ZARZĄDZENIE NR 122/2021
WÓJTA GMINY WEJHEROWO

z dnia 31 sierpnia 2021 r.

w sprawie wprowadzenia dokumentacji związanej z przetwarzaniem danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych

Na podstawie art. 33 ust. 1 i 2 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz.U. z 2021 r. poz. 1372) i art. 24 oraz 25 Rozporządzenia w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.), zarządza się, co następuje:

§ 1. Wprowadza się w Urzędzie Gminy Wejherowo „Politykę Bezpieczeństwa Informacji i Ochrony Danych Osobowych" stanowiącą załącznik nr 1 do niniejszego zarządzenia wraz z załącznikami.

§ 2. Wprowadza się w Urzędzie Gminy Wejherowo „Instrukcję postępowania w przypadku naruszenia zasad ochrony Danych Osobowych" stanowiącą załącznik nr 2 do niniejszego zarządzenia.

§ 3. Wprowadza się w Urzędzie Gminy Wejherowo „Instrukcję zabezpieczenia pomieszczeń Urzędu Gminy Wejherowo oraz postępowania z kluczami stanowiącą załącznik nr 3 do niniejszego zarządzenia.

§ 4. Zobowiązuje się wszystkich pracowników Urzędu Gminy Wejherowo, do zapoznania się z treścią niniejszego zarządzenia.

§ 5. Odpowiedzialnymi za wykonanie zarządzenia i przestrzegania zapisów dokumentów określonych w §1 – 3 są wszyscy pracownicy Urzędu Gminy Wejherowo oraz inne osoby upoważnione do przetwarzania danych.

§ 6. Nadzór nad wykonaniem zarządzenia powierza się Sekretarzowi Gminy Wejherowo.

§ 7. Traci moc Zarządzenie Wójta Gminy Wejherowo nr 42/2019 z dnia 14 marca 2019 r. w sprawie wprowadzenia dokumentacji związanej z przetwarzaniem danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

Wójt

Przemysław Kiedrowski

Załącznik Nr 1 do zarządzenia Nr 122/2021
Wójta Gminy Wejherowo
z dnia 31 sierpnia 2021 r.

POLITYKA BEZPIECZEŃSTWA INFORMACJI I OCHRONY DANYCH OSOBOWYCH W URZĘDZIE GMINY WEJHEROWO

2021 r.

Metryka dokumentu

Data	Wersja	Opis zmiany	Autor
18.05.2018 r.	1.0	Stworzenie dokumentu	Podmiot zewnętrzny MBM Sp. z o.o. z siedzibą w Białymstoku
19.03.2019 r.	2.0.	Aktualizacja dokumentu	Inspektor Ochrony Danych
31.08.2021 r.	3.0.	Aktualizacja dokumentu	Inspektor Ochrony Danych

Dokument przygotował:

Imię i nazwisko	Stanowisko	Podpis
Monika Wegner	Inspektor Ochrony Danych	
Jarosław Domarus	Starszy Informatyk – Administrator Systemów Informatycznych	

Dokument zatwierdził:	
Wójt Gminy Wejherowo	
Przewodniczący Rady Gminy	

DZIAŁ I

Rozdział 1

Postanowienia ogólne

§ 1

1. Polityka Bezpieczeństwa Informacji i Ochrony Danych Osobowych, zwana dalej „Polityką”, jest dokumentem określającym środki techniczne i organizacyjne przyjęte i stosowane przez Administratora Danych w celu zapewnienia ochrony danych osobowych. Ponadto celem niniejszej Polityki jest usprawnienie i usystematyzowanie organizacji pracy Administratora Danych, w zakresie przetwarzania danych osobowych.
2. Tryb postępowania w przypadku stwierdzenia naruszenia zabezpieczenia danych osobowych przetwarzanych w systemie informatycznym lub papierowym albo w sytuacji powzięcia podejrzenia o takim naruszeniu reguluje Instrukcja postępowania w przypadku naruszenia zasad ochrony danych osobowych stanowiąca integralną część Polityki Bezpieczeństwa Informacji.
3. Polityka jest dokumentem wewnętrznym Urzędu Gminy Wejherowo oraz w powiązaniu z innymi regulaminami, instrukcjami oraz zarządzeniami w przedmiocie ochrony danych wprowadzonymi przez administratora, tworzy kompleksowy system ochrony danych osobowych.
4. Polityka jest jednocześnie dokumentem określającym zadania osób zajmujących stanowiska kierownicze, samodzielne stanowiska pracy, pracowników oraz pracowników obsługi, a także pracowników i współpracowników podmiotów trzecich, które na mocy zawartych umów mają dostęp do informacji chronionych.
5. Polityka dotyczy wszystkich danych przetwarzanych przez Urząd Gminy Wejherowo, niezależnie od formy przetwarzania oraz od tego, czy dane są lub mogą być przetwarzane w zbiorach danych. Polityka reguluje w szczególności przetwarzanie danych w zbiorach ewidencyjnych prowadzonych w formie papierowej oraz w systemach informatycznych.
6. Polityka została opracowana zgodnie z wymogami określonymi w Rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych, zwane dalej RODO) i ma na celu wykazanie, że przetwarzanie danych odbywa się zgodnie z tym rozporządzeniem. W przypadku zmiany obowiązujących przepisów prawa powodujących niezgodność niniejszego dokumentu z nimi, Polityka zostanie dostosowana do obowiązujących przepisów.
7. Polityka jest przechowywana w wersji elektronicznej oraz w wersji papierowej w siedzibie Administratora. Dostępna jest u Inspektora Ochrony Danych oraz Sekretariacie Urzędu Gminy Wejherowo.
8. Integralną część Polityki Bezpieczeństwa Informacji stanowią:
   1) Instrukcja postępowania w przypadku naruszenia zasad ochrony danych osobowych;
   2) Instrukcja zabezpieczenia pomieszczeń Urzędu Gminy Wejherowo oraz postępowania z kluczami.

Rozdział 2
Definicje
§ 2

Przez użyte w Polityce określenia należy rozumieć:

1. **Administrator danych osobowych (ADO) –** oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych.
2. **Rozporządzenie** – rozporządzenie Parlamentu Europejskiego i Rady z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych osobowych) (Dz. Urz. UE L 119 z 04.05.2016 , str. 1 oraz Dz. Urz. UE L 127 z 23.05.2018, str. 2) zwana dalej także RODO;
3. **Ustawa** – ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych zwana w dalszej części ustawą;
4. **Inspektor ochrony danych –** rozumie się przez to osobę wyznaczoną przez administratora danych osobowych, posiadającą odpowiednie kwalifikacje zawodowe, wiedzę fachową na temat prawa i praktyk w dziedzinie ochrony danych osobowych oraz umiejętności wymagane do wypełniania zadań związanych z ochroną tych danych powołaną w celu informowania i doradzania Administratorowi, podmiotowi przetwarzającemu oraz pracownikom w zakresie obowiązującego prawa o ochronie danych oraz niniejszej polityki jak również w celu monitorowania ich przestrzegania oraz działania jako punkt kontaktowy dla podmiotów przetwarzających i organu nadzorczego.
5. **Administrator systemu informatycznego -** pracownik lub podmiot zewnętrzny odpowiedzialny za prawidłową pracę systemów informatycznych, w tym utrzymanie ciągłości działania oraz bezpieczeństwa w infrastrukturze informatycznej, inwentaryzowanie, okresowe sprawdzanie stanu urządzeń oraz sprzętu pozwalającego na obsługę czynności przetwarzania danych osobowych w systemach informatycznych.
6. **Dane osobowe** – informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;
7. **Zbiór danych osobowych** – oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;
8. **Przetwarzanie danych –** oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;
9. **Podmiot przetwarzający** - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;
10. **Odbiorca** - osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców;

przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania.

11. **Osoba upoważniona do przetwarzania danych osobowych lub użytkownik** – każda osoba świadcząca na rzecz Administratora pracę lub usługi w oparciu o jakikolwiek stosunek prawny, jeżeli to świadczenie pracy lub usług wiąże się z przetwarzaniem danych osobowych, posiadająca imienne upoważnienie do przetwarzania danych osobowych wydane przez Administratora, określające imię i nazwisko osoby upoważnionej, datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych, a także identyfikator jeżeli dane są przetwarzane w systemie informatycznym.
12. **Zabezpieczenie danych** – zabezpieczenie danych poprzez wdrożenie i eksploatację środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem.
13. **Naruszenie ochrony danych osobowych** – naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.
14. **System informatyczny** – zespół współpracujących ze sobą urządzeń, programów oraz narzędzi programowych zastosowanych w celu przetwarzania danych.
15. **Elektroniczny nośnik danych** – materiał lub urządzenie służące do zapisywania, przechowywania lub odczytywania danych osobowych w postaci cyfrowej lub analogowej;
16. **System tradycyjny** – rozumie się przez to zespół procedur organizacyjnych, związanych z mechanicznym przewarzaniem informacji oraz wyposażenia i środków trwałych w celu przetwarzania danych osobowych na papierze.
17. **Sieć lokalna** – połączenie systemów informatycznych administratora wyłącznie dla jego własnych potrzeb przy wykorzystaniu urządzeń i sieci telekomunikacyjnych.
18. **Identyfikator** – ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący użytkownika upoważnionego do przetwarzania danych w systemie informatycznym.
19. **Hasło** – ciąg znaków literowych, cyfrowych lub innych, znany jedynie Administratorowi oraz Użytkownikowi upoważnionemu do Przetwarzania Danych w Systemie informatycznym.
20. **Uwierzytelnianie** – proces, którego celem jest weryfikacja tożsamości deklarowanej przez Użytkownika.
21. **Pomieszczenia** – rozumie się przez to budynki, pomieszczenia lub części pomieszczeń określone przez Administratora Danych tworzące obszar, w którym przetwarzane są dane osobowe z użyciem stacjonarnego lub mobilnego sprzętu komputerowego oraz w systemie tradycyjnym.
22. **Uchybienie** - świadome lub nieświadome działania zmierzające do zagrożenia wskutek, których może dojść do utraty danych osobowych, kradzieży danych osobowych lub uszkodzenia nośników danych;
23. **Zagrożenie** - świadome lub nieświadome działania wskutek, których doszło do utraty danych osobowych, kradzieży danych osobowych lub uszkodzenia nośników danych.
24. **Urząd –** Urząd Gminy Wejherowo z siedzibą - ul. Transportowa 1, 84-200 Wejherowo;
25. **Wójt –** Wójt Gminy Wejherowo;
26. **Rada Gminy –** Rada Gminy Wejherowo;

