ZARZĄDZENIE NR 2/2017

WÓJTA GMINY RADZYŃ PODLASKI

z dnia 30 stycznia 2017 roku

w sprawie wprowadzenia „Polityki Bezpieczeństwa Informacji" oraz „Instrukcji Zarządzania Systemem Informatycznym" w Urzędzie Gminy Radzyń Podlaski

Na podstawie art. 36 ust. 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. (t.j. Dz. U. z 2016 r. poz. 922), oraz § 3 i 4 rozporządzenia Ministra Spraw Wewnętrznych i Administracyjnych z dnia 29.04.2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych (Dz. U. Nr 100, poz. 1024) w Urzędzie Gminy Radzyń Podlaski

§ 1

Wprowadzam do użytku służbowego **Politykę Bezpieczeństwa Informacji** w brzmieniu załącznika nr 1, określającą zasady zarządzania bezpieczeństwem, informacji i danych osobowych, w Urzędzie Gminy Radzyń Podlaski oraz rozwiązania organizacyjno-techniczne zawarte w **Instrukcji Zarządzania Systemem Informatycznym** w brzmieniu załącznika nr 2.

§ 2

1. Wykonanie zarządzenia powierzam odpowiednio Administratorowi Bezpieczeństwa Informacji, Administratorowi Systemów Informatycznych wskazanym w ww. dokumentach określających zasady nadzoru nad prawidłowością stosowania procedur ochrony danych.

2. Zobowiązuję pracowników do zapoznania się z w/w dokumentami i przestrzegania procedur zawartych w w/w. dokumentach.

§ 3

Zarządzenie wchodzi w życie z dniem podpisania.

Wójt Gminy
Radzyń Podlaski
Wiesław Mazurek

.....

(podpis Wójta - Administratora Danych Osobowych)

Załącznik nr 1
do Zarządzenia nr 2/2017
Wójta Gminy Radzyń Podlaski
z dnia 30 stycznia 2017 r.

POLITYKA BEZPIECZEŃSTWA INFORMACJI URZĘDU GMINY RADZYŃ PODLASKI

	Polityka Bezpieczeństwa Informacji Urzędu Gminy Radzyń Podlaski

Załącznik nr 1
do Zarządzenia nr 2/2017
Wójta Gminy Radzyń Podlaski
z dnia 30 stycznia 2017 r.

Spis treści:

SPIS ZAŁĄCZNIKÓW 2
WPROWADZENIE 3
TERMINOLOGIA 4
PRZEPISY 5
Opis zdarzeń naruszających ochronę danych osobowych 7
Organizacja przetwarzania danych osobowych 8
Infrastruktura przetwarzania danych osobowych 11
Struktura zbiorów danych 11
Powierzenie przetwarzania danych 12
Udostępnienie danych osobowych 12
Strategia zabezpieczenia danych osobowych 13
Postępowanie w przypadku naruszenia ochrony danych osobowych 15
Przegląd polityki bezpieczeństwa i audyt systemu 16
Ochrona budynków i pomieszczeń Urzędu Gminy Radzyń Podlaski 17
Postępowanie w sytuacjach kryzysowych 17
Postanowienia końcowe 19

SPIS ZAŁĄCZNIKÓW	
Załącznik nr 1	Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe
Załącznik nr 2	Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych.
Załącznik nr 3	Rejestr zbiorów danych osobowych
Załącznik nr 4	Wzór oświadczenia podpisywanego przez pracowników
Załącznik nr 5	Wzór wykazu (ewidencji) osób upoważnionych do przetwarzania danych
Załącznik nr 6	Wzór upoważnienia do przetwarzania danych osobowych
Załącznik nr 7	Wykaz osób które zapoznane zostały z Polityką Bezpieczeństwa (PBI) i Instrukcją Zarządzania Systemem Informatycznym (IZSI)
Załącznik nr 8	Wzór raportu z naruszenia bezpieczeństwa systemu informatycznego w Urzędzie
Załącznik nr 9	Instrukcja postępowania na wypadek zagrożenia atakiem terrorystycznym
Załącznik nr 10	Instrukcja postępowania w przypadku otrzymania przesyłek niewiadomego pochodzenia
Załącznik nr 11	Wzór umowy powierzenia przetwarzania danych osobowych
Załącznik nr 12	Wzór powołania na stanowisko ABI
Załącznik nr 13	Wzór wniosku o udostępnienie danych osobowych
Załącznik nr 14	Wzór decyzji odmownej udostępnienia danych osobowych
Załącznik nr 15	Wzór rejestru umów powierzenia

WPROWADZENIE

Niniejszy dokument opisuje reguły dotyczące bezpieczeństwa danych osobowych zawartych w Urzędzie Gminy w Radzyniu Podlaskim. Opisane reguły określają granice dopuszczalnego zachowania wszystkich pracowników Urzędu Gminy. Dokument zwraca uwagę na konsekwencje, jakie mogą ponosić osoby przekraczające określone granice oraz procedury postępowania dla zapobiegania i minimalizowania skutków zagrożeń.
Odpowiednie zabezpieczenia, ochrona przetwarzanych danych oraz niezawodność funkcjonowania są podstawowymi wymogami.
Dokument „Polityka bezpieczeństwa informacji" wskazuje na sposób przetwarzania danych osobowych osób zatrudnionych w Urzędzie Gminy i postępowanie w sytuacji naruszenia bezpieczeństwa tychże danych.

Potrzeba jego opracowania wynika z § 3 i 4 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024).

1. „Polityka bezpieczeństwa informacji" określa tryb postępowania w przypadku, gdy:
   - stwierdzono naruszenie zabezpieczenia systemu informatycznego,
   - stwierdzono incydent naruszenia bezpieczeństwa danych osobowych,
   - stan urządzeń, zawartość zbiorów danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci informatycznej mogą wskazywać na naruszenie zabezpieczeń danych.
2. „Polityka bezpieczeństwa informacji" obowiązuje wszystkich pracowników Urzędu Gminy w Radzyniu Podlaskim.
3. Wykonywanie postanowień tego dokumentu ma zapewnić właściwą reakcję, ocenę i udokumentowanie przypadków naruszenia bezpieczeństwa systemów oraz zapewnić właściwy tryb działania w celu przywrócenia bezpieczeństwa danych.

Polityka bezpieczeństwa została oparta również na zapisach Polskiej Normy PN-ISO/IEC 17799, PN-I-02000, PN-I-13335-1 oraz PN-ISO/IEC 27001 określających praktyczne zasady zarządzania bezpieczeństwem informacji w obszarze technik informatycznych, która jako cel polityki bezpieczeństwa wskazuje „zapewnienie kierunków działania i wsparcie kierownictwa dla bezpieczeństwa informacji".

TERMINOLOGIA

a) **Dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden z kilku specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne;

b) **Zbiór danych osobowych** - każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony (jego części znajdują się w różnych miejscach) lub podzielony funkcjonalnie (przetwarzany za pomocą programów realizujących różne funkcje);

c) **Przetwarzanie danych osobowych** – jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, udostępnianie, opracowywanie i usuwanie;

d) **System informatyczny** – system przetwarzania informacji wraz ze związanymi z nimi ludźmi oraz zasobami technicznymi i finansowymi, które dostarcza i rozprowadza informacje. Ochronie podlegają nie tylko informacje osobowe, ale także ludzie, zasoby techniczne i finansowe;

e) **Bezpieczeństwo systemu informatycznego** – wdrożenie stosowanych środków administracyjnych, technicznych i fizycznych w celu zabezpieczenia zasobów technicznych oraz ochrony przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych, a także ich utratą;

f) **Administrator Danych Osobowych (ADO)** – organ, jednostka organizacyjna, podmiot lub osoba decydująca o celach i środkach przetwarzania danych osobowych. Administratorem danych jest Wójt Urzędu Gminy, który ponosi pełnię odpowiedzialności wynikającej z przepisów ustawy o ochronie danych osobowych w odniesieniu do zbiorów danych osobowych znajdujących się w jego ustawowej dyspozycji;

g) **Administrator Bezpieczeństwa Informacji (ABI)** – należy przez to rozumieć osobę wyznaczoną przez Administratora Danych Osobowych do nadzorowania przestrzegania zasad ochrony oraz wymagań w zakresie ochrony, wynikających z powszechnie obowiązujących przepisów o ochronie danych osobowych;

h) **Administrator Systemów Informatycznych (ASI)** – należy przez to rozumieć pracownika lub pracowników Informatyki odpowiedzialnych za stosowanie technicznych i organizacyjnych środków ochrony danych osobowych;

i) **Osoba upoważniona lub użytkownik systemu** – osoba posiadająca upoważnienie wydane przez ADO lub osoba uprawniona przez niego i dopuszczona jako użytkownik do przetwarzania danych osobowych w systemie informatycznym danej komórki organizacyjnej, w zakresie wskazanym w upoważnieniu, zwana dalej użytkownikiem;

j) **Osoba uprawniona** – osoba posiadająca uprawnienie wydane przez ADO na mocy którego wykonuje w jego imieniu określone czynności;

k) **Identyfikator użytkownika (LOGIN)** – ciąg znaków literowych i cyfrowych, lub innych, jednoznacznie identyfikujących osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;

l) **Hasło** – ciąg znaków literowych cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;

m) **Zalogowanie** – uwierzytelnienie czyli działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;

n) **Odbiorca danych** – rozumie się przez to każdego, komu udostępnia się dane osobowe, z wyłączeniem:
- osoby, której dane dotyczą,
- osoby, upoważnionej do przetwarzania danych,
- przedstawiciela, o którym mowa w art. 31a ustawy o ochronie danych osobowych,
- podmiotu, o którym mowa w art. 31 ustawy o ochronie danych osobowych,
- organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem.

o) **Aktywa** – wszystko, co ma wartość dla organizacji (zasoby ludzkie, finansowe);

p) **GIODO** – Generalny Inspektor Ochrony Danych Osobowych.

PRZEPISY

Przetwarzanie Danych Osobowych następuje przy poszanowaniu norm i zasad wypływających w szczególności z następujących źródeł:

1. Konwencja Rady Europy Nr 108 z dnia 28 stycznia 1981 r.
2. Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady WE z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych.
3. art. 47 oraz art. 51 Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz. U. z 1997 r. Nr 78, poz. 483 z późn. zm.).
4. Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. (t.j. Dz. U. z 2016 r. poz. 922) - zwana dalej "Ustawą".

Akty wykonawcze:

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).
6. Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbiorów danych (Dz. U. z 2015 poz. 719).
7. Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewniania przestrzegania przepisów

o ochronie danych osobowych przez administratora bezpieczeństwa informacji (Dz. U. z 2015 poz. 745).

8. Rozporządzenie Ministra Spraw Wewnętrznych I Administracji z dnia 11 grudnia 2008 r. w sprawie wzoru zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (Dz. U. z 2008 Nr 229 poz. 1536).
9. Wytyczne Ministra Infrastruktury i Rozwoju w zakresie warunków gromadzenia i przekazywania danych w postaci elektronicznej na lata 2014-2020.

Rozdział 1

Opis zdarzeń naruszających ochronę danych osobowych

1. Podział zagrożeń:
   - zagrożenia losowe zewnętrzne (np. klęski żywiołowe, przerwy w zasilaniu), ich występowanie może prowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej systemu, ciągłość systemu zostaje zakłócona, nie dochodzi do naruszenia poufności danych,
   - zagrożenia losowe wewnętrzne (np. niezamierzone pomyłki operatorów, administratora, awarie sprzętowe, błędy oprogramowania), może dojść do zniszczenia danych, może zostać zakłócona ciągłość pracy systemu, może nastąpić naruszenie poufności danych,
   - zagrożenia zamierzone, świadome i celowe - najpoważniejsze zagrożenia, naruszenia poufności danych, (zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy), zagrożenia te możemy podzielić na: nieuprawniony dostęp do systemu z zewnątrz (włamanie do systemu), nieuprawniony dostęp do systemu z jego wnętrza, nieuprawniony przekaz danych, pogorszenie jakości sprzętu i oprogramowania, bezpośrednie zagrożenie materialnych składników systemu.
2. Przypadki zakwalifikowane jako naruszenie lub uzasadnione podejrzenie naruszenia zabezpieczenia systemu informatycznego, w którym przetwarzane są dane osobowe:
   - sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu jak np.: wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej itp.,
   - niewłaściwe parametry środowiska, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy lub wibracje pochodzące od urządzeń przemysłowych,
   - awaria sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych lub wręcz sabotaż, a także niewłaściwe działanie serwisu, a w tym sam fakt pozostawienia serwisantów bez nadzoru,
   - pojawienie się odpowiedniego komunikatu alarmowego od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu,
   - jakość danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie,
   - nastąpiło naruszenie lub próba naruszenia integralności systemu lub bazy danych w tym systemie,
   - stwierdzono próbę lub modyfikację danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji),
   - nastąpiła niedopuszczalna manipulacja danymi osobowymi w systemie,
   - ujawniono osobom nieupoważnionym dane osobowe lub objęte tajemnicą procedury ochrony przetwarzania albo inne strzeżone elementy systemu zabezpieczeń,
   - praca w systemie lub jego sieci komputerowej wykazuje nieprzypadkowe odstępstwa od założonego rytmu pracy wskazujące na przełamanie lub zaniechanie ochrony danych osobowych - np. praca przy komputerze lub

w sieci osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu, itp.,
- ujawniono istnienie nieautoryzowanych kont dostępu do danych lub tzw. "bocznej furtki", itp.,
- podmieniono lub zniszczono nośniki z danymi osobowymi bez odpowiedniego upoważnienia lub w sposób niedozwolony skasowano lub skopiowano dane osobowe,
- rażąco naruszono dyscyplinę pracy w zakresie przestrzegania procedur bezpieczeństwa informacji (nie wylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych osobowych w drukarce, na ksero, nie zamknięcie pomieszczenia z komputerem, nie wykonanie w określonym terminie kopii bezpieczeństwa, prace na danych osobowych w celach prywatnych, itp.).

3. Za naruszenie ochrony danych uważa się również stwierdzone nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania danych osobowych (otwarte szafy, biurka, regały, urządzenia archiwalne i inne) na nośnikach tradycyjnych tj. na papierze (wydrukach), kliszy, folii, zdjęciach, dyskietkach, płytach CD, DVD w formie niezabezpieczonej, itp.

Rozdział 2

Organizacja przetwarzania danych osobowych

1. Administrator Danych Osobowych reprezentowany przez Wójta Gminy Radzyń Podlaski realizuje zadania w zakresie ochrony danych osobowych:
   a) Powołuje Administratora Bezpieczeństwa Informacji, wzór stanowi ***załącznik nr 12*** do niniejszej Polityki.
   b) podejmuje decyzje o odpowiednich działaniach w przypadku naruszenia lub podejrzenia naruszenia procedur bezpiecznego przetwarzania danych osobowych,
   c) podejmuje decyzje o celach i środkach przetwarzania danych osobowych zwłaszcza z uwzględnieniem zmian w obowiązującym prawie, organizacji administratora danych oraz technik zabezpieczenia danych osobowych,
   d) sprawuje nadzór nad wdrożeniem stosowanych środków organizacyjnych, technicznych i fizycznych w celu zapewnienia bezpieczeństwa,
   e) sprawuje nadzór nad funkcjonowaniem systemu zabezpieczeń, a także nad prowadzeniem ewidencji z zakresu ochrony danych osobowych,
   f) decyduje o udostępnianiu danych osobowych odbiorcom danych i innym podmiotom,
   g) spełnia obowiązek informacyjny względem osób których dane dotyczą.

