kopie zapasowe:
   a. kopie zapasowe zbioru danych osobowych oraz oprogramowania i narzędzi programowych zastosowanych do przetwarzania danych są przechowywane w metalowej szafie w Urzędzie Gminy w Żarnowie, w pokoju nr ASI.
   b. dostęp do kopii zapasowych mają tylko upoważnieni pracownicy, tj. IOD oraz ASI.
   c. cotygodniowe kopie bezpieczeństwa przechowywane są przez ASI do momentu kolejnego nagrania wynikającego z cyklu rotacyjnego zapisu nośników.
14. Kopie archiwalne miesięczne przechowywane są przez okres ok. 3 miesięcy, po czym nośnik poddawany jest kolejnemu procesowi zapisania danych archiwalnych.
15. Nośniki, na których znajdują się kopie zawierające dane osobowe, są oznaczone w sposób trwały, jednoznaczny i czytelny i zaewidencjonowany w „Rejestrze nośników komputerowych zawierających ważne dane" stanowiącym.
16. Kopie archiwalne należy:
   a. okresowo sprawdzać pod kątem ich dalszej przydatności do odtwarzania,
   b. bezzwłocznie usuwać po ustaniu użyteczności.
17. Wydruki
   a. wydruki/dokumenty np.: umowy, faktury, zawierające dane osobowe, przechowuje się w pokojach stanowiących obszar przetwarzania danych osobowych, określony w polityce ochrony danych osobowych,
   b. wydruki/dokumenty, zawierające dane osobowe, należy niszczyć przez pojęcie w niszczarce lub spalać w miejscu do tego wyznaczonym.
18. Za bezpieczeństwo danych osobowych zapisanych w formie tradycyjnej odpowiedzialne są osoby je przetwarzające.

Procedura zabezpieczenia systemu informatycznego, przed działalnością oprogramowania złośliwego
§ 14.

Za ochronę antywirusową odpowiada ASI. Na każdej stacji roboczej w sieci oraz serwerze przetwarzającym dane osobowe powinno być zainstalowane oprogramowanie antywirusowe skanujące na bieżąco system informatyczny.

1. Każdy komputer z dostępem do danych osobowych wyposażony jest w skaner antywirusowy.
2. Programy antywirusowe, winne być uaktywnione cały czas podczas pracy danego systemu.
3. Wszystkie pliki otrzymane z zewnątrz, jak również wysyłane na zewnątrz, podlegają sprawdzeniu pod kątem występowania wirusów najnowszą dostępną wersją programu antywirusowego.
4. W przypadku stwierdzenia pojawienia się wirusów, każdy użytkownik winien powiadomić ASI.

Zasady i sposób odnotowywania w systemie informacji o udostępnieniu danych osobowych
§ 15.

1. Odbiorcą danych jest każdy, komu udostępnia się dane osobowe, z wyłączeniem:
   a. osoby, której dane dotyczą,
   b. osoby – użytkownika systemu lub innej osoby upoważnionej do przetwarzania danych osobowych w urzędzie,
   c. podmiotu, któremu powierzono przetwarzanie danych,
   d. organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem,
   e. dane osobowe administrowane przez Urząd Gminy w Żarnowie mogą być udostępnione osobom lub podmiotom uprawnionym do ich otrzymania na mocy ustawy o ochronie danych osobowych oraz innych przepisów powszechnie obowiązujących.
2. Dane osobowe udostępnia sią na pisemny, umotywowany wniosek, chyba, że przepis innej ustawy stanowi inaczej.
3. Dane udostępniane urzędowi przez inny podmiot można wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.
4. IOD prowadzi ewidencje udostępniania danych, o których mowa w pkt. 2. „Ewidencję udostępniania danych osobowych innym podmiotom" przedstawia załącznik nr 6.
5. Odnotowanie obejmuje informację o:
   a. nazwie jednostki organizacyjnej lub imieniu i nazwisku osoby, której udostępniono dane,
   b. zakresie udostępnianych danych,
   c. dacie udostępniania.
6. Odnotowanie informacji powinno nastąpić niezwłocznie po udostępnieniu danych.
7. Na żądanie osoby, której dane zostały udostępnione, informacje o udostępnienie danych są zamieszczane w pisemnym raporcie.