Rozdział 3
Zakres i cel stosowania

§ 3

1. Celem Polityki Bezpieczeństwa jest ustalenie zasad przetwarzania danych osobowych zgodnie z przepisami dotyczącymi ochrony danych osobowych oraz ich ochrona przed udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów określających zasady postępowania przy przetwarzaniu danych osobowych oraz przed uszkodzeniem, zniszczeniem lub nieupoważnioną zmianą.
2. Zastosowane zabezpieczenia mają służyć osiągnięciu powyższych celów i zapewnić:
   1) **poufność danych** – rozumianą jako właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom;
   2) **integralność danych** – rozumianą jako właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
   3) **rozliczalność danych** – rozumianą jako właściwość zapewniającą, że działania osoby mogą być przypisane w sposób jednoznaczny tylko tej osobie;
   4) **integralność systemu** – rozumianą jako nienaruszalność systemu, niemożność jakiejkolwiek manipulacji, zarówno zamierzonej, jak i przypadkowej;
   5) **dostępność informacji** – rozumianą jako zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią zasobów wtedy, gdy jest to potrzebne.
3. Miarą bezpieczeństwa jest wielkość ryzyka związanego z ochroną danych osobowych, a zarządzanie ryzykiem rozumiane jest jako proces identyfikowania, kontrolowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa, które może dotyczyć systemów informatycznych i tradycyjnych (papierowych) służących do przetwarzania danych osobowych.

§ 4

1. W zależności od czynności przetwarzania danych osobowych oraz przepisów prawa określających zadania i kompetencje danych podmiotów za administratora danych osobowych w Gminie Wejherowo uznaje się **Wójta Gminy Wejherowo, Urząd Gminy Wejherowo reprezentowany przez Wójta Gminy Wejherowo, Radę Gminy Wejherowo reprezentowaną przez Przewodniczącego Rady Gminy Wejherowo.**

2. Administratorzy danych osobowych, o których mowa w ust. 1, powołują wspólnego Inspektora Ochrony Danych. Wzór upoważnienia dla Inspektora Ochrony Danych stanowi załącznik nr 1 do niniejszej Polityki.

3. Dopuszcza się możliwość powołania Zastępcy Inspektora Ochrony Danych Osobowych, do którego zadań będzie należała pomoc Inspektorowi Ochrony Danych w wykonywaniu zadań o których mowa w § 6 pkt 2 oraz zastępowanie Inspektora Ochrony Danych w przypadku jego usprawiedliwionej nieobecności. Wzór upoważnienia dla zastępcy Inspektora Ochrony Danych stanowi załącznik nr 2 do niniejszej Polityki.

4. Administratorzy Danych Osobowych, o których mowa w ust. 1, powołują wspólnego Administratora Systemów Informatycznych. Wzór upoważnienia dla Administratora Systemów Informatycznych stanowi załącznik nr 3 do niniejszej Polityki.

§ 5

1. Polityka ma zastosowanie wobec wszystkich administratorów wskazanych w § 4 ust. 1 oraz wobec wszystkich procesów przebiegających w ramach przetwarzania danych osobowych.
2. Zakres ochrony danych osobowych określony przez dokument Polityki ma zastosowanie w szczególności do:
   1) wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych oraz tradycyjnych (papierowych), w których przetwarzane są dane osobowe podlegające ochronie;
   2) wszystkich lokalizacji – budynków i pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie**;**
   3) wszystkich podmiotów odpowiedzialnych za ochronę i przetwarzanie danych osobowych, tj. pracowników, stażystów, praktykantów, wolontariuszy i innych osób mających dostęp do informacji podlegających ochronie.

Rozdział 4
Podmioty odpowiedzialne za ochronę danych i przetwarzanie danych osobowych
§ 6

Podmiotami odpowiedzialnymi za ochronę i przetwarzanie danych osobowych są:

1) Administrator Danych Osobowych (ADO), do którego zadań należą:
   a) podejmowanie decyzji o celach i środkach przetwarzania danych osobowych,
   b) wdrażanie odpowiednich środków technicznych i organizacyjnych, mających na celu zabezpieczanie przetwarzanych danych oraz zapewnianie poufności, integralności i dostępności danych,
   c) wyznaczenie Inspektora Ochrony Danych oraz ewentualnie Zastępcy Inspektora Ochrony Danych oraz zawiadomienie o tym fakcie Prezesa Urzędu Ochrony Danych Osobowych,
   d) wyznaczenie Administratora Systemów Informatycznych oraz określenie zakresu jego zadań i czynności w zakresie ochrony danych osobowych,
   e) podejmowanie odpowiednich działań w przypadku naruszenia lub podejrzenia naruszenia przetwarzanych danych zgodnie z procedurami określonymi w niniejszej Polityce,
   f) upoważnienie poszczególnych osób do przetwarzania danych osobowych w określonym indywidualnie zakresie,
   g) podejmowanie decyzji dotyczących przeprowadzenia oceny skutków planowanych operacji przetwarzania danych po konsultacji z Inspektorem Ochrony Danych,
   h) wdrożenie Polityki Bezpieczeństwa Informacji wraz z załącznikami,
   i) wdrożenie Instrukcji Postępowania w przypadku naruszenia zasad ochrony danych osobowych,
   j) wdrożenie Instrukcji zabezpieczenia pomieszczeń Urzędu Gminy Wejherowo oraz postępowania z kluczami,
   k) kontrola przestrzegania procedur przetwarzania danych osobowych w Urzędzie Gminy Wejherowo.

2) Inspektor Ochrony Danych Osobowych (IODO), do którego zadań należą:

   a) organizacja bezpieczeństwa i ochrony danych osobowych zgodnie z wymogami ustawy i Rozporządzenia,

b) informowanie Administratora oraz osób, które przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy obowiązujących przepisów, kodeksów postępowania i zatwierdzonych mechanizmów certyfikacji,
c) nadzorowanie i monitorowanie przestrzegania przepisów prawa o ochronie danych osobowych oraz wewnętrznych procedur w dziedzinie ochrony danych osobowych,
d) prowadzenie szkoleń z zakresu ochrony danych osobowych,
e) aktualizacje i sprawowanie nadzoru nad dokumentacją z zakresu ochrony danych osobowych;
f) prowadzenie i aktualizacja rejestru czynności przetwarzania danych (RCPD) oraz rejestru wszystkich kategorii przetwarzania,
g) nadzorowanie wydawania i anulowania upoważnień do przetwarzania danych osobowych,
h) prowadzenie rejestru upoważnień do przetwarzania danych,
i) prowadzenie i aktualizacja rejestru umów powierzenia przetwarzania danych osobowych,
j) prowadzenie i aktualizacja rejestru naruszeń zasad ochrony danych osobowych,
k) informowanie Administratora o wystąpieniu incydentu,
l) współpraca z Administratorem w zakresie oceny skutków planowanych operacji przetwarzania danych,
m) pełnienie funkcji punktu kontaktowego dla Prezesa Urzędu Ochrony Danych Osobowych w kwestiach związanych z przetwarzaniem danych osobowych,
n) weryfikacja zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych,
o) nadzorowanie i monitorowanie realizacji obowiązku informacyjnego zgodnie z wymogami RODO.