2. Administrator Bezpieczeństwa Informacji odpowiada za realizację zadań ADO, a w szczególności:
   a) określa potrzeby w zakresie zabezpieczenia Zbiorów Danych Osobowych,
   b) określa cele, strategię i politykę bezpieczeństwa Danych Osobowych,
   c) kontroluje zgodność przetwarzania Danych Osobowych z Ustawą i zasadami Polityki Bezpieczeństwa Informacji,
   d) składa ADO roczne sprawozdania o stanie bezpieczeństwa Danych Osobowych.

Sprawozdanie, o którym mowa powyżej powinno zawierać informację co najmniej o:
- zmianach w ewidencjach Zbiorów Danych Osobowych,

- stanie zabezpieczenia Zbiorów Danych Osobowych wraz z informacją o ewentualnych naruszeniach ochrony danych osobowych,
- fakcie powierzenia do przetwarzania innym podmiotom Zbiorów Danych Osobowych,
- udostępnieniu danych osobowych na zewnątrz,
- przeprowadzonych szkoleniach,
- liczbie osób, którym udzielono informacji o przetwarzaniu ich Danych Osobowych.

e) podejmuje działania zmierzające do wyjaśnienia okoliczności naruszenia przepisów prawa w zakresie ochrony Danych Osobowych oraz usunięcia stwierdzonych uchybień,
f) ocenia skuteczność i poprawność wymagań i wytycznych w zakresie ochrony Danych Osobowych oraz podejmuje działania w celu ich usprawnienia,
g) współdziała z Biurem GIODO w wypełnianiu przez Urząd Gminy obowiązków wynikających z Ustawy,
h) koordynuje przygotowania wniosku zgłoszenia Zbiorów Danych Osobowych (w przypadku konieczności rejestracji wynikającej z Ustawy),
i) wykonuje zgłoszenia lub aktualizację Zbiorów Danych Osobowych do rejestracji (w przypadku konieczności rejestracji wynikającej z Ustawy) z wykorzystaniem procedury dostępnej na http://www.giodo.gov.pl,
j) prowadzi Jawny Rejestr Zbiorów Danych Osobowych podlegających jak i nie podlegających rejestracji w GIODO. Rejestr powinien być aktualizowany na bieżąco i zawierać co najmniej następujące informacje:
   - nazwa Zbioru Danych Osobowych, data utworzenia Zbioru Danych Osobowych,
   - cel i forma przetwarzania Danych Osobowych w Zbiorze Danych,
   - miejsca (obszar) przetwarzania danych osobowych w Zbiorze Danych Osobowych,
   - sposób zbierania oraz udostępniania Danych Osobowych,
   - informacje o odbiorcach Danych Osobowych wraz z datą udostępnienia lub powierzenia przetwarzania Danych Osobowych ze Zbioru Danych,
   - data zgłoszenia Zbioru Danych Osobowych do rejestracji w GIODO,
   - daty aktualizacji zgłoszenia Zbioru Danych Osobowych do rejestracji w GIODO,
   - data zaprzestania przetwarzania Danych Osobowych i sposób ich usunięcia ze Zbioru Danych Osobowych;
   - prowadzenie i aktualizację: wykazu zarejestrowanych Zbiorów Danych Osobowych, ewidencji osób upoważnionych do przetwarzania Danych Osobowych, wykazu miejsc przetwarzania Danych Osobowych;

k) koordynację działań zapewniających właściwy poziom ochrony danych osobowych,
l) nadzór i analizę stanu bezpieczeństwa przetwarzanych danych osobowych,
m) opracowanie projektów instrukcji i wewnętrznych aktów prawnych dotyczących ochrony Danych Osobowych,
n) opiniowanie umów, których przedmiotem jest powierzenie przetwarzania danych osobowych,
o) realizację programów szkoleniowych dla osób przetwarzających dane,
p) określanie zabezpieczeń adekwatnych do zidentyfikowanych zagrożeń i ryzyka,
q) monitorowanie wdrożonych zabezpieczeń,
r) podejmowanie interwencji w przypadku naruszeń zabezpieczeń,

s) kontrolowanie przestrzegania przez pracowników zasad ochrony Danych Osobowych,
t) usuwanie zbiorów Danych Osobowych zgodnie z wymaganiami Ustawy o ochronie danych osobowych, Rozporządzenia Ministra Spraw Wewnętrznych i Administracji oraz niniejszej Polityki Bezpieczeństwa Informacji.

3. Administrator Systemów Informatycznych w szczególności:
   a) zarządza systemem informatycznym, w którym przetwarzane są dane osobowe, posługując się hasłem dostępu do wszystkich stacji roboczych z pozycji administratora,
   b) przeciwdziała dostępowi osób niepowołanych do systemu informatycznego, w którym przetwarzane są dane osobowe,
   c) przydziela użytkownikom identyfikator i hasło do systemu informatycznego oraz na polecenie administratora danych dokonuje ewentualnych modyfikacji uprawnień,
   d) nadzoruje działanie mechanizmów uwierzytelniania użytkowników oraz kontroli dostępu do danych osobowych,
   e) podejmuje działania w zakresie ustalania i kontroli identyfikatorów dostępu do systemu informatycznego,
   f) wyrejestrowuje użytkowników na polecenie administratora danych lub danego kierownika Referatu Urzędu Gminy i zmienia w poszczególnych stacjach roboczych hasła dostępu, ujawniając je wyłącznie danemu użytkownikowi, a w razie potrzeby administratorowi danych,
   g) w sytuacji stwierdzenia naruszenia zabezpieczeń systemu informatycznego informuje administratora danych o naruszeniu i współdziała z nim przy usuwaniu skutków naruszenia,
   h) prowadzi szczegółową dokumentację naruszeń bezpieczeństwa danych osobowych przetwarzanych w systemie informatycznym,
   i) nadzoruje wykonywanie napraw, konserwację oraz likwidację urządzeń komputerowych, na których zapisane są dane osobowe, sprawuje nadzór nad wykonywaniem kopii zapasowych, ich przechowywaniem oraz okresowym sprawdzaniem pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu informatycznego,
   j) podejmuje działania służące zapewnieniu niezawodności zasilania komputerów, innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych oraz zapewnieniu bezpiecznej wymiany danych w sieci wewnętrznej i bezpiecznej teletransmisji.

4. Kierownik Referatu Urzędu Gminy w szczególności:
   a) występuje z wnioskiem do administratora danych o nadanie upoważnienia do przetwarzania danych osobowych,
   b) występuje z wnioskiem do administratora systemu o nadanie identyfikatora i przyznanie hasła osobie upoważnionej do przetwarzania danych osobowych,
   c) występuje z wnioskiem o odwołanie upoważnienia do przetwarzania danych osobowych i/lub wyrejestrowania użytkownika z systemu informatycznego.

5. Osoba upoważniona do przetwarzania danych osobowych

Użytkownik może przetwarzać dane osobowe wyłącznie w ustalonym indywidualnie przez administratora danych i tylko w wykonywaniu nałożonych na niego obowiązków. Zakres dostępu do danych przypisany jest do niepowtarzalnego identyfikatora użytkownika niezbędnego do rozpoczęcia pracy w systemie. Rozwiązanie pracy, odwołanie z pełnionej funkcji powoduje wygaśnięcie upoważnienia do przetwarzania danych osobowych.

Użytkownicy danych pisemnie oświadczają, że zobowiązują się do zachowania tajemnicy danych osobowych oraz przestrzegania ich bezpiecznego przetwarzania – wzór oświadczenia stanowi ***załącznik nr 4*** do niniejszej Polityki. Przestrzeganie tajemnicy danych osobowych obowiązuje przez cały czas zatrudnienia u administratora danych, a także po ustaniu stosunku lub odwołaniu z pełnionej funkcji.
Naruszenie przez użytkowników danych osobowych procedur bezpiecznego przetwarzania tych danych, w szczególności świadome udostępnienie danych osobie niepowołanej, jest ciężkim naruszeniem obowiązków pracowniczych i uzasadnia rozwiązanie umowy o pracę.

Wszyscy użytkownicy danych zobowiązani są do:

- zapoznania się z przepisami prawa w zakresie ochrony danych osobowych, w tym przepisami niniejszej polityki i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych,
- stosowania określonych przez administratora danych procedur oraz wytycznych mające na celu zgodne z prawem, w tym zwłaszcza adekwatne przetwarzanie danych,
- odpowiedniego zabezpieczenia danych przed ich udostępnianiem osobom nieupoważnionym.

Rozdział 3

Infrastruktura przetwarzania danych osobowych

1. Obszar przetwarzania danych osobowych ***zawiera załącznik nr 1.***
2. Zbiory danych:
   Dokładny ***opis zbiorów danych osobowych*** wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych zawiera ***załącznik nr 2.***
3. Ewidencje.
   ABI prowadzi ewidencje osób upoważnionych do przetwarzania danych osobowych oraz osób, które zapoznały się z Polityką Bezpieczeństwa, wzór upoważnienia stanowi ***załącznik nr 6,*** a wzór ***ewidencji załącznik nr 5***, wzór oświadczenia ***załącznik nr 4.*** ABI prowadzi ewidencję udostępnień danych odbiorcom danych oraz innym podmiotom.

Rozdział 4

Struktura zbiorów danych

Dokładny opis struktury zbiorów danych przetwarzanych w Urzędzie czyli jawny rejestr zbiorów zawiera ***załącznik nr 3.*** Uwzględniając kategorię przetwarzania danych, zagrożenia oraz fakt, iż system informatyczny połączony jest z siecią publiczną zgodnie z § 6 ust. 4 rozporządzenia, zapewnia się **wysoki poziom bezpieczeństwa** przetwarzania danych osobowych w systemie informatycznym. Wynikające z tego konsekwencje uwzględnia się w instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

Rozdział 5

Powierzenie przetwarzania danych

1. Administrator Danych Osobowych może zlecić innemu podmiotowi przetwarzanie danych osobowych w celu realizacji określonego zadania.
2. W sytuacji powierzenia danych osobowych podmiotowi zewnętrznemu podstawę współpracy stanowi **umowa powierzenia** przetwarzania danych w formie pisemnej.
3. Wzór umowy powierzenia przetwarzania Danych Osobowych stanowi ***załącznik nr 11*** do niniejszej Polityki. Dopuszcza się modyfikację tego wzoru w zależności od uwarunkowań regulowanego stosunku cywilno-prawnego.
4. Wzór rejestru umów powierzenia stanowi ***załącznik nr 15*** do niniejszej Polityki.
5. Umowa, o której mowa w pkt 2, powinna wyraźnie określać:
   a) zakres i cel przetwarzania danych,
   b) przypadku powierzenia Danych Osobowych nie jest wymagana zgoda osoby, której dane dotyczą,
   c) podmiot, któremu powierzono przetwarzanie Danych Osobowych jest zobowiązany do podjęcia środków zabezpieczających przed przystąpieniem do przetwarzania danych,
   d) w zakresie przestrzegania obowiązujących przepisów prawa podmiot ponosi odpowiedzialność jak administrator danych,
   e) przekazywanie Danych Osobowych do państwa trzeciego w rozumieniu Ustawy następuje na zasadach określonych w Ustawie o ochronie danych osobowych i Polityce Bezpieczeństwa Informacji. Decyzję w tej sprawie podejmuje Administrator Danych Osobowych.

Rozdział 6

Udostępnienie danych osobowych

1. Dane Osobowe udostępnia się na pisemny, umotywowany wniosek osób trzecich - na podstawie przepisów prawa.
2. Wniosek o udostępnienie Danych Osobowych powinien wskazywać zakres, przeznaczenie Danych oraz podstawy prawne, wzór stanowi ***załącznik nr 13.***
3. Jednostka wnioskująca o udostępnienie danych osobowych powinna posiadać zabezpieczenia spełniające wymagania przepisów prawa.
4. Dane Osobowe mogą być także udostępnione w celach innych niż włączenie do Zbioru Danych Osobowych, a ich udostępnienie nie naruszy praw i wolności osób, których Dane dotyczą.
5. Na udostępnienie Danych Osobowych na wniosek upoważnionych organów państwa wykonujących zadania na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego zgodę wyraża ADO.
6. Wzór decyzji w sprawie rozpatrywania wniosku o udostępnienie danych osobowych ze zbioru zawiera ***załącznik nr 14.***
7. Odmawia się udostępnienia Danych Osobowych ze Zbioru Danych, jeżeli spowodowałoby:
   - ujawnienie wiadomości stanowiących tajemnicę państwową,
   - zagrożenie dla obronności lub bezpieczeństwa państwa, życia i zdrowia ludzi lub bezpieczeństwa i porządku publicznego,
   - zagrożenie dla podstawowego interesu gospodarczego lub finansowego państwa,
   - istotne naruszenie dóbr osobistych osób, których dane dotyczą lub innych.

Rozdział 7

Strategia zabezpieczenia danych osobowych

1. Administrator danych osobowych jest zobowiązany do zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych informatycznych w systemach informatycznych Urzędu w Radzyniu Podlaskim, a w szczególności:
   a) zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym,
   b) zapobiegać przed zabraniem danych przez osobę nieuprawnioną,
   c) zapobiegać przetwarzaniu danych z naruszeniem ustawy oraz zmianie, utracie, uszkodzeniu lub zniszczeniu tych danych.
2. Do zastosowanych środków technicznych należy:
   a) przetwarzanie danych osobowych w wydzielonych pomieszczeniach położonych w strefie administracyjnej,
   b) zabezpieczenie wejścia do pomieszczeń, w których przetwarzane są dane,
   c) szczególne zabezpieczenie centrum przetwarzania danych (komputery serwerownia),
   d) wyposażenie pomieszczeń w szafy dające gwarancję bezpieczeństwa dokumentacji.
3. Do zastosowanych środków organizacyjnych należą przede wszystkim następujące zasady:
   a) zapoznanie każdej osoby z przepisami dotyczącymi ochrony danych osobowych, przed dopuszczeniem jej do pracy przy przetwarzaniu danych osobowych,
   b) przeszkolenie pracowników w zakresie bezpiecznej obsługi urządzeń i programów związanych z przetwarzaniem i ochroną danych osobowych,
   c) kontrolowanie otwierania i zamykania pomieszczeń, w których są przetwarzane dane osobowe.
   d) politykę kluczy określa Instrukcja postępowania z kluczami oraz zabezpieczenia pomieszczeń i obiektu Urzędu Gminy Radzyń Podlaski stanowiąca załącznik do Zarządzenia nr 62/2016 Wójta Gminy Radzyń Podlaski z dnia 3 listopada 2016 r.
   e) Wykaz pomieszczeń, w których przetwarzane są dane i ich zabezpieczeń zawiera ***załącznik nr 1***.
4. Zabezpieczenie przed nieautoryzowanym dostępem do baz danych Urzędu
   a) wszystkie gniazda lokalnej sieci komputerowej są galwanicznie oddzielone od szkieletu sieci elektrycznej. Podłączenie danego użytkownika do sieci komputerowej dokonuje Administrator Systemu Informatycznego.
   b) aby uzyskać dostęp do zasobów sieci, należy zwrócić się do Administratora Systemu Informatycznego z odpowiednim wnioskiem, w którym podane będą dane nowego użytkownika oraz zasoby jakie ma on mieć udostępnione.
   c) w systemie informatycznym Urzędu zastosowano podwójną autoryzację użytkownika. Pierwszej autoryzacji należy dokonać w momencie uzyskania dostępu do komputerów Urzędu, podając login użytkownika i hasło. Drugiej autoryzacji należy dokonać uruchamiając program użytkowy, podając login użytkownika i hasło. Dostęp do wybranej bazy danych Urzędu uzyskuje się dopiero po poprawnym podwójnym zalogowaniu się do systemu informatycznego Urzędu.