8. Realizacja wymogów, o których mowa w § 7 ust. 1 pkt 4 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. spełniona jest poprzez prowadzenie „Ewidencji udostępniania danych".

Procedury wykonywania przeglądów i konserwacji

§ 16.

1. Aktualizacja oprogramowania powinna być przeprowadzana zgodnie z zaleceniami producentów oraz opinią rynkową co do bezpieczeństwa i stabilności nowych wersji.
2. Za terminowość przeprowadzenia przeglądów i konserwacji oraz ich prawidłowy przebieg odpowiada ASI.
3. Zauważone nieprawidłowości w działaniach systemu informatycznego oraz oprogramowanie powinny być niezwłocznie usunięte, a ich przyczyny przeanalizowane.
4. Wszelkie prace konserwacyjne i naprawcze sprzętu komputerowego oraz uaktualnianie systemu informatycznego, wykonywane przez podmiot zewnętrzny, powinny odbywać się na zasadach określonych w szczegółowej umowie z uwzględnianiem klauzuli dotyczącej ochrony danych.
5. W przypadku naprawy sprzętu komputerowego dane osobowe należy zabezpieczyć, natomiast w przypadku naprawy sprzętu poza terenem danej jednostki, po zabezpieczeniu usunąć z dysku. Gdy nie ma możliwości usunięcia danych, naprawa powinna być nadzorowana przez osobę upoważnioną przez administratora systemu.

Plan ciągłości działania na wypadek awarii systemu informatycznego

§ 17.

1. Celem procedury jest minimalizacja zakłóceń w realizacji działalności Urzędu Gminy w Żarnowie w związku z wystąpieniem zdarzeń mających wpływ na działanie systemu informatycznego w jednostce.
2. Przedmiotem procedury jest określenie sposobu działania w razie zaistnienia zdarzeń mających wpływ na działanie systemu informatycznego.
3. Każdy użytkownik systemu (pracownik) w razie zaistnienia awarii jest zobowiązany do jej zgłoszenia działowi informatycznemu.
4. Typowe rodzaje incydentów:
   a. Awaria serwera,
   b. Awaria komputera,
   c. Awaria urządzeń aktywnych sieci,
   d. Awaria infrastruktury sieciowej,
   e. Awaria oprogramowania,

   Przy czym przez awarie rozumie się stan niesprawności w/w elementów systemu informatycznego uniemożliwiający jego funkcjonowanie, występujący nagle i powodujący jego niewłaściwe działanie lub całkowite unieruchomienie.
5. Przyczynami powyżej wymienionych zdarzeń mogą być m.in.:
   a. umyślne lub nieumyślne działania osób zatrudnionych w jednostce,
   b. ingerencja osób zewnętrznych (m. in. atak hackerski),
   c. zdarzenie losowe (zanik zasilania, zalanie)

6. O uruchomieniu procedury decyduje:
   a. kierownik jednostki,
   b. Inspektor Ochrony Danych,
   c. kierownicy poszczególnych Referatów (po poinformowaniu kierownika jednostki)
   d. Administrator Systemu Informatycznego