3) Administrator Systemów Informatycznych (ASI), do którego zadań należą:
a) nadzór nad działaniem systemów informatycznych, w których przetwarzane są dane osobowe,
b) nadzór nad zapewnieniem awaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania,
c) nadzór nad tym aby komputery przenośne, w których przetwarzane są dane osobowe zabezpieczone były hasłem dostępu przed nieautoryzowanym uruchomieniem oraz aby komputery te nie były udostępniane osobom nieupoważnionym do przetwarzania danych osobowych,
d) nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych na których zapisane są dane osobowe,
e) zarządzanie hasłami użytkowników i sprawowanie nadzoru nad przestrzeganiem procedur określających częstotliwość ich zmiany zgodnie z wytycznymi, które zawarte są w Polityce w części odnoszącej się do sposobu zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji,
f) nadzór nad czynnościami związanymi ze sprawdzaniem systemu pod kątem obecności wirusów komputerowych, częstości ich sprawdzania, nadzór nad wykonywaniem procedur uaktualniania systemów antywirusowych i ich konfiguracji,
g) nadzór nad wykonywaniem kopii awaryjnych, ich przechowywaniem oraz okresowym sprawdzaniem pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu,

h) nadzór nad przeglądami, konserwacjami oraz uaktualnieniami systemów służących do przetwarzania danych osobowych oraz wszystkimi innymi czynnościami wykonywanymi na bazach danych osobowych,
i) nadzór nad systemem komunikacji w sieci komputerowej oraz przesyłaniem danych za pośrednictwem urządzeń teletransmisji,
j) nadzór nad obiegiem oraz przechowywaniem dokumentów zawierających dane osobowe generowanych przez system informatyczny. W zakresie nadzoru, o którym mowa wyżej administrator danych osobowych powinien dopilnować, aby osoby zatrudnione przy przetwarzaniu danych osobowych miały dostęp do niszczarki dokumentów w celu niszczenia błędnie utworzonych lub już niepotrzebnych wydruków komputerowych z danymi osobowymi,
k) nadzór nad funkcjonowaniem mechanizmów uwierzytelniania użytkowników w systemie informatycznym przetwarzającym dane osobowe oraz kontrolą dostępu do danych osobowych,
l) nadzór nad tym, aby – jeżeli istnieją odpowiednie możliwości techniczne – ekrany monitorów stanowisk komputerowych, na których przetwarzane są dane osobowe, automatycznie wyłączały się po upływie ustalonego czasu nieaktywności użytkownika,
m) podejmowanie natychmiastowych działań zabezpieczających stan systemu informatycznego w przypadku otrzymania informacji o naruszeniu zabezpieczeń systemu informatycznego lub informacji o zmianach w sposobie działania programu lub urządzeń wskazujących na naruszenie bezpieczeństwa danych,
n) analiza sytuacji, okoliczności i przyczyny, które doprowadziły do naruszenia bezpieczeństwa danych (jeśli takie wystąpiło) i przygotowanie oraz przedstawienie wraz z Inspektorem Ochrony Danych Administratorowi Danych odpowiednich zmian do instrukcji zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych. Zmiany te powinny być takie, aby wyeliminować lub ograniczyć wystąpienie podobnych sytuacji w przyszłości.

4) Osoby upoważnione do przetwarzania danych osobowych, do których zadań należą:

a) przestrzeganie przepisów prawa powszechnie obowiązującego i regulacji dotyczących ochrony danych osobowych w tym przestrzegania zasad wynikających z konieczności realizowania obowiązku informacyjnego,
b) zgłaszanie nowych zbiorów danych oraz nowych czynności przetwarzania danych do Inspektora Ochrony Danych,
c) zgłaszanie Inspektorowi Danych Osobowych konieczności zawarcia umowy powierzenia przetwarzania danych osobowych, a w przypadku jakichkolwiek w tym zakresie wątpliwości konsultowania zasadności jej zawarcia z Inspektorem Ochrony Danych,
d) bieżąca ocena funkcjonowania mechanizmów zabezpieczeń i ochrony,
e) występowanie z wnioskami w sprawie wprowadzenia niezbędnych zmian w zakresie ochrony danych osobowych,
f) dokładanie należytej staranności w celu ochrony interesu osób, których dane są gromadzone i przetwarzane,
g) przestrzeganie i realizowanie praw osób, których dane są przetwarzane wynikających z Rozporządzenia,

h) powiadamianie osób, których dane dotyczą o sprostowaniu lub usunięciu danych osobowych lub o ograniczeniu przetwarzania, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku,
i) przetwarzanie danych zgodnie z zakresem udzielonego upoważnienia,
j) zachowanie w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia w trakcie wykonywania czynności związanych z przetwarzaniem danych osobowych jak również po ich zakończeniu,
k) niezwłoczne zgłaszanie incydentów dotyczących bezpieczeństwa danych osobowych zgodnie z instrukcją postępowania w przypadku naruszenia zasad ochrony danych osobowych,
l) konsultowanie z administratorem lub inspektorem ochrony danych osobowych wszelkich wątpliwości z zakresu interpretacji przepisów odnoszących się do zasad ochrony danych osobowych,
m) wypełnianie wobec osób, których dane dotyczą obowiązków informacyjnych , o których mowa w art. 13 i 14 Rozporządzenia,
n) konsultowanie z Inspektorem Ochrony Danych klauzul informacyjnych, umów powierzenia przetwarzania danych oraz formularzy zgód na przetwarzanie danych osobowych przed ich zastosowaniem.

Rozdział 5
Podstawy przetwarzania danych osobowych

§ 7

1. Przetwarzanie danych osobowych jest dopuszczalne tylko wtedy, gdy zostanie spełniona jedna z przesłanek wynikających z art. 6 ust. 1 lit. a - f Rozporządzenia w przypadku przetwarzania danych zwykłych, bądź jedna z przesłanek wskazanych w art. 9 ust. 2 lit. a – j Rozporządzenia w przypadku danych szczególnej kategorii.

2. W przypadku przetwarzania danych na podstawie zgody osoby, której dane dotyczą, należy stosować oświadczenie o wyrażeniu zgody na przetwarzanie danych osobowych.

3. W każdym wypadku zgoda na przetwarzanie danych osobowych musi mieć charakter dobrowolny, a nadto spełniać warunki, o których mowa w art. 7 Rozporządzeniu.

4. Przed zastosowaniem zgody na przetwarzanie danych osobowych każdy pracownik zobowiązany jest skonsultować formularz zgody z Inspektorem Ochrony Danych.

DZIAŁ II

Przetwarzanie danych osobowych

Rozdział 1
Zbiory danych osobowych i obszary przetwarzania danych
§ 8

1. W celu zapewnienia bezpiecznych warunków przetwarzania danych w systemach Urzędu, określa się obszary przetwarzania danych jako:
1) obiekty, wydzielone pomieszczenia lub części pomieszczeń, w których przetwarzane są

dane,

2) części obiektów, w których znajdują się informatyczne urządzenia - wyjścia (np. monitory, drukarki itp.).

2. Wykaz budynków i pomieszczeń, w których przetwarzane są dane osobowe znajduje się w załączniku nr 4 do niniejszej Polityki.

3. Przetwarzanie danych osobowych z użyciem stacjonarnego sprzętu komputerowego oraz w systemie tradycyjnym odbywa się wyłącznie w obszarze przetwarzania, o którym mowa w ust. 2.

4. Przetwarzanie danych osobowych w urządzeniach przenośnych może odbywać się poza obszarem przetwarzania danych, na warunkach wskazanych w niniejszej Polityce.

5. Dane osobowe gromadzone są w zbiorach danych w ramach poszczególnych czynności ich przetwarzania.

6. Administrator prowadzi Rejestr Czynności Przetwarzania Danych Osobowych zwany dalej „RCPD" i który jest na bieżąco aktualizowany jest przez Inspektora Ochrony Danych Osobowych. Wzór RCPD stanowi załącznik nr 5 do niniejszej Polityki. Dopuszcza się prowadzenie RCPD w formie elektronicznej.

7. W przypadku przetwarzania danych w imieniu innego Administratora podmiot przetwarzający prowadzi rejestr wszystkich kategorii czynności przetwarzania. Wzór rejestru wszystkich kategorii przetwarzania stanowi załącznik nr 6 do niniejszej Polityki. Dopuszcza się prowadzenie rejestru wszystkich kategorii przetwarzania w formie elektronicznej.

8. Każdy pracownik podejmujący się nowej czynności przetwarzania ma obowiązek poinformowania o niej Inspektora Ochrony Danych, celem jej wprowadzenia do RCPD.

9. Osoby upoważnione do przetwarzania danych osobowych mogą przetwarzać dane tylko w wyznaczonych do tego miejscach z zachowaniem dedykowanego do tej czynności sprzętu informatycznego oraz innych urządzeń.

§ 9

1. W celu należytej ochrony danych osobowych oraz ograniczenia dostępu osób postronnych do pomieszczeń, w których zlokalizowano przetwarzanie danych osobowych pomieszczenie określone jako obszar przetwarzania danych powinno spełniać następujące warunki:
   1) być wyposażone w zamek mechaniczny lub elektroniczny zamykany każdorazowo, gdy opuszczają go pracownicy zatrudnieni przy przetwarzaniu danych. Nie dotyczy to pomieszczeń technicznych wyposażonych w drukarkę oraz skaner do której dostęp mają wszyscy pracownicy Urzędu;
   2) wyposażenie (meble) w tej części pomieszczenia powinny być tak ustawione, aby uniemożliwić lub utrudnić dostęp do tego obszaru przetwarzania danych osobom nieuprawnionym;
   3) monitory komputerów, na których dokonuje się przetwarzania danych, powinny być ustawione w sposób uniemożliwiający ich podgląd osobom nieuprawnionym;
   4) obszar przetwarzania powinien być chroniony przez wszystkie dni w roku przy czym ochronie powinny podlegać wszystkie pomieszczenia w stopniu adekwatnym do ich przeznaczenia;
   5) pomieszczenia, w których znajdują się serwery były wyposażone w miarę możliwości w

sprawne systemy klimatyzacji, ochrony przeciwpożarowej oraz przeciwwłamaniowej.