W efekcie zapewnione jest:

a) zabezpieczenie sieci przed atakiem z zewnątrz poprzez blokowanie wybranych portów,
b) filtrowanie pakietów i blokowanie niektórych usług,
c) objęcie ochroną antywirusową wszystkich danych ściąganych z internetu na stacjach lokalnych,
d) zapisywanie logów połączeń użytkowników z siecią Internet.

5. Do pomieszczeń w których następuje przetwarzanie danych osobowych mają dostęp tylko uprawnione osoby bezpośrednio związane z nadzorem nad serwerami lub aplikacjami.
6. Zabezpieczenie przed nieuprawnionym dostępem do danych, prowadzone jest przez Administratora Systemu Informatycznego zgodnie z przyjętymi procedurami nadawania uprawnień do systemu informatycznego.
7. W pomieszczeniach w których znajdują się serwery zamontowane są czujniki dymu.
8. W pomieszczeniach w których znajdują się serwery zamontowana jest klimatyzacja.
9. W pobliżu serwerowni znajduje się gaśnica, która okresowo jest napełniana i sprawdzana przez specjalistę.
10. Zakres działania archiwum zakładowego:
Archiwum zakładowe gromadzi materiały archiwalne (kat. „A") i dokumentację niearchiwalną (kat. „B").

Do zakresu działania archiwum zakładowego należy:

1) przyjmowanie w stanie uporządkowanym materiałów archiwalnych i dokumentacji niearchiwalnej z poszczególnych referatów Urzędu Gminy;
2) przechowywanie i zabezpieczanie zgromadzonej dokumentacji oraz prowadzenie jej ewidencji;
3) porządkowanie przechowywanej dokumentacji, przejętej w latach wcześniejszych w stanie nieuporządkowanym;
4) udostępnianie przechowywanej dokumentacji;
5) przeprowadzanie kwerend archiwalnych, czyli poszukiwanie w dokumentacji informacji na temat osób, zdarzeń, czy problemów;
6) inicjowanie brakowania dokumentacji niearchiwalnej i przekazywanie jej do zniszczenia odpowiednim firmom;
7) przygotowanie materiałów archiwalnych do właściwego archiwum państwowego;
8) za realizację zadań archiwum zakładowego odpowiedzialny jest upoważniony pracownik
9) archiwum mieści się w zamykanym pomieszczeniu, po zamknięciu klucze plombowane są w woreczkach do tego przeznaczonych;
10) przejmowanie dokumentacji do archiwum zakładowego:
   a) przekazywanie dokumentacji do archiwum zakładowego następuje w trybie i na warunkach, określonych w instrukcji kancelaryjnej;
   b) przekazywanie dokumentacji odbywa się na podstawie spisu zdawczo-odbiorczego akt;
   c) dokumentację przed przekazaniem przegląda i porządkuje prowadzący sprawę z referatu, który przekazuje dokumentację;
11) przekazywanie materiałów archiwalnych do archiwum państwowego następuje na podstawie przepisów art. 5 ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach oraz przepisów wydanych na ich podstawie;

12) po przekazaniu materiałów archiwalnych pracownik odpowiedzialny za prowadzenie archiwum zakładowego odnotowuje w środkach ewidencyjnych datę przekazania tych materiałów;
13) dokumentacja z przekazywania materiałów archiwalnych do archiwum państwowego przechowywana jest przez archiwum zakładowe.

Rozdział 8

Postępowanie w przypadku naruszenia ochrony danych osobowych

1. W przypadku stwierdzenia naruszenia:
   a) zabezpieczenia systemu informatycznego,
   b) technicznego stanu urządzeń,
   c) zawartości zbioru danych osobowych,
   d) ujawnienia metody pracy lub sposobu działania programu,
   e) jakości transmisji danych w sieci telekomunikacyjnej mogącej wskazywać na naruszenie zabezpieczeń tych danych,
   f) innych zdarzeń mogących mieć wpływ na naruszenie danych osobowych (np. zalanie, pożar, itp.)

Każda osoba zatrudniona przy przetwarzaniu danych osobowych jest obowiązana niezwłocznie powiadomić o tym fakcie Administratora Bezpieczeństwa Informacji.

2. W razie niemożliwości zawiadomienia ABI należy powiadomić bezpośredniego przełożonego.

3. Do czasu przybycia na miejsce naruszenia ochrony danych osobowych ABI, należy:
   a) niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego naruszenia, o ile istnieje taka możliwość, a następnie uwzględnić w działaniu również ustalenie przyczyn lub sprawców,
   b) rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia,
   c) zaniechać - o ile to możliwe - dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić udokumentowanie i analizę,
   d) podjąć inne działania przewidziane i określone w instrukcjach technicznych i technologicznych stosownie do objawów i komunikatów towarzyszących naruszeniu,
   e) podjąć stosowne działania, jeśli zaistniały przypadek jest określony w dokumentacji systemu operacyjnego, dokumentacji bazy danych lub aplikacji użytkowej,
   f) zastosować się do innych instrukcji i regulaminów, jeżeli odnoszą się one do zaistniałego przypadku,
   g) udokumentować wstępnie zaistniałe naruszenie,
   h) nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia ABI.

4. Po przybyciu na miejsce naruszenia lub ujawnienia ochrony danych osobowych, ABI lub osoba go zastępująca:

a) zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metody dalszego postępowania mając na uwadze ewentualne zagrożenia dla prawidłowości pracy Urzędu,
b) może żądać dokładnej relacji z zaistniałego naruszenia od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem,
c) rozważa celowość i potrzebę powiadamia o zaistniałym naruszeniu Administratora Danych Osobowych,
d) nawiązuje bezpośredni kontakt, jeżeli zachodzi taka potrzeba, ze specjalistami spoza Urzędu.

5. Administrator Bezpieczeństwa Informacji dokumentuje zaistniały przypadek naruszenia oraz sporządza raport wg wzoru stanowiącego ***załącznik nr 8,*** który powinien zawierać w szczególności:
   - wskazanie osoby powiadamiającej o naruszeniu oraz innych osób zaangażowanych lub odpytanych w związku z naruszeniem,
   - określenie czasu i miejsca naruszenia i powiadomienia,
   - określenie okoliczności towarzyszących i rodzaju naruszenia,
   - wyszczególnienie wziętych faktycznie pod uwagę przesłanek do wyboru metody postępowania i opis podjętego działania,
   - wstępną ocenę przyczyn wystąpienia naruszenia,
   - ocenę przeprowadzonego postępowania wyjaśniającego i naprawczego.
6. Po wyczerpaniu niezbędnych środków doraźnych po zaistniałym naruszeniu ABI zasięga niezbędnych opinii i proponuje postępowanie naprawcze, w tym ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń oraz terminu wznowienia przetwarzania danych.
7. Zaistniałe naruszenie może stać się przedmiotem szczegółowej, zespołowej analizy prowadzonej przez Kierownictwo Urzędu, Pełnomocnika ds. Ochrony Informacji Niejawnych, Administratora Systemu Informatycznego.
8. Analiza, o której mowa w ust. 7, powinna zawierać wszechstronną ocenę zaistniałego naruszenia, wskazanie odpowiedzialnych, wnioski, co do ewentualnych przedsięwzięć proceduralnych, organizacyjnych, kadrowych i technicznych, które powinny zapobiec podobnym naruszeniom w przyszłości.

Rozdział 9

Przegląd polityki bezpieczeństwa i audyt systemu

1. Administrator Danych Osobowych sprawuje nadzór nad przestrzeganiem zasad ochrony danych wynikających z ustawy o ochronie danych osobowych oraz zasad ustanowionych w niniejszym dokumencie.
2. Administrator Bezpieczeństwa Informacji sporządza plany kontroli oraz dokonuje oceny stanu bezpieczeństwa danych osobowych.
3. Raz w roku dokonywany jest wewnętrzny lub zewnętrzny audyt bezpieczeństwa.

Rozdział 10

Ochrona budynków i pomieszczeń Urzędu Gminy Radzyń Podlaski

Postępowanie w sytuacjach kryzysowych

Zasady i zadania funkcjonowania oraz strukturę organizacyjną Urzędu Gminy w Radzyniu Podlaskim określono w Regulaminie Organizacyjnym z dnia 29 lipca 2016 r. wprowadzonym Zarządzeniem nr 36/2016 Administratora Danych Osobowych, Wójta Gminy w Radzyniu Podlaskim.
Realizacja zadań Urzędu odbywa się w siedzibie urzędu przy ulicy Warszawskiej 32 w Radzyniu Podlaskim od poniedziałku do piątku w godzinach 7:30-15:30, za wyjątkiem dni ustawowo wolnych od pracy.
Budynki i pomieszczenia stanowiące siedzibę Urzędu Gminy w Radzyniu Podlaskim podlegają ochronie. Ochrona fizyczna polega na stałym monitoringu budynku i znajdujących się w nim pomieszczeń poprzez system alarmowy zintegrowany z jednostką Policji. Kody do instalacji alarmowej do budynku Urzędu posiadają wyznaczeni pracownicy urzędu. Zasady, organizację i porządek pracy w Urzędzie, w tym przebywanie pracownika na terenie Urzędu poza godzinami urzędowania, określono w Regulaminie Organizacyjnym z dnia 29 lipca 2016 r. W budynku Urzędu Gminy na parterze i II piętrze poszczególne strefy na poziomach oddzielone są szklanymi, zabezpieczonymi drzwiami. Na korytarzach zamontowane są kamery monitorujące. Rejestrator znajduje się w pomieszczeniu informatyka. Nagrania są nadpisywane po 30 dniach. Pomieszczenia zamykane są i zakodowywane po zakończeniu pracy przez sprzątaczki urzędu. Rano pomieszczenia rozkodowywane są przez osoby upoważnione przez administratora danych.
Wszystkie procedury wejścia i wyjścia do Urzędu Gminy w Radzyniu Podlaskim szczegółowo określone zostały w „Instrukcji postępowania z kluczami oraz zabezpieczenia pomieszczeń i obiektu Urzędu Gminy Radzyń Podlaski" wprowadzonej Zarządzeniem nr 62 Wójta Gminy Radzyń Podlaski z dnia 3 listopada 2016 r. przez Administratora Danych Osobowych – Wójta Gminy w Radzyniu Podlaskim.

1. Możliwe zagrożenia zewnętrzne dla Urzędu stanowią między innymi :
   a) możliwość napadu przez pojedynczych przestępców, możliwość napadu przez przypadkowe osoby wykorzystujące nadarzającą się okazję z powodu nieprawidłowości w ochronie mienia Urzędu.
   b) wzmożone zainteresowanie osób postronnych obiektem, pomieszczeniami Urzędu objawiające się m.in.: podejmowaniem prób pozyskania informacji o danym obiekcie, pomieszczeniu od pracowników podczas luźnych rozmów po „przypadkowym" spotkaniu,
   c) nawiązanie rozmów przez osoby postronne z pracownikami,
   d) podszywanie się pod byłych pracowników Urzędu i przejawianie zainteresowania tym, co się po latach zmieniło,
   e) interesowanie się osobami funkcyjnymi, w tym także ich przywarami oraz sposobem wykonywania obowiązków służbowych,
   f) obserwacja sposobu działania systemu ochronnego, sekretariatu, sprzątaczki,
   g) rozpoznawanie systemu technicznych zabezpieczeń, w tym stosowanych urządzeń alarmowych,
   h) możliwość napadu przez zorganizowane grupy przestępcze i terrorystyczne, działające w sposób profesjonalny, przemyślany i zorganizowany,

i) celowe uszkadzanie urządzeń alarmowych, linii telefonicznych, oświetlenia,
j) próby pozyskania do grup przestępczych pracowników Urzędu (dotyczy głównie osób mających problemy finansowe, towarzyskie, a także służbowe).

2. W celu zminimalizowania wyżej przedstawionych kierunków zagrożeń należy wykonywać czynności uprzedzające ewentualne możliwości zaistnienia zagrożeń poprzez :
   a) systematyczną, skrupulatną i wnikliwą kontrolę systemu ochrony przez osoby odpowiedzialne za pracę danego referatu,
   b) zwracanie szczególnej uwagi przez pracowników Urzędu w czasie dnia pracy na możliwość zaistnienia ewentualnych zagrożeń, w tym sygnalizacja przełożonym o podejrzeniach lub próbach penetracji o których wyżej mowa,
   c) sprawowany w miarę możliwości nadzór nad wykonywanymi pracami porządkowymi i remontowymi przez osoby niezatrudnione w Urzędzie, zwłaszcza w strefach przetwarzania danych osobowych i innych strefach bezpieczeństwa.

3. Możliwe, zidentyfikowane zagrożenia wewnętrzne w Urzędzie mogą stanowić:
   a) próby zaboru dokumentów lub mienia przez pracowników Urzędu,
   b) próby powielania, kserowania dokumentów służbowych dla celów prywatnych,
   c) byli pracownicy Urzędu zwolnieni dyscyplinarnie,
   d) rozpoznawanie organizacji pracy Urzędu przez grupy przestępcze celem uzyskania łatwiejszej działalności przestępczej na terenie Urzędu,
   e) próby wglądu w dokumenty przez osoby nieuprawnione,
   f) spożywanie alkoholu – przesłanka do wykroczeń dyscyplinarnych i przestępstw.

4. W celu wyeliminowania lub zminimalizowania wyżej przedstawionych kierunków zagrożeń i ich skutków, należy wykonywać czynności uprzedzające ewentualne możliwości zaistnienia zagrożeń poprzez :
   a) zwracanie szczególnej uwagi na osoby, które mogą być zainteresowane zaborem dokumentów,
   b) nie pozostawianie pomieszczeń służbowych otwartych i bez nadzoru uprawnionych pracowników Urzędu,
   c) nie pozostawianie w miejscach ogólnie dostępnych dokumentów niejawnych lub innych, ważnych z punktu widzenia interesu Urzędu, w tym decyzji administracyjnych, które po zakończonej pracy należy przechowywać na stanowisku pracy, w meblach biurowych zamykanych na klucz, tzw. „zasada czystego biurka po zakończonej pracy",
   d) prowadzenie szczególnego nadzoru, by nie dokonywano prób kserowania, kopiowania bez zgody przełożonego,
   e) uwrażliwianie pracowników w trakcie prowadzonych szkoleń na możliwość kontaktu grup przestępczych z pracownikami, którzy mają dostęp do dokumentów szczególnie ważnych.