7. W razie wystąpienia awarii należy wypełnić wszystkie punkty poniższego planu:

Lp.	Działanie	Opis działania
1.	Zweryfikować zasadność zgłoszenia od użytkownika.	Sprawdzić, czy zgłoszenie dotyczy zdarzenia spowodowanego awarią systemu informatycznego.
2.	Ustalić źródło awarii.	Ustalić, co jest przyczyną awarii: • przerwa w zasilaniu prądem, • brak połączenia z siecią Internet, • wadliwe działanie sprzętu, • wadliwe działania aplikacji, • wadliwe działanie systemu, na którym jest uruchomiona aplikacja.
3.	Określić skalę awarii.	Ustalić, czy awaria powoduje zatrzymanie pracy: • jednego pomieszczenia pracy lub działu, • kilku pomieszczeń lub działów, • całego budynku, • wszystkich budynków.
4.	Ustalić, czy wznawianie usługi może odbywać się w dotychczasowej lokalizacji.	Działanie ma na celu zweryfikowanie, czy wznawianie usługi uruchamiane będą w dotychczasowej lokalizacji, czy w lokalizacjach alternatywnych.
5.	Zakupić niezbędne elementy wyposażenia, dokonać naprawy (wymiany) urządzeń, uruchomić aplikację.	W przypadku braku możliwości zakupu należy znaleźć rozwiązanie alternatywne (np. zdecydować o przeniesieniu aplikacji na stałe na inny serwer).
6.	Przygotować serwer zastępczy.	Jako serwer zastępczy można wykorzystać np. komputer typu desktop, który należy odpowiednio skonfigurować. Po uruchomieniu aplikacji na serwerze zastępczym należy przetestować jej działanie.
7.	Podjąć decyzję o terminie odtworzenia maszyny.	W razie konieczności należy skontaktować się z właściwymi kierownikami komórek organizacyjnych.
8.	Przywrócić funkcjonowanie aplikacji / systemu.	Spróbować usunąć przyczynę nieprawidłowego działania. W razie konieczności należy odtworzyć aplikację korzystając z kopii zapasowych.
9.	Sprawdzenie aplikacji / systemu.	Po przeniesieniu / uruchomieniu należy zweryfikować prawidłowe funkcjonowanie aplikacji / systemów zainstalowanych na serwerze.
10.	Uruchomienie usługi w systemie informatycznym.	Po uruchomieniu usługi należy powiadomić właściwych kierowników o tym fakcie.

11.	Określić czy awaria / incydent miała wpływ na przetwarzanie danych osobowych.	• Określić czy dane osobowe przetwarzane w systemie zostały utracone, zmodyfikowane lub udostępnione osobom postronnym. • Poinformować Inspektora Ochrony Danych o awarii / incydencie mającym wpływ na dane osobowe. • Zastosować się do wytycznych Inspektora Ochrony Danych

W przypadku wystąpienia awarii / incydentu jest on odnotowywany w dzienniku ASI, który jest niezwłocznie dostarczany Inspektorowi Ochrony Danych. Dziennik ASI prowadzony jest na podstawie odrębnych dokumentów obowiązujących w jednostce.

W celu realizacji niniejszej procedury administrator danych osobowych (kierownik jednostki) zapewnia środki materialne i osobowe w celu doprowadzenia do zgodności z przepisami prawa m. in.:

- kontakt z kluczowymi pracownikami działów, lista z numerami telefonów,
- dostęp do najbardziej aktualnej wersji aplikacji,
- dostęp do aktualnej bazy danych,
- zapewnienie środków, dowolnego typu, które w podstawowym zakresie pozwolą na zrealizowanie niniejszej procedury.

Administrator Danych Osobowych może wykonać powyższe przy użyciu Administratora Systemu Informatycznego

Załącznik nr 2
do Polityki ochrony danych osobowych
w Urzędzie Gminy w Żarnowie

Rejestr zbioru danych osobowych- RODOprotektor

Załącznik nr 3
do Polityki ochrony danych osobowych
w Urzędzie Gminy w Żarnowie

Ewidencja osób upoważnionych – RODOprotektor

Załącznik nr 4
do Polityki ochrony danych osobowych
w Urzędzie Gminy w Żarnowie

UPOWAŻNIENIE
DO PRZETWARZANIA DANYCH OSOBOWYCH [UPDO-2]

W oparciu o ROZPORZĄDZENIE 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.