2. W pomieszczeniach, w których przetwarzane są dane osobowe, należy stosować szczególne środki ostrożności, w tym:
   1) interesanci powinni wchodzić pojedynczo i pozostawać w pomieszczeniu tylko w obecności osoby upoważnionej do przetwarzania danych;
   2) dane osobowe przetwarzane w systemie tradycyjnym (papierowym) należy zabezpieczyć przed dostępem osób nieuprawnionych, chowając je na swoje miejsce po każdorazowym użyciu;
   3) po każdorazowym zakończeniu pracy należy zamknąć w szafach wszelką dokumentację, a następnie osobiście zabezpieczyć klucze z zachowaniem wszelkich zasad bezpieczeństwa;
   4) nie należy pozostawiać dokumentów papierowych i nośników elektronicznych w miejscach umożliwiających ich wykorzystanie przez osoby nieuprawnione. Dotyczy to również pomieszczeń technicznych wyposażonych w drukarkę oraz skaner, do której dostęp mają wszyscy pracownicy Urzędu;
   5) drukarki i urządzenia peryferyjne powinny być usytuowane lub zabezpieczone tak, aby osoby nieuprawnione nie miały dostępu do dokumentów na nich przetwarzanych. Należy zwracać uwagę czy do pomieszczeń, w których znajduje się drukarka i skaner nie mają dostępu interesanci;
   6) administrator danych osobowych powinien dopilnować, aby osoby zatrudnione przy przetwarzaniu danych osobowych miały dostęp do niszczarki dokumentów w celu niszczenia błędnie utworzonych lub już niepotrzebnych wydruków komputerowych z danymi osobowymi.

3. Przebywanie po godzinach pracy w pomieszczeniach, w których przetwarzane są dane osobowe jest dopuszczalne tylko w związku z pełnionymi obowiązkami i jedynie za zgodą administratora lub osoby przez niego upoważnionej.

§ 10

1. Poza miejsca przetwarzania danych wskazane w załączniku nr 4 nie wolno wynosić żadnej dokumentacji, ani akt związanych z wykonywaniem czynności służbowych, a zwłaszcza dokumentów lub innych nośników zawierających dane osobowe chyba, że jest to uzasadnione koniecznością wykonywania pracy zdalnej na wyraźne polecenie bezpośredniego przełożonego bądź po uzyskaniu jego uprzedniej zgody.
2. O możliwości wykonywania pracy zdalnej decyduje Administrator Danych Osobowych w odrębnym zarządzeniu.
3. Przepis powyższy nie dotyczy tych osób, których zakres obowiązków wymaga dokonywania czynności służbowych z dokumentacją lub innymi nośnikami zawierającymi dane osobowe poza obszarem przetwarzania danych, a także czynności związanych z przesyłaniem i transportem korespondencji.
4. Wykonywanie czynności, o których mowa w pkt 3 poza obszarem przetwarzania wymaga zgody kierownika referatu lub bezpośredniego przełożonego oraz uprzedniego poinformowania Inspektora Ochrony Danych.
5. Osoby opisane w ust. 4, które wynoszą jakiekolwiek dane poza obszar przetwarzania danych określony w załączniku nr 4, są zobowiązane stosować środki zapewniające ochronę powierzonych danych osobowych podczas ich transportu, przechowywania i użytkowania poza obszarem przetwarzania danych, a w szczególności zabezpieczyć te dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną,

przetwarzaniem z naruszeniem Rozporządzenia oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

6. Osoby takie ponoszą pełną odpowiedzialność za powierzony im sprzęt oraz dokumentację wyniesioną poza obszar przetwarzania danych.
7. Osoby posiadające komputery przenośne z zapisanymi w nich danymi osobowymi należy przeszkolić w kierunku zachowania szczególnej uwagi podczas ich transportu oraz uczulić na to, aby komputery te przechowywane były we właściwie zabezpieczonym pomieszczeniu.
8. Odpowiedzialność za bezpieczeństwo dokumentacji lub akt wynoszonych poza obszar przetwarzania danych ponosi pracownik lub inna osoba upoważniona do przetwarzania danych, która te akta wynosi, z chwilą ich pobrania. Odpowiedzialność ta dotyczy również danych znajdujących się na nośnikach cyfrowych.
9. Po zwrocie akt i dokumentacji lub przenośnych komputerów oraz innych cyfrowych nośników danych przez pracownika lub inną osobę upoważnioną do przetwarzania danych, osoba odpowiedzialna za wydanie akt i dokumentacji zobowiązana jest do jej sprawdzenia pod kątem zgodności ze stanem sprzed wypożyczenia.

Rozdział 2
Szkolenia pracowników
§ 11

1. Każdy pracownik, którego obowiązki wiążą się z przetwarzaniem danych osobowych przed dopuszczeniem do pracy z systemem informatycznym przetwarzającym dane osobowe lub zbiorami danych osobowych w wersji tradycyjnej (papierowej), zostaje poddany przeszkoleniu w zakresie ochrony danych osobowych w systemie informatycznym i tradycyjnym (papierowym).
2. Za zorganizowanie szkolenia odpowiada Administrator, który zleca jego przeprowadzenie Inspektorowi Ochrony Danych.
3. Przeprowadzenie szkolenia może zostać również zlecone Administratorowi Systemów Informatycznych lub podmiotowi zewnętrznemu posiadającemu odpowiednią wiedzę i doświadczenie do jego przeprowadzenia.
4. W przypadku nieobecności Inspektora Ochrony Danych szkolenie z zakresu ochrony danych osobowych przeprowadza bezpośredni przełożony pracownika w oparciu o postanowienia zawarte w niniejszym dokumencie, instrukcji postępowania w przypadku naruszenia zasad ochrony danych osobowych oraz instrukcji postępowania z kluczami oraz zabezpieczeń pomieszczeń Urzędu Gminy Wejherowo;
5. Szkolenie zostaje zakończone podpisaniem przez pracownika oświadczenia o wzięciu udziału w szkoleniu i jego zrozumieniu oraz zobowiązaniu się do przestrzegania przedstawionych w trakcie szkolenia zasad ochrony danych osobowych. Wzór potwierdzenia uczestnictwa w szkoleniu stanowi załącznik nr 7 do niniejszej Polityki.
6. Dokument, o którym mowa w ust. 5 jest przechowywany w aktach osobowych użytkowników i stanowi podstawę do podejmowania działań w celu nadania im uprawnień do korzystania z systemu informatycznego i tradycyjnego (papierowego) przetwarzającego dane osobowe, jak również w celu wyciągania konsekwencji w przypadku ich nieprzestrzegania.
7. Stosownie do potrzeb wynikających ze zmian w systemie informatycznym (zmiana sprzętu na sprzęt nowszej generacji, zmiana oprogramowania) oraz w związku ze zmianą przepisów o ochronie danych osobowych lub zmianą wewnętrznych regulacji wszyscy użytkownicy oraz pracownicy podlegają zaznajomieniu z wprowadzoną dokumentacją.

8. Fakt zaznajomienia z wprowadzonymi procedurami bądź odpowiednimi do niej zmianami powinien znajdować odzwierciedlenie w stosownej dokumentacji.

Rozdział 3
Procedura nadawania upoważnień do przetwarzania danych osobowych

§ 12

1. Do przetwarzania danych osobowych mogą być dopuszczone tylko osoby posiadające pisemne upoważnienia do przetwarzania danych osobowych, wydane przez ADO, wraz z oświadczeniem o zobowiązaniu się do zachowania w tajemnicy i poufności danych osobowych. Wzór upoważnienia stanowi załącznik nr 8 do niniejszej Polityki.

2. Z wnioskiem o nadanie upoważnienia do przetwarzania danych osobowych występuje do Inspektora Ochrony Danych:

   1) w stosunku do pracowników zatrudnionych na samodzielnych stanowiskach pracy oraz kierowników referatów – Sekretarz Gminy;
   2) w stosunku do pozostałych pracowników samorządowych - Kierownik Referatu, w którym pracownik zostaje zatrudniony;
   3) w stosunku do osoby niebędącej pracownikiem Urzędu – pracownik Urzędu koordynujący działania osoby, dla której upoważnienie jest wydawane.