5. Pracowników należy zapoznać także z ***załącznikiem nr 9*** stanowiącym ***„Instrukcję postępowania na wypadek zagrożenia atakiem terrorystycznym" oraz załącznikiem nr 10*** **stanowiącym** ***„Instrukcję postępowania w przypadku otrzymania przesyłki niewiadomego pochodzenia".***

6. Z treścią niniejszego rozdziału należy zapoznać wszystkich pracowników Urzędu Gminy Radzyń Podlaski.

Rozdział 11

Postanowienia końcowe

1. Wobec osoby, która w przypadku naruszenia zabezpieczeń lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także, gdy nie zrealizowała stosownego działania dokumentującego ten przypadek nakłada się karę porządkową.
2. Administrator Bezpieczeństwa Informacji zobowiązany jest prowadzić ewidencję osób, które zostały zapoznane z niniejszym dokumentem i zobowiązują się do stosowania zasad w nim zawartych wg wzoru stanowiącego ***załącznik nr 7*** do niniejszego dokumentu.
3. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu mogą być potraktowane, jako ciężkie naruszenie obowiązków pracowniczych, w szczególności przez osobę, która wobec naruszenia zabezpieczenia systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie powiadomiła o tym Administratora Bezpieczeństwa Informacji i Administratora Danych Osobowych.
4. Orzeczona kara dyscyplinarna, wobec osoby uchylającej się od powiadomienia administratora danych osobowych nie wyklucza odpowiedzialności karnej tej osoby zgodnie z ustawą z dnia 29 sierpnia 1997 roku o ochronie danych osobowych oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.
5. W sprawach nie uregulowanych niniejszym dokumentem mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych, Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r., Nr 100, poz. 1024).
6. Niniejsza Polityka Bezpieczeństwa Informacji wchodzi w życie z dniem jej podpisania przez Wójta Gminy Radzyń Podlaski.

Wójt Gminy
Radzyń Podlaski
Wiesław Mazurek

	Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane **URZĄD GMINY RADZYŃ PODLASKI**	załącznik nr 1/PBI

WYKAZ BUDYNKÓW, POMIESZCZEŃ LUB CZĘŚCI POMIESZCZEŃ, TWORZĄCYCH OBSZAR, W KTÓRYM PRZETWARZANE SĄ DANE OSOBOWE

Lp.	Budynek	Pomieszczenie	Nazwa zbioru
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			
10.			
11.			
12.			
13.			
14.			
15.			
16.			
17.			
18.			

	Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych **URZĄD GMINY RADZYŃ PODLASKI**	załącznik nr 2/PBI

WYKAZ ZBIORÓW DANYCH OSOBOWYCH WRAZ ZE WSKAZANIEM PROGRAMÓW ZASTOSOWANYCH DO PRZETWARZANIA TYCH DANYCH

Lp.	Nazwa zbioru danych osobowych	Nazwa programu
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.		
10.		
11.		
12.		
13.		
14.		
15.		
16.		
17.		

	Rejestr zbiorów danych osobowych z uwzględnieniem pomieszczeń i systemów **URZĄD GMINY RADZYŃ PODLASKI**	**załącznik nr 3/PBI**

(podpis ABI)

Rejestr zbiorów danych osobowych z uwzględnieniem pomieszczeń i systemów (załącznik nr 3/PBI)

L.p.	Nazwa zbioru danych osobowych	Cel i podstawa prawna przetwarzania danych osobowych	Struktura zbiorów	Sposób przetwarzania danych	Systemy informatyczne służące do przetwarzania danych	Obszar przetwarzania danych osobowych	Data rejestracji zbioru	Data aktualizacji / wykreślenia zbioru
1.								
2.								
3.								
4.								
5.								
6.								
7.								
8.								
9.								
10.								

(podpis ABI)

	Oświadczenie **URZĄD GMINY RADZYŃ PODLASKI**	załącznik nr 4/PBI

.....
(miejscowość, data)

.....
(imię i nazwisko pracownika)

OŚWIADCZENIE

(tekst oświadczenia podpisywanego przez pracowników Urzędu Gminy oraz służb pomocniczych – konserwator, sprzątaczka)

1. Stwierdzam własnoręcznym podpisem, że znana mi jest treść przepisów

   1.1. ochronie i postępowaniu z wiadomościami, stanowiącymi tajemnicę służbową,
   1.2. o zasadach ochrony oraz środkach i zabezpieczeniach danych osobowych wynikających z Ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (t.j. Dz. U. z 2016 r. poz. 922) oraz rozporządzenia Ministra Spraw Wewnętrznych z dnia 29 kwietnia 2004 roku (Dz. U. z 2004 Nr 100, poz. 1024) oraz o odpowiedzialności karnej za naruszenie ochrony danych osobowych.

2. Jednocześnie zobowiązuję się nie ujawniać wiadomości, z którymi zapoznałem(am) się z racji wykonywanej pracy w Urzędzie Gminy, a w szczególności:

   2.1. zachowania w tajemnicy informacji prawnie chronionych w tym danych osobowych, przetwarzanych w trakcie wykonywania obowiązków służbowych, zarówno w czasie trwania stosunku pracy, jak i po jego ustaniu lub w trakcie wykonywania zadań zleconych przez Administratora Danych Osobowych,
   2.2. ochrony danych osobowych przed dostępem do nich osób nieupoważnionych,
   2.3. stosowania zabezpieczeń mających na celu ochronę przed zniszczeniem i nielegalnym ujawnieniem przetwarzanych danych osobowych,
   2.4. zachowania w tajemnicy sposobów zabezpieczenia danych osobowych,
   2.5. niewykorzystywania danych osobowych w celach pozasłużbowych bądź niezgodnych ze zleceniem.

3. Pracownik zobowiązany jest dbać o bezpieczeństwo powierzonych mu do przetwarzania, archiwizowania lub przechowywania danych zgodnie z obowiązującą w Urzędzie Polityką Bezpieczeństwa, regulaminami i instrukcjami wewnętrznymi, w tym:

   3.1 chronić dane przed dostępem osób nieupoważnionych,
   3.2 chronić dane przed przypadkowym lub nieumyślnym zniszczeniem, utratą lub modyfikacją,
   3.3 chronić nośniki i wydruki komputerowe,
   3.4 utrzymywać w tajemnicy powierzone hasła, częstotliwość ich zmiany oraz szczegóły techniczne systemów, także po ustaniu zatrudnienia w Urzędzie,
   3.5 archiwizować dane zgodnie z Polityką Bezpieczeństwa.

.....
(podpis pracownika)

.....
(podpis przełożonego potwierdzający złożenie oświadczenia przez pracownika)

	Wykaz osób upoważnionych do przetwarzania danych osobowych URZĄD GMINY RADZYŃ PODLASKI	załącznik nr 5/PBI

WYKAZ OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH W URZĘDZIE GMINY RADZYŃ PODLASKI

Lp.	Stanowisko	Imię i nazwisko	Zakres upoważnienia do przetwarzania danych osobowych (podać kolejne numery pozycji przypisane zbiorom zgodnie z zał. nr 3/PBI)	Data nadania	Data wygaśnięcia
1.					
2.					
3.					
4.					
5.					
6.					
7.					
8.					
9.					
10.					
11.					
12.					
13.					
14.					
15.					
16.					
17.					
18.					
19.					

	Upoważnienie **URZĄD GMINY RADZYŃ PODLASKI**	załącznik nr 6/PBI

.....
(miejscowość, data)

U P O W A Ż N I E N I E Nr.....

Z dniem .....na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2016 r. poz. 922)

Upoważniam Pana/Panią .....

zatrudnioną(ego) na stanowisku: .....

do przebywania w pomieszczeniach, w których przetwarzane są dane osobowe oraz do przetwarzania danych osobowych zgodnie z zakresem czynności na zajmowanym stanowisku oraz do obsługi systemu informatycznego i urządzeń wchodzących w jego skład, służących do przetwarzania danych osobowych w Urzędzie Gminy w Radzyniu Podlaskim.

Lp.	*Zbiór danych*	*Zakres przetwarzania*
1.		
2.		
3.		
4.		
5.		

Niniejsze upoważnienie jest ważne w okresie od dn. ..... do dn. ..... /odwołania w czasie trwania stosunku pracy na danym stanowisku.

Administrator Danych Osobowych

.....
(data, podpis)

Zobowiązuję się do zachowania w tajemnicy przetwarzanych danych osobowych i sposobów ich zabezpieczeń, zgodnie z art. 39 ust. 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2016 r. poz. 922), również po ustaniu stosunku pracy, oraz do przestrzegania instrukcji i procedur związanych z ochroną danych osobowych.

.....
(data, podpis osoby upoważnionej)

	Wykaz osób, które zostały zapoznane z Polityką Bezpieczeństwa Informacji, Instrukcją Zarządzania Systemem Informatycznym URZĄD GMINY RADZYŃ PODLASKI	załącznik nr 7/PBI

WYKAZ OSÓB, KTÓRE ZOSTAŁY ZAPOZNANE Z POLITYKĄ BEZPIECZEŃSTWA INFORMACJI I INSTRUKCJĄ ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM URZĘDU GMINY RADZYŃ PODLASKI

Przyjąłem(am) do wiadomości i stosowania zapisy Polityki Bezpieczeństwa Informacji i Instrukcji Zarządzania Systemem Informatycznym

Imię i nazwisko	Komórka organizacyjna	Data, podpis

	Raport z naruszenia bezpieczeństwa informacji URZĄD GMINY RADZYŃ PODLASKI	załącznik nr 8/PBI

RAPORT
Z NARUSZENIA BEZPIECZEŃSTWA INFORMACJI
W URZĘDZIE GMINY W RADZYNIU PODLASKIM

1. *Data:*..... *Godzina:*.....
(dd.mm.rr) *(00:00)*

2. *Osoba powiadamiająca o zaistniałym zdarzeniu:*

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

3. Lokalizacja zdarzenia:

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

4. *Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące:*

.....

5. *Podjęte działania:*

.....

6. *Przyczyny wystąpienia zdarzenia:*

.....

.....

7. *Postępowanie wyjaśniające:*

.....
(data, podpis Administratora Bezpieczeństwa Informacji)

INSTRUKCJA POSTĘPOWANIA NA WYPADEK ZAGROŻENIA ATAKIEM TERRORYSTYCZNYM

Podstawową cechą terroryzmu jest to, że nie ma wyraźnych znaków ostrzegawczych o możliwości wystąpienia ataku terrorystycznego lub są one trudno dostrzegalne, terrorysta nie zawsze musi wyróżniać się z tłumu szczególnym wyglądem.

W celu zminimalizowania skutków ewentualnego zagrożenia zaleca się na zwracanie uwagi na rzeczy dziejące się w najbliższym otoczeniu ze szczególnym uwzględnieniem :

1. Nie pozostawiania pomieszczeń służbowych otwartych i bez nadzoru.
2. Nie pozostawiania w tych pomieszczeniach bez nadzoru osób nie będących pracownikami Urzędu Gminy Radzyń Podlaski.
3. Zwracania szczególnej uwagi na niezidentyfikowane paczki, pakunki, torby pozostawione w pomieszczeniach Urzędu bez jakiegokolwiek nadzoru.
4. W przypadkach zauważenia przedmiotów budzących uzasadnione obawy co do ich niewiadomego pochodzenia powiadomić natychmiast bezpośredniego przełożonego i w porozumieniu z nim odpowiednio: Wójta lub Zastępcę Wójta, Administratora Bezpieczeństwa Informacji, a w przypadku ich nieobecności Sekretarza Urzędu. O powiadomieniu właściwych służb ratowniczych: Straży Miejskiej, Policji, Straży Pożarnej decydują wyżej wymienione osoby stanowiące Kierownictwo Urzędu.
5. Zwracania szczególnej uwagi na osoby zachowujące się nerwowo, chaotycznie lub osoby o których wiadomo, że weszły do Urzędu z pakunkiem, a opuściły go bez niego.
6. Każdorazowo o zauważonych nieprawidłowościach powiadamiać bezpośredniego przełożonego lub w/w Kierownictwo Urzędu.
7. W każdym przypadku zachować spokój w celu uniknięcia ewentualnej paniki, która może spotęgować skutki zagrożenia i doprowadzić do utraty życia, uszczerbku na zdrowiu osób lub uszczerbku mienia.

W przypadku zgłoszenia o podłożeniu lub znalezieniu ładunku wybuchowego w budynku Urzędu należy przyjąć następujący tryb postępowania:

Osoba, która przyjęła zgłoszenie o podłożeniu ładunku wybuchowego albo zauważyła w obiekcie przedmiot niewiadomego pochodzenia mogący być ładunkiem wybuchowym jest zobowiązana o tym powiadomić:

- Wójta, w przypadku jego nieobecności odpowiednio: Zastępcę Wójta, Sekretarza Urzędu, Administratora Bezpieczeństwa Informacji.
- Policję: tel. 997, komórka 112.

Zawiadamiając Policję należy podać treść rozmowy ze zgłaszającym o podłożeniu ładunku wybuchowego, którą należy przeprowadzić wg następujących wskazówek:

1) miejsce i opis zlokalizowanego przedmiotu, który może być ładunkiem wybuchowym,
2) numer telefonu, z którego prowadzona jest rozmowa i swoje stanowisko,
3) uzyskać od policji potwierdzenie przyjętego zawiadomienia,
4) przekazać w miarę możliwości informację o uzyskanej wiedzy w trakcie przeprowadzonej rozmowy o rozmówcy, kierując się następującymi przesłankami :
   - czy to był mężczyzna, czy kobieta,
   - dziecko, młodociany/młodociana, czy osoba dorosła,
   - czy na podstawie rozmowy (o podłożeniu ładunku wybuchowego) można było wysnuć wniosek, że rozmówca znajdował się pod wpływem środków zmieniających tożsamość (alkohol, narkotyki),
   - czy rozmawiał w sposób spokojny, czy był zdenerwowany,
   - inne, ważne zdaniem pracownika informacje o treści przeprowadzonej rozmowy.

Akcja poszukiwawcza ładunku wybuchowego po uzyskaniu informacji o jego podłożeniu :

1. Do czasu przybycia policji akcją kieruje Wójt, a w czasie jego nieobecności Zastępca Wójta, Administrator Bezpieczeństwa Informacji, Sekretarz bądź inna upoważniona osoba.
2. Kierujący akcją zarządza, aby użytkownicy pomieszczeń dokonali sprawdzenia, czy w tych pomieszczeniach znajdują się:
   1) przedmioty, rzeczy lub urządzenia, paczki, itp., których wcześniej nie było i nie wnieśli ich użytkownicy pomieszczeń,
   2) ślady przemieszczania elementów wyposażenia pomieszczeń,
3) zmiany w wyglądzie zewnętrznym przedmiotów, rzeczy, urządzeń, które przedtem w pomieszczeniu były oraz emitowane z nich sygnały (np. dźwięki mechanizmów zegarowych, świecące elementy elektroniczne, itp.).
3. Pomieszczenia ogólnodostępne takie jak: korytarze, klatka schodowa, toalety, piwnice, itp. oraz najbliższe otoczenie zewnętrzne obiektu powinny być sprawdzone przez wyznaczonych do tego pracowników.
4. Zlokalizowanych przedmiotów, rzeczy, urządzeń, których w ocenie użytkowników obiektu przedtem nie było, a zachodzi podejrzenie, że mogą to być ładunki wybuchowe nie wolno dotykać! O ich umiejscowieniu należy natychmiast powiadomić policję.
5. W przypadku, gdy użytkownicy pomieszczeń faktycznie stwierdzą obecność przedmiotów (rzeczy, urządzeń), których wcześniej nie było lub zmiany w wyglądzie i usytuowaniu przedmiotów stale znajdujących się w tych pomieszczeniach, należy domniemywać, że pojawienie się tych przedmiotów lub zmiany w ich wyglądzie i usytuowaniu mogły nastąpić na skutek działania sprawcy podłożenia ładunku wybuchowego. W takiej sytuacji kierujący akcją może wydać decyzję ewakuacji osób z zagrożonego obiektu przed przybyciem policji. Po jej ogłoszeniu należy opuścić miejsce pracy, zabierając rzeczy osobiste np. torebki, siatki, nesesery, itp.
6. Należy zachować spokój i opanowanie, aby nie dopuścić do przejawów paniki.