NR _____ z dnia

PRACOWNIK _____ ID:

PODSTAWA _____

STANOWISKO _____

Zbiór danych osobowych	Zakres upoważnienia	Programy i zasoby	Data udzielenia	od dnia	do dnia	Akty wny

Upoważniający (podpis)	Pracownik (podpis)

RODOprotektor

Załącznik nr 5
do Polityki ochrony danych osobowych
w Urzędzie Gminy w Żarnowie

Rejestr osób upoważnionych- RODOprotektor

Załącznik nr 6
do Polityki ochrony danych osobowych
w Urzędzie Gminy w Żarnowie

EWIDENCJA UDOSTĘPNIONYCH DANYCH OSOBOWYCH INNYM PODMIOTOM

L.p.	**Imię i Nazwisko/Nazwa zbioru** *(możliwie najpełniejszy opis osoby, której dane zostały udostępnione lub całego zbioru)*	**Data udostępnienia**	**Nazwa podmiotu, któremu udostępniono dane** *(np. upoważniony organ, instytucja lub inny, który wykazał uprawnienie do udostępnienia mu danych)*	**Cel udostępnienia** *(podstawa prawna/numer umowy)*	**Zakres udostępnionych danych** *(jakie dane zostały udostępnione)*	**Rodzaj zbioru/zasobu i jego lokalizacja** *(np. papierowy wydruk, dane w formie elektronicznej)*
1.						
2.						
3.						
4.						
5.						
6.						
7.						
8.						
9.						

Załącznik nr 7
do Polityki ochrony danych osobowych
w Urzędzie Gminy w Żarnowie

DZIENNIK UCHYBIEŃ I ZAGROŻEŃ

Lp.	Data i godzina zdarzenia	Rodzaj zdarzenia (uchybienie lub zagrożenie)	Opis zdarzenia	Skutki zdarzenia	Działania naprawcze	Podpis IOD

Załącznik nr 8
do Polityki ochrony danych osobowych
w Urzędzie Gminy w Żarnowie

PROTOKÓŁ UCHYBIENIA/ZAGROŻENIA

Data i godzina wystąpienia uchybienia ……..

Opis uchybienia/zagrożenia

……
……
……
……
…….

Przyczyny powstania uchybienia/zagrożenia

……
……
……
……
…….

Zaistniałe skutki uchybienia/zagrożenia

……
……
……
…….

Podjęte działania naprawczo-zapobiegawcze

……
……
……
…….

Inspektor Ochrony Danych

……..

Administrator Danych Osobowych

…….

Załącznik nr 9
do Polityki ochrony danych osobowych
w Urzędzie Gminy w Żarnowie

Żarnów, dn. …….

……
(Imię i nazwisko)

OŚWIADCZENIE
o zachowaniu poufności

Oświadczam, że zapoznałem/-am się z przepisami dotyczącymi ochrony danych osobowych, w tym z ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r., poz. 1000), wydanych na jej podstawie aktów wykonawczych oraz wprowadzonych i wdrożonych do stosowania przez Administratora Danych Osobowych „Polityki ochrony danych osobowych" oraz Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych".

Zobowiązuję się do:
- nie ujawniania danych osobowych nieuprawnionym osobom lub instytucją w jakiejkolwiek formie bez zgody pracodawcy,
- przestrzegania zapisów zawartych w wyżej wymienionych dokumentach,
- korzystania z oprogramowania wyłącznie w związku z wykonywaniem obowiązków pracowniczych,
- wykorzystywania jedynie legalnego oprogramowania pochodzącego z innych źródeł,
- wnoszenia, wynoszenia i użytkowania komputerów przenośnych bądź innych nośników danych wyłącznie za wiedzą i zgodą pracodawcy,
- należytej dbałości o powierzony sprzęt i oprogramowanie,
-korzystanie z produktów w wersjach ewaluacyjnych, testowych lub w jakichkolwiek inny sposób ograniczony umowami licencyjnymi może być użytkowane zgodnie z ich przeznaczeniem, wyłącznie za zgodą pracodawcy.

Naruszenie przez pracownika jego podstawowych obowiązków pracowniczych w zakresie wskazanym powyżej, będzie stanowić podstawę do podjęcia przez pracodawcę przysługujących mu środków prawnych, a w szczególności, może stanowić przyczynę uzasadniającą wypowiedzenie przez pracodawcę umowy o pracę lub rozwiązanie przez pracodawcę tejże umowy, zgodnie z ustawą z dnia 26 czerwca 1974 r. Kodeks pracy (Dz. U. z 2020 r., poz. 1320).

…….
(data i podpis osoby oświadczającej)