3. Upoważnienia do przetwarzania danych osobowych dla pierwszego oraz drugiego zastępcy wójta, sekretarza, skarbnika nadaje samodzielnie Wójt Gminy Wejherowo.
4. W przypadku nieobecności Inspektora Ochrony Danych wniosek, o którym mowa w ust. 2 kieruje się bezpośrednio do Administratora Danych Osobowych.
5. Inspektor Ochrony Danych po przygotowaniu upoważnień, na wniosek o którym mowa w ust. 2, przekazuje dokument Administratorowi Danych Osobowych do podpisu.
6. Wzór wniosku o nadanie upoważnienia do przetwarzania danych osobowych stanowi załącznik nr 9 do niniejszej Polityki.
7. Nadzór nad nadawaniem upoważnień sprawuje Inspektor Ochrony Danych oraz Administrator Danych Osobowych.
8. Upoważnienie do przetwarzania danych osobowych w systemie tradycyjnym oraz informatycznym nadaje się w jednym dokumencie, o którym mowa w ust. 1 z zastrzeżeniem regulacji zawartej w § 21 niniejszej Polityki.
9. Administrator danych osobowych nadając pracownikom i innym osobom, przetwarzającym dane pisemne upoważnienia odbiera od nich oświadczenie o:
   1) zachowaniu danych w poufności na czas trwania stosunku pracy lub innego tytułu, na podstawie którego nadano upoważnienie, jak również po jego ustaniu;
   2) zapoznaniu się z dokumentami określającymi zasady zabezpieczania i przetwarzania danych osobowych w podmiocie, tj. Polityką Bezpieczeństwa, Instrukcją Postępowania w przypadku naruszenia ochrony danych osobowych oraz Instrukcją postępowania z kluczami oraz zabezpieczeń pomieszczeń Urzędu Gminy Wejherowo.
10. Wydane upoważnienia podlegają ewidencji w rejestrze upoważnień do przetwarzania danych osobowych, prowadzonego przez Inspektora Ochrony Danych, którego wzór stanowi załącznik nr 10 do niniejszej Polityki, przy czym dopuszcza się możliwość prowadzenia ewidencji w formie elektronicznej.
11. Od osób, których zakres obowiązków pracowniczych nie jest związany z przetwarzaniem danych osobowych odbiera się oświadczenie o obowiązku zachowania danych w poufności, do

których uzyskać mogą dostęp przy okazji wykonywania obowiązków pracowniczych. Wzór oświadczenia stanowi załącznik nr 11 do niniejszej Polityki.

12. Oświadczenia o obowiązku zachowania danych w poufności podlegają ewidencji w rejestrze przyjętych oświadczeń prowadzonym przez Inspektora Ochrony Danych, którego wzór stanowi załącznik nr 12 do niniejszej Polityki, przy czym dopuszcza się możliwość prowadzenia ewidencji w formie elektronicznej.
13. Upoważnienia do przetwarzania danych osobowych mogą być również nadawane w formie poleceń (np. upoważnienia do przeprowadzenia kontroli, audytów, wykonywania czynności służbowych, udokumentowanego polecenia Administratora w postaci umowy powierzenia przetwarzania danych).
14. Oryginał upoważnienia do przetwarzania danych osobowych oraz oświadczenie, o zachowaniu danych w poufności przechowuje się w aktach osobowych pracownika.
15. Rozwiązanie stosunku pracy lub odwołania z pełnionej funkcji powoduje wygaśnięcie upoważnienia do przetwarzania danych osobowych bez konieczności wydawania przez administratora unieważnienia.
16. Upoważnienia do przetwarzania danych osobowych udzielane są również wolontariuszom, praktykantom, stażystom, zleceniobiorcom.
17. Zakończenie stażu, praktyki, wolontariatu powoduje wygaśnięcie upoważnienia do przetwarzania danych osobowych bez konieczności wydawania przez administratora unieważnienia.
18. W przypadku rozwiązania stosunku pracy lub odwołania z pełnionej funkcji, zakończenia stażu, praktyki, wolontariatu lub zakończenia innych czynności związanych z nadanym upoważnieniem administrator systemów informatycznych zobowiązany jest unieważnić przydzielony użytkownikowi dostęp do wszystkich systemów informatycznych obsługiwanych w Urzędzie Gminy Wejherowo. Podstawą do unieważnienia dostępu jest informacja przekazana przez Kierownika Referatu Organizacyjnego i Kadr lub Inspektora Ochrony Danych Osobowych.
19. W przypadku zmiany stanowiska, zakresu obowiązków lub w sytuacji, która wpływa bezpośrednio na rodzaj i zakres przetwarzanych danych osobowych, podmioty, o których mowa w ust. 2 są zobowiązanie do niezwłocznego zgłoszenia tego faktu Inspektorowi Ochrony Danych w celu odpowiedniego zmodyfikowania upoważnienia. W takim przypadku stosuje się odpowiednio zapisy dotyczące nadawania upoważnień.
20. Względem nadanych upoważnień stosuje się następującą metodykę numeracji:

    1) wobec upoważnień dla pracowników: kolejny numer upoważnienia/rok, w którym nadawane jest upoważnienie (Przykład: 1/2021);

    2) wobec stażysty, praktykanta, wolontariusza: kolejny numer upoważnienia/rok, w którym nadawane jest upoważnienie/oznaczenie odpowiednio: praktykant, stażysta, wolontariusz (Przykłady: 1/2021/Praktykant, 1/2021/Stażysta, 1/2021/Wolontariusz);

    3) wobec innych osób, którym nadawane są upoważnienia oraz zleceniobiorców: kolejny numer upoważnienia/rok, w którym nadawane jest upoważnienie/oznaczenie przedmiotu upoważnienia (Przykład: 1/2021/Zleceniobiorca, 1/2021/Monitoring; 1/2021/Podatki);

    4) wobec pracownika, zleceniobiorcy, praktykanta, stażysty, wolontariusza lub innej upoważnionej osoby, dla którego nadawane jest upoważnienie do kolejnego systemu informatycznego, lub innego zbioru danych: stosuje się metodę wskazaną w punkcie od 1-3 oraz dodatkowe oznaczenie numeru aktualizacji upoważnienia zaczynając od numeru „2”, (Przykład: 1/2021/2, 1/2021/Praktykant/2).

Rozdział 4
§ 13
Zbieranie danych osobowych

1. Dane osobowe przetwarzane w urzędzie gminy mogą być pozyskiwane bezpośrednio od osób, których te dane dotyczą bądź z innych źródeł.
2. Administrator podczas pozyskiwania danych osobowych bezpośrednio od osób, których dane dotyczą podaje informacje wynikające z obowiązku informacyjnego, o którym mowa w § 15 niniejszej Polityki.
3. W przypadku zbierania danych osobowych nie od osoby, której te dane dotyczą, należy zapewnić, że istnieje podstawa prawna przetwarzania danych i również wypełnić obowiązek informacyjny określony w § 15 niniejszej Polityki chyba, że zachodzi jeden z przypadków, o którym mowa w art. 14 ust. 5 lit. a – d Rozporządzenia.
4. Przetwarzanie, w tym przechowywanie danych osobowych powinno się odbywać w postaci umożliwiającej identyfikację osób, których dotyczą.
5. Przetwarzanie, w tym przechowywanie danych osobowych powinno się odbywać nie dłużej niż jest to niezbędne do realizacji celu przetwarzania.
6. Dane osobowe, które są zbierane powinny być merytorycznie poprawne.
7. Zakres danych osobowych, które są zbierane powinien być adekwatny w stosunku do celu, w jakim dane zostały zebrane.
8. Zebrane dane po upływie realizacji celu przetwarzania mogą być przechowywane w dalszym ciągu w przypadku, gdy odpowiedni przepis prawa wymaga ich archiwizacji przez określony czas.

Rozdział 5
Udostępnienie i powierzanie danych osobowych

§ 14

1. Administrator danych osobowych jest uprawniony do udostępnienia danych wyłącznie podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa oraz osobom, których dane dotyczą.
2. Udostępnienie danych osobowych może nastąpić tylko za zgodą Administratora Danych.
3. Dane osobowe powinny być przekazywane uprawnionym podmiotom lub osobom za potwierdzeniem odbioru listem poleconym, za pokwitowaniem odbioru lub innym bezpiecznym sposobem, określonym prawem lub umową.
4. Udostępniając dane osobowe innym podmiotom należy fakt ten odnotować bezpośrednio w systemie informatycznym, z którego udostępniono dane osobowe, o ile system posiada takie właściwości lub w inny zatwierdzony sposób, np. w odrębnym rejestrze. Udostępniając dane osobowe należy odnotować informacje o osobie udostępniającej dane osobowe, odbiorcy danych osobowych, dacie udostępnienia danych oraz zakresie udostępnionych danych osobowych.