Współpraca z Policją w czasie akcji.

1. Po przybyciu do obiektu policjanta bądź policyjnej grupy interwencyjnej kierujący akcją powinien przekazać im wszelkie informacje dotyczące zdarzenia oraz wskazać miejsce zlokalizowanych przedmiotów (rzeczy, urządzeń) obcego pochodzenia i punkty newralgiczne w obiekcie.
2. Policjant lub dowódca grupy interwencyjnej przejmuje kierowanie akcją, a kierujący dotychczas akcją winien udzielić mu wszechstronnej pomocy.
3. Na wniosek policjanta kierującego akcją, Wójt lub wyznaczona osoba do kierowania akcją, podejmuje decyzję o ewakuacji użytkowników i innych osób z obiektu, o ile wcześniej to nie nastąpiło.
4. Identyfikacją i rozpoznaniem zlokalizowanych przedmiotów, rzeczy, urządzeń obcych oraz neutralizowaniem ewentualnie podłożonych ładunków wybuchowych zajmują się uprawnione i wyspecjalizowane ogniwa organizacyjne policji, przy wykorzystaniu specjalistycznych środków technicznych.
5. Policjant kierujący akcją po zakończeniu działań przekazuje protokolarnie obiekt Wójtowi.

Postanowienia końcowe dotyczące działań w przypadku zgłoszenia o podłożeniu ładunku wybuchowego.

1. Osobom przyjmującym zgłoszenie o podłożeniu ładunku wybuchowego oraz Wójtowi nie wolno lekceważyć żadnej informacji. Każdorazowo osoby te winny zawiadomić o tym policję, która z urzędu dokona sprawdzenia wiarygodności każdego zgłoszenia.
2. Wójt lub wyznaczony przez niego pracownik Urzędu, powinien na bieżąco organizować szkolenie pracowników w zakresie sposobu zachowania w sytuacjach wymienionych w tej części Planu oraz winien znać rozmieszczenie newralgicznych punktów - węzły energetyczne i wodne, które udostępnia się na żądanie policjanta kierującego akcją.

Telefony alarmowe.

- **999 – Pogotowie Ratunkowe,**
- **998 – Straż Pożarna,**
- **997 – Policja,**
- **987 – Wojewódzkie Centra Zarządzania Kryzysowego,**
- **112 – Centrum Powiadamiania Ratunkowego – telefon alarmowy dla użytkowników sieci telefonów komórkowych,**
- **0 800 120 226 – infolinia Policji (połączenie bezpłatne)**

Wójt Gminy
Radzyń Podlaski
Wiesław Mazurek

	Instrukcja postępowania w przypadku otrzymania przesyłki niewiadomego pochodzenia URZĄD GMINY RADZYŃ PODLASKI	załącznik nr 10/PBI

INSTRUKCJA POSTĘPOWANIA W PRZYPADKU OTRZYMANIA PRZESYŁKI NIEWIADOMEGO POCHODZENIA

W przypadku otrzymania jakiejkolwiek przesyłki niewiadomego pochodzenia lub budzącej podejrzenia z jakiegokolwiek innego powodu :

- brak nadawcy
- brak adresu nadawcy,
- przesyłka pochodzi od nadawcy lub z miejsca, z którego nie spodziewamy się,
- inne podejrzenia

NIE NALEŻY OTWIERAĆ TEJ PRZESYŁKI !

Należy natomiast :

1) umieścić przesyłkę w grubym worku plastikowym, szczelnie zamknąć.
2) Worek należy umieścić w drugim plastikowym worku, szczelnie zamkniętym, zakleić taśmą lub plastrem.
3) Paczki nie należy przemieszczać, należy pozostawić ją na miejscu.
4) Powiadomić:
   - Policję, tel. 997;
   - Państwową Straż Pożarną, tel. 998.
   - Centrum Powiadamiania Ratunkowego - komórka: tel. 112.

Służby te podejmą wszelkie niezbędne kroki w celu bezpiecznego przejęcia przesyłki.

W przypadku, gdy podejrzana przesyłka została otwarta i zawiera jakąkolwiek podejrzaną zawartość w formie stałej (galaretę, pianę, pył lub inną) **należy:**

1) Nie naruszać zawartości – nie rozsypywać, nie przenosić, nie dotykać, nie wąchać, nie powodować ruchu powietrza w pomieszczeniu (wyłączyć systemy wentylacyjne, zamknąć okna).
2) Całą zawartość umieścić w worku plastikowym, zamknąć go i zakleić taśmą lub plastrem.
3) Dokładnie umyć ręce.
4) Zaklejony worek umieścić w drugim worku, zamknąć go i zakleić.
5) Ponownie umyć ręce.
6) Powiadomić:
   - Policję, tel. 997.
   - Państwową Straż Pożarną, tel. 998.
   - Powiatową Stację Sanitarno- Epidemiologiczną - tel. alarmowy (kom.): 668 838 347.
   - Pogotowie Ratunkowe, tel. 999.
   - Centrum Powiadamiania Ratunkowego - komórka: tel. 112.

Po przybyciu właściwej służby należy bezwzględnie stosować się do jej zaleceń.

Wójt Gminy
Radzyń Podlaski
Wiesław Mazurek

	Wzór umowy powierzenia przetwarzania danych osobowych URZĄD GMINY RADZYŃ PODLASKI	załącznik nr 11/PBI

Umowa powierzenia przetwarzania danych osobowych

Niniejsza umowa, o postanowieniach przedstawionych niżej, została zawarta w dniu ..... pomiędzy:

Stronami:

Urząd Gminy RADZYŃ PODLASKI

reprezentowany przez Administratora Danych Osobowych:

.....

(zwanego dalej w umowie "Zleceniodawcą")

a

.....NIP.....

z siedzibą w

.....

reprezentowaną przez:

.....

(zwaną dalej w umowie "Zleceniobiorcą")

§ 1

1. Zleceniodawca oświadcza, że jest właścicielem zbiorów danych osobowych zawierających dane .....(zwanych dalej Zbiorami Danych Osobowych).
2. Zleceniodawca jest Administratorem Danych wymienionych Zbiorów Danych Osobowych w rozumieniu ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. (t.j. Dz. U. z 2016 r. poz. 922).
3. Zleceniobiorca jest zleceniobiorcą w rozumieniu art. 31 ustawy o ochronie danych osobowych i ponosi odpowiedzialność na zasadach określonych w przywołanej ustawie.

§ 2

W ramach niniejszej umowy Zleceniodawca powierza Zleceniobiorcy przetwarzanie danych osobowych, zawartych w Zbiorach Danych Osobowych w celu wykonywania czynności:

.....

.....

§ 3

1. Zakresy powierzonych do przetwarzania Zbiorów Danych Osobowych obejmuje:

.....

2. Jakakolwiek zmiana zakresu powierzonych Zbiorów Danych Osobowych wymaga aneksu do umowy.

§ 4

Zleceniobiorca zobowiązuje się przetwarzać powierzone Zbiory Danych Osobowych wyłącznie w celu wykonania przyjętych na siebie zobowiązań, określonych w niniejszej umowie, tj. wyłącznie w celu określonym w § 2 i nie udostępniać danych innym podmiotom, chyba że przepisy prawa stanowią inaczej.

§ 5

1. Zleceniobiorca zobowiązuje się do zastosowania przy przetwarzaniu Zbiorów Danych Osobowych środków technicznych i organizacyjnych zapewniających ochronę danych, co najmniej w zakresie określonym w art. 36 - 39a Ustawy o ochronie danych osobowych.
2. Zleceniobiorca jest obowiązany zapewnić, aby urządzenia i systemy informatyczne, służące do przetwarzania powierzonych mu danych, były zgodne z wymogami 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. W sytuacjach nadzwyczajnych, nieprzewidzianych w umowie, Zleceniobiorca zobowiązuje się do przetwarzania danych osobowych, mając na uwadze ochronę danych osobowych oraz interes Zleceniodawcy.
4. Wszelkie ustalenia dotyczące przetwarzania danych, odbiegające od ustaleń zawartych w niniejszej umowie, powinny być uzgadniane w formie pisemnej, pod rygorem ich nieważności.

§ 6

1. Strony ustalają, że podczas realizacji niniejszej umowy będą ze sobą ściśle współpracować za pośrednictwem Administratorów Bezpieczeństwa Informacji, informując się wzajemnie o wszystkich okolicznościach mających lub mogących mieć wpływ na wykonanie niniejszej umowy. Osoby te będą wymienione w załączniku do niniejszej umowy.
2. Zleceniodawca upoważnia Zleceniobiorcę w razie potrzeby do powierzania wykonania zadań, wynikających z niniejszej umowy innym podmiotom, w drodze umowy na piśmie.
3. Zleceniodawca nie jest odpowiedzialny za zobowiązania Zleceniobiorcy wobec osób trzecich nie przewidziane niniejszą umową.
4. Zleceniodawca ma prawo do kontroli sposobu wykonywania niniejszej umowy przez Zleceniobiorcę odnośnie zobowiązań, o których mowa w § 5 ust. 1 i 2, w formie inspekcji. Na pisemne wezwanie Zleceniodawcy, wyrażone przez przedstawiciela Urzędu Gminy lub osobę upoważnioną, Zleceniobiorca zobowiązany jest do przedstawienia odpowiednich dokumentów do kontroli w terminie 3 dni od daty otrzymania wezwania.
5. Wezwanie takie musi zawierać określenie:
   a) osoby lub podmiotu upoważnionego do wykonania kontroli w imieniu Zleceniodawcy,
   b) zakresu kontroli z określeniem weryfikowanych danych.
6. Kontrola wykonywana będzie w siedzibie Zleceniobiorcy, w obecności upoważnionego na piśmie przedstawiciela Zleceniobiorcy, w dni robocze od poniedziałku do piątku, w godzinach pracy biura Zleceniobiorcy i zamknięta zostanie podpisanym przez przedstawicieli obu stron Protokołem przedstawiającym wnioski z kontroli.

7. Przedstawicieli Zleceniobiorcy i Zleceniodawcy obowiązuje klauzula poufności, dotycząca przekazanych w trakcie kontroli danych, a dokumenty Zleceniobiorcy przedstawione do kontroli nie powinny być kopiowane ani udostępniane osobom trzecim w żadnej formie.

§ 7

Zleceniobiorca zobowiązuje się do niezwłocznego usunięcia Zbioru Danych Osobowych, jeśli przetwarzanie danych nie jest już uzasadnione wykonywaniem niniejszej umowy oraz do potwierdzenia tego faktu pisemnym oświadczeniem.

§ 8

Strony niniejszej umowy uzgodnią sposób przekazywania informacji, będących elementem Zbioru Danych Osobowych, który zapewni bezpieczeństwo danych.

§ 9

1. W przypadku wykonania umowy w sposób niezgodny z zakresem umowy lub w sposób nieprawidłowy oraz w przypadku złamania przez Zleceniobiorcę obowiązku właściwego zabezpieczenia Zbioru Danych Osobowych, Zleceniobiorca zapłaci karę umowną w wysokości: ....., co nie wyklucza możliwości dochodzenia przez Zleceniodawcę odszkodowania, przewyższającego karę umowną na zasadach ogólnych.
2. Termin płatności kary wynosi 14 dni od dnia doręczenia na piśmie żądania zapłaty.

§ 10

1. W zakresie nieuregulowanym niniejszą umową, mają zastosowanie przepisy Ustawy o ochronie danych osobowych oraz Kodeksu cywilnego.
2. Wszelkie zmiany niniejszej umowy wymagają formy pisemnej pod rygorem nieważności.

§ 11

Niniejszą umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.

....

(Zleceniodawca) *(Zleceniobiorca)*

	Powołanie na stanowisko Administratora Bezpieczeństwa Informacji URZĄD GMINY RADZYŃ PODLASKI	Załącznik nr 12/PBI

Powołanie na stanowisko

ADMINISTRATORA BEZPIECZEŃSTWA INFORMACJI

Na podstawie art. 36 ust. 3 Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2016 r. poz. 922), z dniem 30 stycznia 2017 roku w Urzędzie Gminy Radzyń Podlaski **wyznaczam**:

Panią/Pana .....
/Imię i Nazwisko/

na

ADMINISTRATORA BEZPIECZEŃSTWA INFORMACJI

W zakresie realizacji zadań nałożonych na Administratora Danych Osobowych, Administrator Bezpieczeństwa Informacji podlega bezpośrednio Wójtowi Gminy w Radzyniu Podlaskim.

DO ZAKRESU OBOWIĄZKÓW ABI NALEŻĄ:

1. organizacja bezpieczeństwa i ochrony danych osobowych zgodnie z wymogami ustawy o ochronie danych osobowych oraz rozporządzeń wykonawczych,
2. nadzorowanie opracowania i aktualizowania dokumentacji ochrony danych osobowych oraz przestrzegania zasad w niej określonych,
3. zapewnienie przetwarzania danych zgodnie z uregulowaniami Polityki Bezpieczeństwa, Instrukcji Zarządzania Systemem Informatycznym i procedurami wewnętrznym Urzędu.
4. zapewnienie zapoznania pracowników z przepisami w zakresie ochrony danych osobowych oraz zagrożeń związanych z ich przetwarzaniem,
5. wydawanie i anulowanie upoważnień do przetwarzania danych,
6. prowadzenie „Ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych",
7. prowadzenie postępowania wyjaśniającego w przypadku naruszenia ochrony danych osobowych,
8. nadzór nad fizycznymi i organizacyjnymi zabezpieczeniami danych osobowych,
9. kontrola działań komórek organizacyjnych pod względem zgodności przetwarzania danych z przepisami o ochronie danych osobowych,
10. inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia ochrony danych osobowych.

ADMINISTRATOR BEZPIECZEŃSTWA INFORMACJI MA PRAWO :

1. wyznaczania, rekomendowania i egzekwowania wykonania zadań związanych z ochroną danych osobowych w całym Urzędzie.
2. wstępu do pomieszczeń w których zlokalizowane są zbiory danych i przeprowadzenia niezbędnych badań lub innych czynności kontrolnych w celu oceny zgodności przetwarzania danych z ustawą,
3. żądać złożenia pisemnych lub ustnych wyjaśnień w zakresie niezbędnym do ustalenia stanu faktycznego,
4. żądać okazania dokumentów i wszelkich danych mających bezpośredni związek z problematyką kontroli,
5. żądać udostępnienia do kontroli urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych.

Szczegółowy zakres zadań, upoważnień i odpowiedzialności Administratora Bezpieczeństwa Informacji określa Polityka Bezpieczeństwa Danych Osobowych.