5. Podmiot występujący o udostępnienie danych osobowych powinien wskazać podstawę prawną upoważniającą go do otrzymania tych danych albo uzasadnioną potrzebę żądania ich udostępniania w celu dokonania oceny, czy w określonym przypadku udostępnienie danych jest prawnie dopuszczalne i czy nie będzie ono stanowić naruszenia zasad ochrony danych osobowych.
6. W przypadku niewskazania podstawy prawnej Administrator wzywa podmiot występujący z wnioskiem o udostępnienie danych o wskazanie podstawy prawnej udostępnienia wyznaczając termin 14 dni od dnia odbioru wezwania.
7. W przypadku niewskazania podstawy prawnej wniosek o udostępnienie danych pozostawia się bez rozpoznania.
8. Wzór wniosku o udostępnienie danych osobowych stanowi załącznik nr 13 do niniejszej Polityki.
9. Kierownicy referatów oraz osoby zajmujące samodzielne stanowiska urzędnicze są zobowiązani do samodzielnego prowadzenia rejestru udostępniania danych.
10. W przypadku konieczności powierzenia przetwarzania danych przez administratora podmiotom zewnętrznym, które będą przetwarzać dane w imieniu administratora niezbędne jest zawarcie pisemnej umowy powierzenia przetwarzania danych.
11. Umowa powierzenia przetwarzania danych powinna określać w szczególności zakres i cel przetwarzania danych. Umowa musi także określać zakres odpowiedzialności podmiotu, któremu powierzono przetwarzanie danych z tytułu niewykonania lub nienależytego wykonania umowy oraz sposób rozwiązania umowy. Powierzenie przetwarzania danych osobowych musi uwzględniać ponadto wymogi określone w art. 28 Rozporządzenia. W szczególności podmiot zewnętrzny, któremu ma zostać powierzone przetwarzanie danych osobowych, jest zobowiązany przed rozpoczęciem przetwarzania danych do podjęcia środków zabezpieczających zbiór danych.
12. W przypadku konieczności zawarcia umowy w trybie przetargowym, która może wiązać się z obowiązkiem zawarcia umowy powierzenia przetwarzania danych przed określeniem wzoru umowy oraz specyfikacji istotnych warunków zamówienia niezbędna jest konsultacja z Inspektorem Ochrony Danych.
13. Powierzenie przetwarzania danych osobowych nie oznacza zwolnienia z odpowiedzialności administratora danych za zgodne z prawem przetwarzanie powierzonych danych, co wymaga umieszczenia, w umowach stanowiących podstawę powierzenia przetwarzania danych, prawa administratora danych do kontroli wykonania przedmiotu umowy w siedzibie podmiotu zewnętrznego w zakresie ochrony danych osobowych bądź w innej formie dogodnej dla administratora.
14. Zawarte umowy powierzenia przetwarzania podlegają ewidencji w wykazie podmiotów którym powierzono przetwarzania danych prowadzonej przez Inspektora Ochrony Danych, który stanowi załącznik nr 14 do niniejszej Polityki, przy czym dopuszcza się możliwość prowadzenia rejestru w formie elektronicznej.
15. Powierzenie przetwarzania danych uregulowane w Polityce Bezpieczeństwa nie ma zastosowania do przekazywania danych podmiotom upoważnionym do ich przetwarzania na podstawie odrębnych przepisów prawa, w tym w szczególności ZUS, Prokuraturze, Policji, Sądom, Komornikom, itp. oraz podmiotom, którym należy udostępnić dane osobowe na podstawie przepisów prawa.
16. Wszyscy pracownicy zobowiązani są do każdorazowej konsultacji z Inspektorem Ochrony Danych zasadności zawierania umowy powierzenia przetwarzania, a po jej zawarciu poinformować Inspektora o tym fakcie. Obowiązek wskazany w zdaniu poprzednim dotyczy

również umów powierzenia przetwarzania danych, w których jako administratora wskazuje się podmiot, z którym Gmina zawiera umowę, a jako podmiot przetwarzający Wójta Gminy Wejherowo.

Rozdział 6
Obowiązek informacyjny przy przetwarzaniu danych

§ 15

1. Obowiązek informacyjny spoczywający na administratorze w myśl art. 13 i 14 RODO jest realizowany poprzez przekazanie osobie, której dane są przetwarzane informacji dotyczących pozyskiwania danych osobowych, a także ich dalszego przetwarzania.
2. Obowiązek informacyjny jest realizowany zarówno w przypadku zbierania danych od osoby, której dane dotyczą, jak również z innych źródeł.
3. Administrator realizuje obowiązek informacyjny poprzez wykorzystanie odpowiednich środków, które umożliwią w zwięzłej, przejrzystej i łatwo dostępnej formie udzielenie osobie, której dane dotyczą wszelkich informacji, o których mowa w art. 13 i 14 RODO.
4. Jedną z form spełniania obowiązku informacyjnego jest udostępnienie osobom, których dane osobowe są przetwarzane, klauzul informacyjnych.
5. Klauzule informacyjne winny być każdorazowo dostosowane do celu przetwarzania, podstawy prawnej i okresu przechowywania danych.
6. Każdy pracownik zobowiązany jest zwracać uwagę na aktualność przekazywanej klauzuli informacyjnej, a w przypadku wątpliwości konsultować jej treść z Inspektorem Ochrony Danych.
7. Zwolnienie z realizacji obowiązku informacyjnego znajduje zastosowanie w sytuacji, gdy dane pozyskiwane są od osoby, której te dane dotyczą a podmiot ten dysponuje już informacjami, o których mowa w art. 13 RODO oraz w zakresie uregulowanym przez przepisy krajowe, w szczególności przez ustawę o ochronie danych osobowych.
8. Obowiązek informacyjny należy spełnić w momencie zbierania danych.
9. W przypadkach, w zakresie których zastosowanie mają przepisy ustawy z dnia 14 czerwca 1960 r. kodeks postępowania administracyjnego obowiązek informacyjny, o którym mowa w art. 13 ust. 1 i 2 Rozporządzenia należy spełniać według zasad przewidzianych w tym kodeksie.
10. Przepisy zawarte w ustawie, o której mowa w ust. 9 regulujące sposób spełniania obowiązku informacyjnego to: art. 2a k.p.a., art. 54 § 1a k.p.a., art. 61 § 5 k.p.a., 122h k.p.a., 217a k.p.a., 226a k.p.a., 231 §2 k.p.a.

Rozdział 7

Prawa osób, których dane dotyczą

§ 16

1. Każdej osobie przysługuje prawo do kontroli przetwarzania danych, które jej dotyczą, zawartych w zbiorach danych osobowych przetwarzanych i przechowywanych w urzędzie gminy, a zwłaszcza prawo do uzyskania wyczerpującej informacji o przetwarzanych danych osobowych, które jej dotyczą.

2. Zgodnie z RODO, osobom, których dane osobowe są przetwarzane przysługują następujące prawa:

   1) Prawo do ochrony danych osobowych;

   2) Prawo do wyrażenia zgody;

   3) Prawo do informacji;

   4) Prawo dostępu do danych;

   5) Prawo do sprostowania danych;

   6) Prawo do usunięcia danych („prawo do bycia zapomnianym”);

   7) Prawo do ograniczenia przetwarzania;

   8) Prawo do przenoszenia danych;

   9) Prawo wniesienia sprzeciwu;

   10) Prawo do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;

   11) Prawo do kontaktu z Inspektorem Ochrony Danych;

   12) Prawo do wniesienia skargi do Urzędu Ochrony Danych Osobowych**,** w przypadku przetwarzania danych osobowych z naruszeniem przepisów RODO.

3. Na wniosek osoby, której dane dotyczą, zgodnie z ust. 1 i 2, ADO jest zobowiązany do udzielenia informacji. Informacja powinna być udzielona w formie pisemnej oraz powszechnie zrozumiałej.

4. W razie wniesienia żądania oraz wykazania przez osobę, które dane dotyczą, że jej dane osobowe są niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem przepisów albo są zbędne do realizacji celu, dla którego zostały zebrane, ADO bez zbędnej zwłoki dokonuje uzupełnienia, uaktualnienia, sprostowania danych, czasowego lub stałego wstrzymania przetwarzania kwestionowanych danych lub ich usunięcia ze zbioru, chyba, że dotyczy to danych osobowych, w odniesieniu do których tryb ich uzupełnienia, uaktualnienia lub sprostowania określają odrębne przepisy.

Rozdział 8
Ogólne środki służące do zabezpieczenia danych osobowych

§ 17

1. Administrator Danych Osobowych jest zobowiązany do zastosowania środków technicznych, organizacyjnych i fizycznych zapewniających ochronę przetwarzanych danych, a w szczególności do:

   1) zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym;

2) zapobiegnięcia zabrania danych przez osobę nieuprawnioną;
3) zapobiegnięcia przetwarzania danych z naruszeniem ustawy o ochronie danych osobowych oraz Rozporządzenia jak również zmianie, utracie, uszkodzeniu lub zniszczeniu tych danych.

2. Administrator w celu zapewnienia zgodności przetwarzania danych osobowych z powszechnie obowiązującymi przepisami wprowadził następujące zabezpieczenia organizacyjne:

1) sporządzono i wdrożono Politykę Bezpieczeństwa Informacji;
2) sporządzono i wdrożono Instrukcję postępowania z kluczami oraz zabezpieczenia pomieszczeń Urzędu Gminy Wejherowo, która stanowi integralną część Polityki bezpieczeństwa;
3) sporządzono Instrukcję postępowania w przypadku stwierdzenia naruszenia ochrony danych osobowych, która stanowi integralną część Polityki bezpieczeństwa;
4) Powołano Inspektora Ochrony Danych;
5) Powołano Administratora Systemów Informatycznych;
6) sporządzono Rejestr Czynności Przetwarzania Danych (RCPD);
7) sporządzono Rejestr wszystkich kategorii przetwarzania danych;
8) do przetwarzania danych zostały dopuszczone wyłącznie osoby posiadające upoważnienia nadane przez Administratora;
9) prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych;
10) osoby upoważnione do przetwarzania danych osobowych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych, treścią Polityki oraz jej załącznikami, Instrukcją postępowania w przypadku stwierdzenia naruszenia ochrony danych osobowych, Instrukcją zabezpieczenia pomieszczeń Urzędu Gminy Wejherowo oraz postępowania z kluczami;
11) osoby upoważnione do przetwarzania danych osobowych zostały zobowiązane do zachowania danych w tajemnicy;
12) osoby zatrudnione przez administratora danych osobowych, które nie zostały upoważnione do przetwarzania danych osobowych zostały zobowiązane do zachowania w poufności danych, do których uzyskają dostęp przy okazji wykonywania obowiązków pracowniczych;
13) przetwarzanie danych osobowych dokonywane jest w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych;
14) przebywanie osób nieuprawnionych w pomieszczeniach, gdzie przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby upoważnionej do przetwarzania danych osobowych oraz w warunkach zapewniających bezpieczeństwo danych;
15) wprowadzono zasadę „czystego biurka" oznaczającą utrzymywanie porządku na stanowisku pracy, a po zakończeniu pracy chowanie do szaf wszelkich dokumentów i akt;
16) wprowadzono zasadę stosowania zasady „czystego ekranu" - w przypadku chwilowego opuszczenia stanowiska pracy użytkownik zobowiązany jest do wylogowania się z systemu bądź zablokowania dostępu do pulpitu stacji roboczej w celu uniemożliwienia dostępu do systemu operacyjnego lub aplikacji przez osoby niepowołane. Ponadto w trakcie pracy użytkownik powinien mieć otwarte tylko te aplikacje, które są niezbędne do wykonywania obowiązków służbowych;
17) dokumenty i nośniki informacji zawierające dane osobowe, podlegające zniszczeniu, neutralizuje się za pomocą urządzeń do tego przeznaczonych lub dokonując modyfikacji, uniemożliwiającej odtworzenie ich treści, bez zaangażowania w to nadmiernych środków. administrator danych osobowych powinien dopilnować, aby osoby zatrudnione przy przetwarzaniu danych osobowych miały dostęp do niszczarki dokumentów w celu niszczenia

błędnie utworzonych lub już niepotrzebnych wydruków komputerowych z danymi osobowymi;