Administrator Danych Osobowych **Administrator Bezpieczeństwa Informacji**

....
/data, pieczęć i podpis ADO/ /data i podpis ABI/

	Wniosek **o udostępnienie danych osobowych** **URZĄD GMINY RADZYŃ PODLASKI**	Załącznik nr 13/PBI

.....
(miejscowość, data)

WNIOSEK O UDOSTĘPNIENIE DANYCH ZE ZBIORU DANYCH OSOBOWYCH

1. Wniosek do .....
(dokładne oznaczenie administratora danych)

2. Wnioskodawca .....
.....
(nazwa firmy i jej siedziba albo nazwisko, imię i adres zamieszkania wnioskodawcy, ew. NIP oraz nr REGON)

3. Podstawa prawna upoważniająca do pozyskania danych albo wskazanie wiarygodnie uzasadnionej potrzeby posiadania danych.....
.....
.....
..... * _ ew. cd. w załączniku nr.....

4. Wskazanie przeznaczenia dla udostępnionych danych .....
.....
.....
..... * _ ew. cd. w załączniku nr.....

5. Oznaczenie lub nazwa zbioru, z którego mają być udostępnione dane: .....
.....
.....

6. Zakres żądanych informacji ze zbioru: .....
.....
..... * _ ew. cd. w załączniku nr.....

7. Informacje umożliwiające wyszukanie w zbiorze żądanych danych: .....
.....
..... * _ ew. cd. w załączniku nr.....

.....
(data, podpis i ew. pieczęć wnioskodawcy)

---

* Jeżeli TAK, to zakreśla kwadrat literą „x”:

	Wzór decyzji w sprawie rozpatrywania wniosku o udostępnienie danych osobowych **URZĄD GMINY RADZYŃ PODLASKI**	załącznik nr 14/PBI

DECYZJA W SPRAWIE ROZPATRYWANIA WNIOSKU O UDOSTĘPNIENIE DANYCH OSOBOWYCH

ze zbioru.....

Postępowanie prowadzi i informacji udziela:
Referat.....

Termin załatwienia sprawy
Wydanie decyzji w sprawie udostępnienie danych następuje w terminie .....

Dane ze zbiorów udostępnia się, o ile są one niezbędne do realizacji ich ustawowych zadań, **następującym podmiotom**:

1. Organom administracji publicznej, sądom i prokuraturze.
2. Policji, Straży Granicznej, Służbie Więziennej, Służbie Kontrwywiadu Wojskowego, Służbie Wywiadu Wojskowego, Żandarmerii Wojskowej, Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, Biuru Ochrony Rządu, Centralnemu Biuru Antykorupcyjnemu i Straży Gminnej.
3. Organom kontroli skarbowej i wywiadu skarbowego.
4. Państwowym i komunalnym jednostkom organizacyjnym oraz podmioty - w zakresie –niezbędnym do realizacji zadań publicznych określonych w przepisach prawa.
5. Polskiemu Czerwonemu Krzyżowi - w zakresie danych osób poszukiwanych.

Dane ze zbiorów mogą być również udostępnione:

1. Osobom i jednostkom organizacyjnym - jeżeli wykażą w tym interes prawny.
2. Jednostkom organizacyjnym - w celach badawczych, statystycznych, badania opinii publicznej lub rynku - pod warunkiem, że udostępnione dane zostaną, po ich wykorzystaniu, poddane takiej modyfikacji, która nie pozwoli na ustalenie tożsamości osób, których dane dotyczą.
3. Innym osobom i podmiotom - jeżeli uwiarygodnią one interes faktyczny w otrzymaniu danych i za zgodą osób, których dane dotyczą.

DECYZJA/UZASADNIENIE

.....

UWAGA:

- **Sposób załatwienia wniosku** *(zaznaczyć właściwe)*
  - ✗ informacja udostępniająca żądane dane osobowe (w przypadku uwzględnienia wniosku),
  - ✗ decyzja odmawiająca udostępnienia danych

Tryb odwoławczy - od decyzji Wójta o odmowie udostępnienia danych służy odwołanie do .....w terminie 14 dni od daty otrzymania decyzji, za pośrednictwem Wójta Gminy Radzyń Podlaski.

.....

(podpis z podaniem imienia, nazwiska i stanowiska służbowego osoby upoważnionej do wydania decyzji)

	Rejestr umów powierzenia **URZĄD GMINY RADZYŃ PODLASKI**	Załącznik nr 15/PBI

Rejestr umów powierzenia

Lp.	Nazwa firmy	Zakres świadczonych usług	Numer umowy	Uwagi
1.				
2.				
3.				
4.				
5.				

Załącznik nr 2
do Zarządzenia nr 2/2017
Wójta Gminy Radzyń Podlaski
z dnia 30 stycznia 2017 r.

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM URZĘDU GMINY RADZYŃ PODLASKI

Załącznik nr 2
do Zarządzenia nr 2/2017
Wójta Gminy Radzyń Podlaski
z dnia 30 stycznia 2017 r.

Spis treści

I. Cel 3
II. Definicje 3
III. Poziom bezpieczeństwa 4
IV. Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych 5
V. Stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzeniem i użytkowaniem. 5
VI. Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu. 6
VII. Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania. 7
VIII. Sposób, miejsce i okres przechowywania: elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych, o których mowa w rozdz. 4..... 7
IX. Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego. ..8
X. Kontrola nad wprowadzaniem, dalszym przetwarzaniem i udostępnianiem danych osobowych. 9
XI. Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych. Naprawa urządzeń komputerowych z chronionymi danymi osobowymi. 9
XII. Postanowienia końcowe. 10
Załączniki: 10

I. Cel

Niniejszy dokument zwany dalej „Instrukcją", reguluje sprawy ochrony danych osobowych zawartych w systemach informatycznych eksploatowanych w sieci LAN oraz na pojedynczych komputerach w Urzędzie Gminy Radzyń Podlaski.

II. Definicje

a) **Dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden z kilku specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne;

b) **Zbiór danych osobowych** - każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony (jego części znajdują się w różnych miejscach) lub podzielony funkcjonalnie (przetwarzany za pomocą programów realizujących różne funkcje):

c) **Przetwarzanie danych osobowych** – jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, udostępnianie, opracowywanie i usuwanie;

d) **System informatyczny** – system przetwarzania informacji wraz ze związanymi z nimi ludźmi oraz zasobami technicznymi i finansowymi, które dostarcza i rozprowadza informacje. Ochronie podlegają nie tylko informacje osobowe, ale także ludzie, zasoby techniczne i finansowe;

e) **Bezpieczeństwo systemu informatycznego** – wdrożenie stosowanych środków administracyjnych, technicznych i fizycznych w celu zabezpieczenia zasobów technicznych oraz ochrony przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych, a także ich utratą;

f) **Administrator Danych Osobowych (ADO)** – organ, jednostka organizacyjna, podmiot lub osoba decydująca o celach i środkach przetwarzania danych osobowych. Administratorem danych jest Wójt Urzędu Gminy w Radzyniu Podlaskim, który ponosi pełnię odpowiedzialności wynikającej z przepisów ustawy o ochronie danych osobowych w odniesieniu do zbiorów danych osobowych znajdujących się w jego ustawowej dyspozycji;

g) **Administrator Bezpieczeństwa Informacji (ABI)** – należy przez to rozumieć pracownika urzędu wyznaczonego przez Administratora Danych Osobowych do nadzorowania przestrzegania zasad ochrony oraz wymagań w zakresie ochrony, wynikających z powszechnie obowiązujących przepisów o ochronie danych osobowych;

h) **Administrator Systemów Informatycznych (ASI)** – należy przez to rozumieć pracownika lub pracowników Informatyki odpowiedzialnych za stosowanie technicznych i organizacyjnych środków ochrony danych osobowych,

i) **Osoba upoważniona lub użytkownik systemu** – osoba posiadająca upoważnienie wydane przez ADO lub osoba uprawniona przez niego i dopuszczona jako użytkownik do przetwarzania danych osobowych w systemie informatycznym danej komórki organizacyjnej, w zakresie wskazanym w upoważnieniu, zwana dalej użytkownikiem;

j) **Osoba uprawniona** – osoba posiadająca uprawnienie wydane przez ADO na mocy którego wykonuje w jego imieniu określone czynności;

k) **Identyfikator użytkownika (LOGIN)** – ciąg znaków literowych i cyfrowych, lub innych, jednoznacznie identyfikujących osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;

l) **Hasło (Password)**– ciąg znaków literowych cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;

m) **Zalogowanie** – uwierzytelnienie czyli działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;

n) **Odbiorca danych** – rozumie się przez to każdego, komu udostępnia się dane osobowe, z wyłączeniem:

   a) osoby, której dane dotyczą,
   b) osoby, upoważnionej do przetwarzania danych,
   c) przedstawiciela, o którym mowa w art. 31a ustawy o ochronie danych osobowych,
   d) podmiotu, o którym mowa w art. 31 ustawy o ochronie danych osobowych,
   e) organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem.

o) **Aktywa** - Wszystko, co ma wartość dla organizacji (zasoby ludzkie, finansowe);

p) **GIODO** - Generalny Inspektor Ochrony Danych Osobowych.

q) **Rozporządzenie** - Rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. (Dz. U. z 2004r. Nr 100 poz. 1024) w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, oraz z rozporządzeniem Ministra Sprawiedliwości z dnia 28 kwietnia 2004r. (Dz. U. z 2004r. Nr 100 poz. 1023) w sprawie sposobu technicznego przygotowania systemów i sieci służących do przekazywania informacji – do gromadzenia wykazów połączeń telefonicznych i innych przekazów informacji oraz sposobów zabezpieczania danych informatycznych.

III. Poziom bezpieczeństwa

Uwzględniając kategorię danych osobowych oraz konieczność zachowania bezpieczeństwa ich przetwarzania w systemie informatycznym połączonym z siecią publiczną, wprowadza się **„poziom wysoki" bezpieczeństwa** w rozumieniu § 6 rozporządzenia.

IV. Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności.

Przetwarzać dane osobowe w systemach informatycznych może wyłącznie osoba posiadająca pisemne upoważnienie do przetwarzania danych osobowych, którego wzór stanowi ***załącznik nr 6*** do Polityki Bezpieczeństwa. Uprawnienia do przetwarzania danych w systemach informatycznych wydaje ASI.
Zasady regulujące nadawanie uprawnień do przetwarzania danych oraz rejestrowania uprawnień w systemie informatycznym określono w procedurze: „Nadawanie uprawnień do przetwarzania danych i rejestrowanie tych uprawnień w systemie informatycznym". ASI nadaje uprawnienia w systemie informatycznym na podstawie upoważnienia.
Administrator Bezpieczeństwa Informacji jest odpowiedzialny za nadzór nad stosowaniem niniejszej procedury.

V. Stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzeniem i użytkowaniem.

Każdy użytkownik systemu lub programu otrzymuje parę: identyfikator/hasło.
Do systemu oraz aplikacji można uzyskać dostęp tylko po uprzednim poprawnym uwierzytelnieniu. Identyfikatory przyznawane są indywidualnie dla każdego z użytkowników i znane są tylko właścicielowi. Identyfikatory mają określony schemat w którym ciąg znaków identyfikuje użytkownika. ASI rejestruje nadane uprawnienia oraz daty ich nadania i wygaśnięcia. Identyfikator jest w sposób jednoznaczny przypisany użytkownikowi. Użytkownik odpowiada za wszelkie czynności wykonane przy użyciu identyfikatora.
W przypadku powzięcia przez użytkownika podejrzenia lub stwierdzenia, że z hasłem mogły zapoznać się osoby trzecie, obowiązany jest on niezwłocznie zmienić hasło i powiadomić o tym ASI.
Użytkownicy obowiązani są utrzymywać hasła w tajemnicy również po upływie ich ważności. Zabrania się zapisywania hasła i umieszczania na monitorze, pod klawiaturą lub w szufladzie biurka, na którym stoi stacja oraz w innych dostępnych miejscach.

1. Identyfikator Użytkownika:
   - jest niepowtarzalny,
   - po wyrejestrowaniu użytkownika z systemu informatycznego nie jest przydzielany innej osobie,
   - nie podlega zmianie, z wyjątkiem sytuacji, gdy zostanie ujawniony,
   - użytkownicy zobowiązani są do zachowania w tajemnicy ustalonych dla ich identyfikatorów,
   - jest wpisywany do ewidencji osób zatrudnionych przy przetwarzaniu danych wraz z imieniem i nazwiskiem użytkownika,
2. Hasło użytkownika:
   - jest przydzielane indywidualnie dla każdego z użytkowników i znane tylko użytkownikowi, który się nim posługuje,
   - zostaje zmienione przy pierwszym zastosowaniu (zalogowaniu użytkownika) po przydzieleniu przez ASI,
   - nie jest zapisywane w systemie w postaci jawnej,
   - jest zmieniane nie rzadziej niż 30 dni,
   - jest utrzymywane w tajemnicy, również po upływie jego ważności.
   - składa się z min. ośmiu znaków, zawiera małe i wielkie litery oraz cyfry lub znaki specjalne

Osobą odpowiedzialną w Urzędzie za sposób przydziału haseł dla użytkowników jest ASI, który je rejestruje i wyrejestrowuje.

VI. Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu.

1. Przed rozpoczęciem pracy, w trakcie rozpoczynania pracy z systemem informatycznym oraz w trakcie pracy, każdy pracownik obowiązany jest do zwrócenia bacznej uwagi, czy nie wystąpiły symptomy mogące świadczyć o naruszeniu ochrony danych osobowych. Wszystkie podejrzane sytuację lub błędy zgłaszane są do ASI.
2. Rozpoczęcie pracy użytkownika w systemie jest poprzedzone jego uwierzytelnieniem w systemie komputera. Wymagane jest wybór użytkownika i wpisanie hasła lub wpisanie zestawu: identyfikator/hasło. Po ich prawidłowym podaniu użytkownik może uruchomić aplikację służącą do przetwarzania danych. Dostęp do aplikacji jest również zabezpieczony przez parę identyfikator/hasło.
3. W razie zaistnienia potrzeby zawieszenia przetwarzania danych użytkownik jest zobowiązany do wylogowania się z konta systemu (nie jest konieczne opuszczanie aplikacji).
4. W pomieszczeniu, którym przetwarzane są dane osobowe, mogą znajdować się osoby postronne tylko za zgodą i w towarzystwie użytkownika.
5. Przed osobami postronnymi należy chronić: ekrany komputerów (ustawienie monitora powinno uniemożliwić podgląd), wydruki leżące na biurkach oraz w otwartych szafach.
6. Komputery wyposażone są we włączające się po **15 minutach** od przerwania pracy wygaszacze ekranu.
7. Użytkownik kończy pracę w aplikacji poprzez jej zamknięcie, co powoduje zakończenie sesji przetwarzania danych. Ponowne uruchomienie aplikacji wymaga ponownego uwierzytelnienia. Zakończenie pracy w systemie polega na wyłączeniu stacji roboczej lub wylogowaniu się użytkownika z konta dla niego przeznaczonego.
8. Użytkownik nie instaluje samodzielnie żadnego oprogramowania, dodatków, ani sterowników. Wszystkie wymagane modyfikacje wykonywane są przez ASI lub pod jego nadzorem. To samo dotyczy usuwania niepotrzebnego oprogramowania.
9. Obowiązuje zakaz robienia kopii całych zbiorów danych. Zbiory te mogą być kopiowane tylko przez ASI lub automatycznie przez system, z zachowaniem procedur ochrony danych osobowych.
10. Jednostkowe dane mogą być kopiowane na nośniki magnetyczne lub optyczne po ich zaszyfrowaniu i przechowywane w zamkniętych na klucz szafach. Po ustaniu przydatności kopii należy je trwale zniszczyć.
11. Obowiązuje zakaz wynoszenia na jakichkolwiek nośnikach całych zbiorów danych oraz obszernych z nich wpisów.
12. W określonych przypadkach za zgodą ASI lub ABI możliwe jest wynoszenie zbiorów do celów służbowych na nośnikach po uprzednim zaszyfrowaniu plików.
13. Przetwarzając dane osobowe należy odpowiednio często robić kopie robocze danych, na których się pracuje, tak aby zapobiec ich utracie.
14. Przed opuszczeniem pokoju należy:
    a) zniszczyć w niszczarce lub schować do zamykanych na klucz szaf wszelkie wykonane wydruki zawierające dane osobowe,
    b) wyłączyć komputer, drukarkę i UPS,
    c) zamknąć okna,
    d) umieścić klucze od szaf w ustalonym, przeznaczonym do tego miejscu,
    e) Opuszczając pokój, należy zamknąć za sobą drzwi na klucz, a klucz odnieść

zgodnie z procedurą kluczy.