18) informacji telefonicznych zawierających dane osobowe nie udziela się, względnie udziela się po zidentyfikowaniu rozmówcy i stwierdzeniu jego upoważnienia do uzyskania danych. Identyfikacja rozmówcy powinna odbywać się w oparciu o dane będące już w posiadaniu Urzędu;

19) wszystkie osoby zatrudnione w Urzędzie Gminy lub upoważnione do przetwarzania danych osobowych zobowiązane są do stosowania się do pozostałych instrukcji i zarządzeń wewnętrznych związanych z bezpieczeństwem informacji.

3. Administrator w celu zapewnienia zgodności przetwarzania danych osobowych z powszechnie obowiązującymi przepisami wprowadził następujące środki ochrony fizycznej:

1) przetwarzanie danych osobowych odbywa się w wydzielonych pomieszczeniach położonych w strefie administracyjnej;
2) wykaz pomieszczeń, w których przetwarzane są dane osobowe stanowi załącznik nr 4 do niniejszej Polityki
3) urządzenia służące do przetwarzania danych osobowych oraz dokumentacja zawierającą dane osobowe przetwarzane w sposób tradycyjny przechowywana jest w pomieszczeniach zabezpieczonych drzwiami zwykłymi posiadającymi zamki mechaniczne chyba, że z przepisów prawa wynika obowiązek stosowania drzwi spełniających dodatkowe wymagania techniczne;
4) co do zasady zbiór danych osobowych przetwarzany w systemie tradycyjnym (papierowym) jest przechowywany w zamkniętej niemetalowej szafie, do której dostęp mają wyłącznie użytkownicy. W przypadku gdy wymaga tego przepis prawa zbiór danych w formie papierowej jest przechowywany w zamkniętej metalowej szafie, bądź w zamkniętym sejfie lub kasie pancernej;
5) każdy pracownik po zakończeniu pracy zobowiązany jest zamknąć w szafach wszelką dokumentację, a następnie osobiście zabezpieczyć klucze z zachowaniem wszelkich zasad bezpieczeństwa;
6) gdy wymaga tego szczególny przepis prawa, zbiory danych osobowych przetwarzane są w kancelarii tajnej, prowadzonej zgodnie z wymogami określonymi w odrębnych przepisach;
7) obszar, w którym przetwarzane są dane osobowe, chroniony jest poprzez:
   a) grupę interwencyjną,
   b) system alarmowy,
   c) czujniki ruchu,
   d) zamki patentowe,
   e) w niektórych poszczególnych pomieszczeniach – kraty w oknach, rolety antywłamaniowe;
8) otwieranie i zamykanie Urzędu odbywa się w obecności pracownika ochrony
9) w czasie przebywania w Urzędzie osób upoważnionych poza godzinami otwarcia Urzędu Gminy wejścia do budynku są zabezpieczone przed dostępem osób nieupoważnionych. Osoba opuszczająca budynek ma obowiązek zadbać o ponowne zabezpieczenie wejścia;
10) pomieszczenia, w których przetwarzane są dane osobowe otwierane są przez pierwszą osobę rozpoczynającą pracę oraz zamykane przez ostatnią wychodzącą osobę.

Rozdział 9
Naruszenia zasad ochrony danych osobowych

§ 18

W przypadku stwierdzenia naruszenia zabezpieczeń lub zaistnienia sytuacji, które mogą wskazywać na naruszenie zabezpieczenia danych osobowych, każdy pracownik/użytkownik przetwarzający dane osobowe zobowiązany jest przerwać czynności i niezwłocznie zgłosić ten fakt bezpośredniemu przełożonemu, a nadto postępować zgodnie z Instrukcją postępowania w przypadku naruszenia zasad ochrony danych osobowych.

Rozdział 10

Przeprowadzanie okresowych analiz ryzyka w zakresie bezpieczeństwa informacji

§ 19

1. W celu zapewnienia bezpieczeństwa informacji w Urzędzie Gminy przeprowadzana jest Analiza Ryzyka zgodnie z art. 5 ust. 2 oraz Motywem 76 Preambuły „RODO".
2. Głównym celem analizy ryzyka bezpieczeństwa informacji jest wyznaczenie właściwych kierunków działania kierownictwa oraz określenie priorytetów dla zarządzania ryzykami i zabezpieczeniami. Wyniki analizy ryzyka prowadzą do opracowania planu postępowania z ryzykiem obejmującego wprowadzenie rozwiązań umożliwiających odpowiednio: unikanie tych ryzyk, ograniczanie ich do akceptowanego poziomu, przeniesienie lub świadomą ich akceptację.
3. Zaleca się, by zarządzanie ryzykiem w bezpieczeństwie informacji zapewniało:
   1) zidentyfikowanie ryzyka;
   2) oszacowanie ryzyka z punktu widzenia następstw dla działalności oraz prawdopodobieństwa wystąpienia;
   3) informowanie o prawdopodobieństwie i następstwach ryzyka oraz zrozumienie tych informacji;
   4) ustanowienie priorytetów postępowania z ryzykiem;
   5) określenie priorytetów dla działań podjętych w celu zredukowania ryzyka;
   6) regularne monitorowanie i przegląd różnych typów ryzyka oraz procesu zarządzania ryzykiem;
   7) zbieranie informacji w celu doskonalenia podejścia do zarządzania ryzykiem;
   8) szkolenie kierownictwa oraz osób upoważnionych do przetwarzania danych osobowych w zakresie ryzyka oraz działań podejmowanych w celu postępowania z ryzykiem.

DZIAŁ III

Przetwarzanie danych osobowych w systemach informatycznych

Rozdział 1
Zabezpieczenie danych osobowych przetwarzanych w systemach informatycznych

§ 20

W celu ochrony przed utratą danych w Urzędzie Gminy Wejherowo stosowane są między innymi następujące zabezpieczenia techniczne:

1) ochrona serwerów przed zanikiem zasilania poprzez stosowanie zasilaczy awaryjnych UPS;
2) ochrona przed utratą zgromadzonych danych w systemach serwerowych przez robienie kopii zapasowych na nośnikach zewnętrznych, z których w przypadku awarii odtwarzane są dane;
3) ochrona przed awarią podsystemu dyskowego serwerów przez używanie macierzy dyskowych (uszkodzenie jakiegokolwiek z dysków nie spowoduje utraty danych);
4) zabezpieczenia przed nieautoryzowanym dostępem do baz danych Urzędu;
5) użytkownikami systemu informatycznego są osoby posiadające stosowne upoważnienie do przetwarzania danych osobowych nadane przez Administratora Danych Osobowych;
6) w systemie informatycznym Urzędu zastosowano odpowiednio jedno, dwu lub trzystopniową autoryzację użytkownika:

a) podstawą autoryzacji jest logowanie w celu uzyskania dostępu do stacji roboczej Urzędu, podając login użytkownika i hasło. Nie zawsze daje to dostęp do serwerów. Druga autoryzacja umożliwia podłączenie się do serwerów. Aby dokonać uruchomienia programu użytkowego, umożliwiającego dostęp do baz danych użytkownik po raz kolejny podaje login użytkownika i hasło. Dopuszczalne jest zintegrowanie loginu i hasła do stacji roboczej z loginem i hasłem serwera lub bazy danych;

7) sieć komputerową Urzędu Gminy Wejherowo zabezpieczono poprzez odseparowanie od sieci publicznej za pomocą urządzenia brzegowego UTM z zaporą firewall;
8) stanowiska komputerowe wyposażono w indywidualną licencjonowaną ochronę antywirusową;
9) konfiguracja systemu umożliwia użytkownikom końcowym dostęp do danych osobowych przechowywanych w systemie informatycznym wyłącznie za pośrednictwem używanych aplikacji;
10) komputery zabezpieczono przed możliwością użytkowania przez osoby nieuprawnione do przetwarzania danych osobowych, za pomocą indywidualnego identyfikatora użytkowania zabezpieczonego hasłem. W tym zakresie stosuje się następujące procedury:
    a) stosuje się indywidualne identyfikatory i hasła użytkowników (identyfikatory użytkowników należy wpisać do ewidencji osób upoważnionych do przetwarzania danych osobowych),
    b) zobowiązuje się użytkowników do zmiany haseł zgodnie z wytycznymi zawartymi w niniejszym dokumencie oraz do zachowania haseł w tajemnicy,
    c) pilnuje się aby dostęp do danych osobowych przetwarzanych w systemie był możliwy wyłącznie po podaniu identyfikatora i właściwego hasła,
    e) pilnuje się, aby identyfikatory osób, które utraciły uprawnienia do przetwarzania danych osobowych zastały natychmiast wyrejestrowane, a ich hasła unieważnione,
11) zastosowano wygaszenie ekranu przy dłuższej nieaktywności użytkownika;
12) użytkownik został zobowiązany do zmiany hasła co najmniej raz na 3 miesiące;

13) centrum przetwarzania danych w systemach informatycznych (komputer centralny, serwerownia) objęte są kontrolą dostępu. Kontroli dostępu dokonują Informatycy Urzędu, których pomieszczenie poprzedza pomieszczenie serwerowni.