15. Tryb pracy na komputerach przenośnych.
    a) Jeżeli jest to możliwe, to przy przetwarzaniu danych osobowych na komputerach przenośnych obowiązują procedury określone w niniejszej instrukcji dotyczącej pracy na komputerze stacjonarnym.
    b) Użytkownicy, którym zostały powierzone komputery przenośne, powinni chronić je przed uszkodzeniem, kradzieżą i dostępem osób postronnych: szczególną ostrożność należy zachować podczas ich transportu.
    c) Obowiązuje zakaz używania komputerów przenośnych przez osoby inne niż użytkownicy, którym zostały powierzone.
    d) Dyski zawierające dane osobowe przechowywane na komputerach przenośnych i na pendrive są **zaszyfrowane i opatrzone hasłem dostępu**.
    e) Obowiązuje zakaz samodzielnej modernizacji oprogramowania i sprzętu w powierzonych komputerach przenośnych. Wszelkie zmiany mogą być dokonywane tylko pod nadzorem ASI, stosownie do wymagań niniejszej instrukcji. W razie wystąpienia usterek w pracy komputerów przenośnych lub w razie wystąpienia konieczności aktualizacji ich oprogramowania należy zgłosić to ASI. Naruszenie przez użytkownika wyżej wymienionych postanowień może stanowić podstawę dla pociągnięcia użytkownika do odpowiedzialności dyscyplinarnej, odszkodowawczej lub karnej w trybie i na zasadach przewidzianych przepisami prawa.

VII. Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania.

1. Kopie zapasowe systemów informatycznych tworzy się w określonych systemach w terminach stosownych do potrzeb.
2. Każdą kopie tworzy się na oddzielnym nośniku informatycznym.
3. Zabrania się przechowywania kopii w pomieszczeniach przeznaczonych do przechowywania zbiorów.
4. ASI okresowo sprawdza przydatność kopii do użytku.
5. Stwierdzenie utraty przez kopię awaryjne waloru przydatności upoważnia ASI do ich zniszczenia.
6. Za tworzenie kopii systemów znajdujących się na serwerach odpowiada ASI.
7. Za archiwizowanie danych na stacjach roboczych odpowiada użytkownik chyba, że wcześniej zgłosił ten fakt ASI.
8. ASI prowadzi ewidencję komputerów.

VIII. Sposób, miejsce i okres przechowywania: elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych, o których mowa w rozdz. 4.

1. Wydruki komputerowe z systemu zawierające dane osobowe są:
    a) Sporządzane jedynie dla celów operacyjnych.
    b) Odpowiednio opisane i oznakowane.
    c) Elementem archiwum papierowego i podlegają zasadom dotyczącym przetwarzania danych osobowych w systemie archiwum papierowe.
    d) Przechowywane są w odpowiednich szafach i używane do celów operacyjnych przez określony czas wykorzystywania.

2. Zbiory danych przechowywane są generalnie na serwerach obsługujących systemy informatyczne. Dane przetwarzane w pamięci poszczególnych stacji roboczych są niezwłocznie umieszczane w odpowiednich miejscach na serwerach.
3. Zakazuje się przetwarzania danych osobowych na zewnętrznych nośnikach magnetycznych, optycznych i innych oraz ich przesyłania pocztą elektroniczną bez ich uprzedniego zaszyfrowania.
4. Na nośnikach, o których mowa w punkcie 2 dopuszczalne jest przetwarzanie jedynie jednostkowych danych.
5. Dostęp do nośników zawierających kopie danych mają tylko uprawnione osoby.
6. Nośniki raz użyte do przetwarzania danych osobowych nie mogą być wykorzystane do innych celów i podlegają ochronie w trybie niniejszej instrukcji.
7. Niszczenia nośników elektronicznych i kopii zapasowych na nośnikach magnetycznych, zleca się zewnętrznej firmie. Potwierdzeniem zniszczenia jest sporządzony protokół. Czynności nadzoruje ASI.
8. Kopie zapasowe danych przetwarzanych w tej samej lokalizacji są replikowane okresowo do innej lokalizacji. Kopie mogą być przechowywane w miejscu o odpowiednich zabezpieczeniach fizycznych (szafa metalowa).
9. Wszyscy pracownicy zobowiązani są przestrzegać terminów sporządzania kopii zapasowych oraz okresowo dokonywać kontroli możliwości odczytu danych zapisanych na tych kopiach.

IX. Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego.

1. Stacje robocze służące do przetwarzania danych zabezpieczone są za pomocą oprogramowania antywirusowego. Na bieżące i bezpośrednie sprawdzanie obecności wirusów komputerowych pozwala **oprogramowanie automatycznie monitorujące występowanie wirusów** w tracie załączania, wczytywania danych z zewnętrznych nośników informacji lub poprzez sieć wewnętrzną. Nadzór nad instalowaniem nowego oprogramowania antywirusowego oraz nad bieżącą jego aktualizacją sprawuje ASI. Kontrola antywirusowa jest przeprowadzana na wszystkich nośnikach magnetycznych i optycznych, służących zarówno do przetwarzania danych osobowych w systemie, jak i do celów instalacyjnych. Oprogramowanie antywirusowe jest systematycznie uaktualniane. O każdorazowym wykryciu wirusa przez oprogramowanie monitorujące użytkownik obowiązany jest niezwłocznie poinformować swojego przełożonego lub ASI.
2. Zablokowane są strony o treści pornograficznej, grach online, o treściach zawierających szkodliwy kod (adware, malware), oraz tematyce łamania zabezpieczeń (hacking), gaming. Cały ruch sieciowy do Internetu jest na bieżąco monitorowany, a logi z tego ruchu są przechowywane 180 dni.
3. Obowiązuje zakaz używania na komputerach służbowych prywatnych pendrive'ów oraz przewodowego lub bezprzewodowego podłączania do nich innych prywatnych nośników i urządzeń (np. smartfony, tablety itp.).
4. Obowiązuje zakaz samodzielnej instalacji i podłączania sprzętu komputerowego do sieci informatycznej Urzędu Gminy Radzyń Podlaski. Wszystkie czynności w przedmiotowym zakresie wykonuje ASI.
5. Wprowadza się następujące zabezpieczenia danych w systemach informatycznych: Pomieszczenia zamykane są na klucz, kartoteki znajdują się w zamykanych szafach. W budynkach Urzędu zainstalowany jest system alarmowy.
6. Prowadzone są szkolenia podstawowe dotyczące bezpieczeństwa danych obejmujące wszystkich pracowników Urzędu. System szkoleń szczegółowych

obejmuje pracowników zatrudnionych bezpośrednio przy przetwarzaniu danych, w tym danych osobowych. Tematyka szkoleń obejmuje: przepisy i instrukcje wewnętrzne Urzędu Gminy dotyczące ochrony danych, archiwizacji zasobów i przechowywania nośników, niszczenia wydruków i zapisów na nośnikach magnetycznych i optycznych.

X. Kontrola nad wprowadzaniem, dalszym przetwarzaniem i udostępnianiem danych osobowych.

1. System informatyczny umożliwia automatycznie:
   a) przypisanie wprowadzanych danych użytkownikowi, który te dane wprowadza do systemu,
   b) sygnalizację wygaśnięcia czasu obowiązywania hasła dostępu do stacji roboczej (również komputerów przenośnych),
   c) sporządzenie i wydrukowanie dla każdej osoby, której dane są przetwarzane w systemie, raportu zawierającego datę wprowadzenia danych, identyfikator użytkownika wprowadzającego dane, źródło danych, informację o odbiorcach, którym dane zostały udostępnione, sprzeciwie, o którym mowa w art. 32 ust. 1 pkt. 8 ustawy.

2. Odnotowanie informacji, o których mowa w ust. 1 podpunkt c, następuje automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzania danych.

XI. Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych. Naprawa urządzeń komputerowych z chronionymi danymi osobowymi.

1. Przeglądy i konserwacja systemów służących do przetwarzania danych osobowych wykonuje ASI doraźnie.
2. Przegląd i sprawdzanie poprawności zbiorów danych osobowych dokonuje użytkownik.
3. Prace dotyczące przeglądów, konserwacji i napraw wymagające autoryzowanych firm zewnętrznych, są wykonywane przez uprawnionych przedstawicieli tych firm (serwisantów) lub upoważnionej przez niego osoby bez możliwości dostępu do danych osobowych.
4. Urządzenia, dyski lub inne informatyczne nośniki informacji, przeznaczone do napraw, gdzie wymagane jest zaangażowanie autoryzowanych podmiotów zewnętrznych, pozbawia się przed naprawą zapisu tych danych albo naprawia się je pod nadzorem osoby upoważnionej przez ABI lub ASI.
5. Dostęp do serwerów produkcyjnych oraz serwerowni dla firm serwisujących jest regulowany osobnymi umowami.
6. Nośniki magnetyczne przekazywane na zewnątrz powinny być pozbawione zapisów zawierających dane osobowe. Niszczenie poprzednich zapisów powinno odbywać się poprzez pełne formatowanie nośnika.
7. Uszkodzone nośniki magnetyczne przed ich wyrzuceniem należy fizycznie zniszczyć (przeciąć, złamać).
8. Nośniki optyczne wielokrotnego zapisu CD-RW przekazywane na zewnątrz powinny być pozbawione zapisów zawierających dane osobowe. Niszczenie poprzednich zapisów powinno być wykonywane przez gruntowne kasowanie tych nośników. Nośniki optyczne CD-R nie powinny być przekazywane na zewnątrz jeżeli zawierały

dane osobowe. Niszczenie tych nośników powinno odbywać się w sposób mechaniczny (doszczętne zniszczenie pierwotnego kształtu).

XII. Postanowienia końcowe.

1. W sprawach nieokreślonych niniejszą instrukcją należy stosować instrukcję obsługi i zalecenia producentów aktualnie wykorzystywanych urządzeń i programów.
2. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest do zapoznania się przed dopuszczeniem do przetwarzania danych z niniejsza instrukcją oraz złożyć stosowne oświadczenie potwierdzające znajomość jej treści.
3. Naruszenie obowiązków wynikających z niniejszej instrukcji oraz przepisów o ochronie danych osobowych może być uznane za ciężkie naruszenie obowiązków pracowniczych, podlegające sankcjom dyscyplinarnym oraz sankcjom karnym, w szczególności wynikającym z art. 51-52 Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. (t.j. Dz. U. z 2016 r. poz. 922).

Załączniki:

Załącznik1/IZSI – Wniosek przyznania, zmiany, cofnięcia uprawnień użytkownika w systemie informatycznym,
Załącznik2/IZSI – Imienna karta uprawnień,
Załącznik3/IZSI – Rejestr nośników komputerowych zawierających dane osobowe,
Załącznik4/IZSI – Protokół zniszczenia nośników komputerowych zawierających dane osobowe,
Załącznik5/IZSI – Dziennik Administratora Systemu Informatycznego,
Załącznik6/IZSI – Procedura Zarządzania kopiami zapasowymi,
Załącznik7/IZSI – Polityka Zarządzania Oprogramowaniem.

Wójt Gminy
Radzyń Podlaski
Wiesław Mazurek

	Wniosek przyznania, zmiany, cofnięcia uprawnień użytkownika w systemie informatycznym **URZĄD GMINY RADZYŃ PODLASKI**	Załącznik nr 1/IZSI

Wniosek nr .....

Nadanie uprawnień	Modyfikacja uprawnień	Odebranie uprawnień
☐	☐	☐

Imię i Nazwisko użytkownika:	Stanowisko:
Miejsce przetwarzania danych:	**Dział:**
Identyfikator:	-
	-

Opis zakresu uprawnień:

ADM – uprawnienia administracyjne **P** – przeglądanie **PRN** – drukowanie **A** - archiwizowanie	**D** - dodawanie **E** – edytowanie **U** – usuwanie **I** – inne (jakie)

Nazwa programu/modułu w systemie informatycznym	ADM	P	PRN	A	D	E	U	I

Nazwa zbioru danych osobowych przetwarzanych w formie elektronicznej lub papierowej	ADM	P	PRN	A	D	E	U	I

Uwagi:

Data i podpis przełożonego użytkownika SI	
Data i podpis ASI	**Data i podpis ADO/ABI**

	Imienna ewidencja uprawnień URZĄD GMINY RADZYŃ PODLASKI	Załącznik nr 2/IZSI

IMIENNA EWIDENCJA UPRAWNIEŃ

L.p.	Imię i Nazwisko osoby uprawnionej	Data	Identyfikator użytkownika

	Rejestr nośników zawierających dane osobowe URZĄD GMINY RADZYŃ PODLASKI	Załącznik nr 3/IZSI

REJESTR NOŚNIKÓW ZAWIERAJĄCYCH DANE OSOBOWE

Lp.	*Oznaczenie/opis nośnika*	*Opis zawartości nośnika*	*Miejsce przechowywania*	*Uwagi*	*Data wpisu*	*Osoba odpowiedzialna za nośnik*

	Protokół zniszczenia nośników komputerowych zawierających dane osobowe URZĄD GMINY RADZYŃ PODLASKI	Załącznik nr 4/IZSI

.....
(data)

Protokół zniszczenia nośników komputerowych zawierających dane osobowe nr .....

Jednostka/komórka organizacyjna:

.....

Dnia ..... komisja powołana przez .....

/imię i nazwisko osoby powołującej komisję/

w składzie:

1) Przewodniczący komisji: .....

2) Członkowie: .....

.....

.....

dokonała trwałego zniszczenia nośników komputerowych:

Lp.	*Opis nośnika*	*Nr ewidencyjny*	*Sposób zniszczenia*	*Uwagi*

Dokonanie w/w czynności zostaje potwierdzone własnoręcznymi podpisami komisji:

.....

.....

.....

.....

Administrator Systemu Informatycznego

.....

/data, pieczęć i podpis/

	Dziennik **Administratora Systemu Informatycznego** **URZĄD GMINY RADZYŃ PODLASKI**	Załącznik nr 5/IZSI

DZIENNIK ADMINISTRATORA SYSTEMU INFORMATYCZNEGO

L.p.	Data	Godzina	Opis zdarzenia w systemie	Działania korygujące /zapobiegawcze	Uwagi

Procedura zarządzania kopiami zapasowymi

I. CEL PROCEDURY

Procedura zarządzania kopiami zapasowymi określa zasady tworzenia, przechowywania i testowania kopii zapasowych oraz odzyskiwania z nich danych i systemów informatycznych, w celu zapewnienia integralności i dostępności informacji oraz środków przetwarzania informacji.

II. ZAKRES STOSOWANIA

Działania opisane w niniejszej procedurze obowiązują, we wszystkich referatach, biurach i pozostałych komórkach organizacyjnych Urzędu Gminy Radzyń Podlaski.

Osoba odpowiedzialna za system Informatyczny zobowiązana jest do tworzenia kopii zapasowych. Poniżej procedura zarządzania kopiami zapasowymi. Administrator Systemów Informatycznych zobowiązany jest do prowadzenia rejestru czynności związanych z wykonywaniem kopii zapasowych. Dla każdego systemu powinien być prowadzony osobny rejestr.

III. WYKONYWANIE KOPII SYSTEMÓW INFORMATYCZNYCH

1. Na potrzeby zachowania ciągłości działania systemów informatycznych i utrzymania integralności danych wykonuje się kopie zapasowe zbiorów danych.
2. Zadanie to realizowane jest w cyklu dobowym systemowo, a w innych wymaganych sytuacjach po zakończeniu pracy.
3. Oprócz kopii codziennych wykonuje się kopie zapasowe w cyklu rocznym.
4. Czas przechowywania kopii zapasowych: dziennych – tydzień, rocznych – rok.
5. Kopie awaryjne wykonywane są na nośnikach magnetycznych, pamięciach zewnętrznych lub na nośnikach optycznych, a roczne na nośnikach optycznych.
6. Po ustaniu użyteczności kopii zapasowej jest ona niezwłocznie usuwana. Kopie zapasowe konfiguracji systemów operacyjnych serwerów wykonuje administrator systemu po każdej zmianie konfiguracji oprogramowania (np. po utworzeniu, rekonfiguracji lub usunięciu konta użytkownika w systemie, zmianie praw dostępu itp.)
7. Każda kopia zapasowa powinna być utworzona w ilości zapewniającej prawidłowe odtworzenie systemu.
8. Każdy z egzemplarzy kopii powinien być przechowywany w innej lokalizacji.
9. Przechowywanie nośników kopii zapasowych odbywa się w bezpiecznej odległości od serwerów systemu, aby uniknąć uszkodzeń spowodowanych katastrofą naturalną ośrodka, w którym znajduje się system.
10. Przechowywanie kopii zapasowych powinno odbywać się w sposób uniemożliwiający dostęp do nich osób nieuprawnionych, w tym administratorów innych systemów.
11. Kopie zapasowe muszą być opisane w sposób umożliwiający szybką identyfikację.
12. Za prawidłowość tworzenia kopii zapasowych odpowiada Administrator Systemu.
13. Administrator Systemu musi prowadzić spis posiadanych kopii zapasowych zgodnie z tabelą poniżej.

Spis powinien zawierać:

1) Nazwę systemu dla jakiego kopia została utworzona.
2) Dane osoby tworzącej i przekazującej kopie bezpieczeństwa.
3) Dane osoby pobierającej kopie bezpieczeństwa w celu jej przechowywania.
4) Datę i godzinę wykonania kopii.
5) Typ kopii (np. pełna, przyrostowa itp.).
6) Okres przydatności.

14. Spis może być prowadzony w formie elektronicznej.
15. W przypadku, gdy ważna jest poufność zaleca się, aby dane na nośnikach kopii zapasowych były szyfrowane.
16. Po ustaniu użyteczności kopii zapasowej jest ona niezwłocznie usuwana. Kopie zapasowe konfiguracji systemów operacyjnych serwerów wykonuje administrator systemu po każdej zmianie konfiguracji oprogramowania (np. po utworzeniu, rekonfiguracji lub usunięciu konta użytkownika w systemie, zmianie praw dostępu itp.).
17. Kopie, które przestały być aktualne należy zniszczyć.
18. Zniszczenia dokonuje się komisyjnie z udziałem Administratora Bezpieczeństwa Informacji lub innej osoby upoważnionej przez Administratora Danych Osobowych.
19. Z kopii, które podlegają zniszczeniu nie wolno sporządzać wydruków.

IV. TESTOWANIE KOPII ZAPASOWYCH

Kopie zapasowe sprawdzane są okresowo pod kątem ich dalszej przydatności przez administratora systemu nie rzadziej niż raz na dwa miesiące. Polega to na testowym odtworzeniu zawartości kopii na innym urządzeniu. Administrator systemu sporządza notatkę po każdym teście. Po stwierdzeniu nieprzydatności kopii zapasowych zbiorów, nośnik zostaje pozbawiony danych lub wybrakowany w inny sposób uniemożliwiający dalszy odczyt informacji.

V. ODZYSKIWANIE DANYCH I SYSTEMÓW INFORMATYCZNYCH Z KOPII ZAPASOWYCH

1) Odzyskiwanie danych z kopii zapasowych jest wykonywane w następujących przypadkach:
   a) utraty całości lub części danych na serwerze,
   b) utraty integralności całości lub części danych na serwerze,
   c) w celu odtworzenia poprzedniej wersji danych na wniosek referatu
   d) na wniosek organu kontrolnego (np.: NIK),
   e) przy przenoszeniu danych na nowy serwer.

Odzyskiwanie całego systemu informatycznego jest wykonywane w przypadku awarii sprzętowej lub systemowej nośników danych na których jest on zlokalizowany, uniemożliwiającej korzystanie z danego systemu. Za odzyskiwanie danych z kopii zapasowych odpowiada administrator systemu.

Wójt Gminy
Radzyń Podlaski
Wiesław Mazurek

	Procedura Zarządzania Kopiami Zapasowymi URZĄD GMINY RADZYŃ PODLASKI	Załącznik nr 6/IZSI

REJESTR CZYNNOŚCI ZWIĄZANYCH Z WYKONYWANIEM KOPII ZAPASOWYCH. DLA KAŻDEGO SYSTEMU POWINIEN BYĆ PROWADZONY OSOBNY REJESTR.

....

data wpisu *podpis ASI*

Lp.	Czynność	Sposób
1	Sposób wykonywania kopii	☐ System centralnych kopii zapasowych ☐ Narzędzia systemowe ☐ Narzędzia zewnętrzne ☐ Inne
2	Typ wykonywanych kopii	☐ Kopie pełne ☐ Kopie przyrostowe ☐ Kopie różnicowe
3	Nazwa systemu dla którego została utworzona kopia	☐ ..... ☐ ..... ☐ ..... ☐ .....
4	Dane poddane kopiowaniu	☐ Baza danych ☐ Pliki ☐ Stan systemów ☐ inne
5	Częstotliwość wykonywania kopii	☐ Codziennie ☐ Dwa razy dziennie ☐ Raz w tygodniu ☐ Raz w miesiącu ☐ Zbiorcza, raz na rok
6	Nośnik	☐ Taśma ☐ DVD ☐ Nośniki optyczne ☐ Inne
7	Miejsce przechowywania	☐ Sejf ☐ Metalowa szafa zamknięta na klucz ☐ Osobne pomieszczenie ☐ Osobny budynek
8	Okres przechowywania kopii	☐ Do roku

	zapasowych	☐ Do 3 lat ☐ Do 5 lat
9	Testowanie okresu przydatności kopii do użytku w przypadku awarii systemu	☐ Co 2 miesiące ☐ .....
10	Sposób niszczenia kopii	☐ Nadpisanie całości nośnika losowymi danymi ☐ Zniszczenie fizyczne ☐ Za pomocą dedykowanego urządzenia ☐ Za pomocą dedykowanego oprogramowania
11	Częstotliwość testowania poprawności zapisanych danych na kopii	☐ Raz na miesiąc ☐ Raz na kwartał ☐ Raz na 6 m-cy ☐ .....
12	Dane osoby tworzącej i przekazującej kopię	
13	Dane osoby pobierającej kopie bezpieczeństwa w celu jej przechowywania	
14	Data, godzina wykonania kopii	
15	Inne czynności	

POLITYKA ZARZĄDZANIA OPROGRAMOWANIEM

I. Wstęp

Urząd Gminy Radzyń Podlaski posiada świadomość legalnego i etycznego użytkowania oprogramowania. Ten dokument jest wskazówką dla pracowników jak upewnić się, że Urząd Gminy Radzyń Podlaski używa oprogramowanie zarówno legalnie jak i w sposób etyczny. Wszystkie zasoby oprogramowania są wykorzystywane wyłącznie służbowo i nie są używane przez pracowników we własnych celach.

II. Poziom Bezpieczeństwa

1. Uwzględniając konieczność zachowania bezpieczeństwa informacji w systemie informatycznym wprowadza się „poziom wysoki" bezpieczeństwa w rozumieniu § 6 Rozporządzenia.
2. Uwzględniając konieczność zachowania bezpieczeństwa przetwarzania informacji w systemie informatycznym Internet połączonym z siecią publiczną, wprowadza się „poziom wysoki" bezpieczeństwa w rozumieniu § 6 Rozporządzenia.

III. Polityka ogólna

1. Urząd Gminy Radzyń Podlaski posiada licencjonowane egzemplarze programów komputerowych różnych producentów oprogramowania. Licencjonowane i zarejestrowane egzemplarze programów zostały zainstalowane na komputerach oraz sporządzono odpowiednie kopie zapasowe oprogramowania zgodnie z warunkami umów licencyjnych. Bez pisemnej zgody producenta oprogramowania nie wolno wykonywać żadnych dodatkowych kopii programów ani też ich dokumentacji.
2. Poza oprogramowaniem komercyjnym w Urzędzie Gminy Radzyń Podlaski nie wykorzystuje się oprogramowania darmowego, czyli freeware oraz na licencji GPL. Na wykorzystanie darmowego oprogramowania wymagana jest zgoda ADO.
3. ASI prowadzi **Ewidencję Oprogramowania** zainstalowanego na poszczególnych stacjach roboczych, a w przypadku instalacji dodatkowych programów ASI dokonuje aktualizacji w Ewidencji Oprogramowania.

IV. Oprogramowanie z innych źródeł

1. Urząd Gminy Radzyń Podlaski wyposażył stanowiska komputerowe pracowników w legalne oprogramowanie. Używanie oprogramowania pochodzącego z jakiegokolwiek innego źródła, bez konsultacji z ASI może stanowić zagrożenie dla bezpieczeństwa oraz grozić wszczęciem postępowania prawnego – używanie takiego oprogramowania jest bezwzględnie zabronione.

2. Pracownicy są zobowiązani do zapoznania się z odpowiednimi przepisami o ochronie praw autorskich oraz kodeksu karnego przedstawionymi im przez ASI. Przepisy te mówią o odpowiedzialności pracownika w przypadku korzystania z nielegalnego oprogramowania.

V. Oprogramowanie stwarzające zagrożenia bezpieczeństwa danych

Pracownik nie będzie korzystał z zainstalowanego oprogramowania do nielegalnych celów oraz, nie będzie używał szkodliwych i niebezpiecznych programów (typu p2p, torrentów itp.), plików mp3, filmów w miejscu pracy, gdzie wykorzystywałby je do zabronionych celów.

VI. Dodatkowe kopie

1. W niektórych przypadkach umowa licencyjna pozwala na sporządzenie dodatkowej kopii określonego programu, przeznaczonej do użytkowania na komputerze przenośnym lub komputerze domowym wykorzystywanym do celów służbowych. Pracownicy nie mogą wykonywać dodatkowych kopii oprogramowania lub dokumentacji.
2. Łamanie, czy obchodzenie zabezpieczeń oprogramowania jest dopuszczalne wtedy i tylko wtedy, gdy chcemy wykonać jedną kopię danego oprogramowania do celów zabezpieczenia się w przypadku zniszczenia oryginalnego nośnika programu.
3. Niedopuszczalne jest wykonanie więcej niż jednej kopii oprogramowania. Chyba, że umowa licencyjna na to pozwala.

VII. Wewnętrzna kontrola

1. Urząd Gminy Radzyń Podlaski zastrzega sobie prawo do ochrony swojej reputacji i swoich inwestycji w programy komputerowe poprzez ustanowienie wewnętrznych mechanizmów kontroli zapobiegających wykonywaniu lub użytkowaniu nielegalnych kopii oprogramowania. Mechanizmy te obejmują niezapowiedziane przeglądy zawartości służbowych komputerów umożliwiające stwierdzenie zgodności zainstalowanego oprogramowania z umowami licencyjnymi, usuwanie wszelkich programów zainstalowanych na służbowych komputerach, dla których nie da się stwierdzić ważności licencji lub przedstawić jej dowodu, a także podjęcie postępowania dyscyplinarnego – łącznie ze zwolnieniem z pracy – w stosunku do pracowników naruszających postanowienia niniejszych zasad użytkowania oprogramowania.

VIII. Procedury zarządzania oprogramowaniem

1. Procedura zakupu oprogramowania komputerowego.
    a. ASI kontaktuje się z dystrybutorem oprogramowania w celu uzgodnienia szczegółów zakupu oprogramowania i licencji.
    b. Dostawca dostarcza nośnik z oprogramowaniem, licencję oraz fakturę zakupu, które stanowią podstawę legalności oprogramowania.
    c. W przypadku przedłużenia licencji, opieki autorskiej bądź aktualizacji oprogramowania ASI pisemnie kontaktuje się z odpowiednimi dystrybutorami.
    d. Wszelkie zakupy oprogramowania zatwierdza bezpośredni przełożony ASI.

e. Po zakupie oprogramowania komputerowego ASI wpisuje je do **Ewidencji Oprogramowania Komputerowego** (*wzór załącznik: Ewidencja oprogramowania do Polityki Zarządzania Oprogramowaniem*) oraz przypisuje mu odpowiedni komputer.

2. Procedura instalacji oprogramowania.
   a. Proces instalacji dokonuje tylko ASI lub w pracownik firmy zewnętrznej, ale tylko i wyłącznie w obecności ASI.
   b. ASI zapoznaje pracownika z nowo zainstalowanym oprogramowaniem i poucza o legalnym wykorzystaniu oprogramowania.
3. Procedura aktualizacji oprogramowania.
   a. W przypadku, kiedy pozwala na to licencja programu aktualizacja może być darmowa. Wykonuje ją pracownik lub ASI.
   b. W przypadku programów o określonym czasie licencji i płatnej aktualizacji, ASI wypełnia stosowne wnioski o aktualizacje oprogramowania.
4. Procedura likwidacji oprogramowania.
   a. W przypadku licencji OEM, program jest likwidowany razem ze sprzętem komputerowym.
   b. Programy, które są uważane za nieprzydatne mogą zostać zlikwidowane po trzech latach ich nieużytkowania.
5. Procedura audytu\inwentaryzacji oprogramowania.
   a. Procedura inwentaryzacji oprogramowania powinna odbywać się odbywa się dwa razy w roku. Przeprowadza ją ASI lub inna upoważniona przez Administratora Danych osoba.
   b. ASI po inwentaryzacji aktualizuje Ewidencję Oprogramowania Komputerowego.
   c. Lista programów jest aktualizowana po ewentualnych zakupach oprogramowania.

Wójt Gminy
Radzyń Podlaski
Wiesław Mazurek

	Ewidencja Oprogramowania URZĄD GMINY RADZYŃ PODLASKI	Załącznik Do Polityki Zarządzania Oprogramowaniem

EWIDENCJA OPROGRAMOWANIA W URZĘDZIE GMINY RADZYŃ PODLASKI

Lp.	Numer pomieszczenia	Nazwa programu	Wersja	Numer licencyjny	Numer komputera