Rozdział 2
Nadawanie uprawnień do przetwarzania danych oraz ich rejestrowanie w systemie informatycznym

§21

1. Podstawą do nadania uprawnień do przetwarzania danych osobowych w systemie informatycznym Urzędu jest upoważnienie do przetwarzania danych osobowych nadane zgodnie z postanowieniami § 12.
2. Uprawnienia dostępu do systemu informatycznego nadawane są na wniosek osób wskazanych w § 12 ust. 2. Wniosek kierowany jest do Inspektora Ochrony Danych, a w przypadku jego nieobecności bezpośrednio do Administratora Danych Osobowych i może być połączony z wnioskiem o nadanie upoważnienia do przetwarzania danych w zbiorach przetwarzanych w formie tradycyjnej (papierowej). Wniosek o nadanie upoważnienia do przetwarzania danych w systemach informatycznych powinien zawierać szczegółową nazwę systemu, do którego upoważniony ma mieć dostęp.
3. Inspektor Ochrony Danych po przygotowaniu upoważnienia przekazuje je Administratorowi Danych Osobowych do podpisu.
4. Osobą odpowiedzialną za nadawanie uprawnień do przetwarzania danych w systemach informatycznych jest Administrator Danych Osobowych, Inspektor Ochrony Danych oraz Administrator Systemu Informatycznego.
5. Użytkownikiem systemu informatycznego może być jedynie osoba posiadająca odpowiednie upoważnienie.
6. Administrator danych osobowych prowadzi Rejestr użytkowników systemu w ramach rejestru upoważnień.
7. Nadzór nad prowadzeniem rejestru, o którym mowa w ust. 6 sprawuje Inspektor Ochrony Danych.
8. Każdy zarejestrowany użytkownik korzysta z przydzielonego mu konta użytkownika, opatrzonego identyfikatorem i hasłem dostępu.
9. Nadawanie identyfikatorów i przydzielanie haseł:
   1) hasło składa się z co najmniej 10 znaków, zawiera małe i wielkie litery oraz cyfry lub znaki specjalne;
   2) pierwsze hasło może nadać Informatyk Urzędu. Musi być ono zmienione przez użytkownika po pierwszym zalogowaniu;
   3) zmiana hasła powinna być wykonywana przez każdego użytkownika do każdego systemu nie rzadziej niż co 3 miesiące, obowiązek zmiany hasła dotyczy również stacji roboczej (systemu operacyjnego);
   4) identyfikator użytkownika powinien być inny dla każdego użytkownika, a po jego wyrejestrowaniu z systemu informatycznego, nie powinien być przydzielany innej osobie;
   5) identyfikator użytkownika (login) składa się z pierwszej litery imienia oraz nazwiska. W przypadku nazwisk dwuczłonowych identyfikator składa się z pierwszej litery imienia oraz pierwszego członu nazwiska. Dopuszczalne jest stosowanie loginów w innej konfiguracji, której brzmienie umożliwiać będzie identyfikację danego pracownika;

6) identyfikatory użytkowników ujawnione są w rejestrze osób upoważnionych do przetwarzaniu danych osobowych;
7) hasła pozostają tajne, każdy użytkownik jest zobowiązany do zachowania w tajemnicy swego hasła, także po jego zmianie;
8) obowiązek ten rozciąga się także na okres po upływie ważności hasła;
9) hasło, co do którego zaistniało choćby podejrzenie ujawnienia powinno być niezwłocznie zmienione przez użytkownika;
10) utrata upoważnienia do przetwarzania danych osobowych, powoduje natychmiastowe zablokowanie konta użytkownika systemu informatycznego;
11) w przypadku konieczności skorzystania z dokumentów znajdujących się na stacji roboczej (w systemie operacyjnym) osoby nieobecnej lub, której konto zostało zablokowane kierownik referatu lub osoba zajmujące samodzielne stanowisko występuje z wnioskiem do Administratora Systemów Informatycznych o udzielenie dostępu do dokumentacji. Warunkiem udzielenia dostępu jest posiadanie upoważnienia do przetwarzania danych w zakresie odpowiedniego zbioru lub czynności.

10. Inspektor Ochrony Danych:
1) w przypadku gdy dana osoba otrzymuje po raz pierwszy upoważnienie do przetwarzania danych osobowych – informuje ją o obowiązkach związanych z zapewnieniem ochrony danych osobowych;
2) odbiera od powyższej osoby podpis pod upoważnieniem do przetwarzania danych osobowych i oświadczeniem o zapoznaniu się z obowiązującymi zasadami ochrony danych osobowych.

Rozdział 3
Procedura modyfikacji bądź odbierania uprawnień do przetwarzania danych w systemie informatycznym

§23

1. Po wygaśnięciu stosunku pracy, upoważnienie pracownika do systemu informatycznego, w którym przetwarzane są dane osobowe lub do stacji roboczej zostaje unieważnione. Brak jest konieczności występowania z wnioskiem o unieważnienie upoważnienia. Podstawę zablokowania dostępu do systemów informatycznych stanowi informacja przekazana przez Kierownika Referatu Organizacyjnego i Kadr lub Inspektora Ochrony Danych Osobowych. Za zablokowanie dostępu do systemów informatycznych urzędu odpowiedzialny jest Inspektor Ochrony Danych Osobowych oraz Administrator Systemów Informatycznych lub wyznaczony przez niego Informatyk urzędu.

2. W przypadku wystąpienia długotrwałego zwolnienia lekarskiego (powyżej 30 dni), urlopu bezpłatnego, urlopu macierzyńskiego, urlopu wychowawczego dostęp pracownika do systemu informatycznego, w którym przetwarzane są dane osobowe lub do stacji roboczej zostaje czasowo zawieszony.

3. Podstawę zawieszenia dostępu do systemów informatycznych stanowi informacja przekazana przez Kierownika Referatu Organizacyjnego i Kadr lub Inspektora Ochrony Danych Osobowych. Za zawieszenie dostępu do systemów informatycznych urzędu odpowiedzialny jest Inspektor Ochrony Danych Osobowych oraz Administrator Systemów Informatycznych lub wyznaczony przez niego Informatyk urzędu.

4. Z wnioskiem o czasowe zawieszenie uprawnień występują odpowiednio osoby wskazane w § 12 ust. 2 Polityki Bezpieczeństwa Informacji. Wniosek kierowany jest do Inspektora Ochrony Danych, a w przypadku jego nieobecności bezpośrednio do Administratora Danych Osobowych.
5. W przypadkach, o których mowa w ust. 3, po powrocie pracownika do pracy, w sytuacji zmiany stanowiska, które powoduje zmianę zakresu obowiązków konieczne jest nadanie nowego upoważnienia do przetwarzania danych osobowych.
6. W przypadku konieczności zmiany zakresu upoważnienia – w związku ze zmianą zakresu obowiązków służbowych pracownika dostęp do systemu informatycznego, w którym przetwarzane są dane osobowe zostaje odpowiednio zmodyfikowany. W takim przypadku stosuje się odpowiednio zapisy dotyczące nadawania upoważnień. Nadanie nowego upoważnienia z zapisem, że poprzednio nadane traci moc powoduje brak konieczności występowania z wnioskiem o unieważnienie poprzednio nadanego upoważnienia.

7. Inspektor Ochrony Danych po przygotowaniu odpowiedniego dokumentu przekazuje dokument Administratorowi Danych Osobowych do podpisu.

8. Osobami odpowiedzialnymi za unieważnienie lub czasowe zawieszenie uprawnień do przetwarzania danych w systemach informatycznych są Administrator Danych Osobowych, Inspektor Ochrony Danych oraz Administrator Systemów Informatycznych lub wyznaczony przez niego Informatyk Urzędu.

9. Wzór wniosku o unieważnienie lub czasowe zawieszenie uprawnień do systemu informatycznego stanowi zał. nr 12 do niniejszej Polityki.

10. Wzór unieważnienia lub czasowego zawieszenia uprawnień do systemu informatycznego stanowi zał. nr 13 do niniejszej Polityki.

Rozdział 4
Procedury rozpoczęcia, zawieszenia i zakończenia pracy w systemie informatycznym

§ 24

1. Rozpoczynając pracę w systemie informatycznym przetwarzającym dane osobowe użytkownik:
   1) uruchamia stację roboczą;
   2) wprowadza niezbędne do pracy identyfikatory i hasła w sposób uniemożliwiający ich ujawnienie osobom postronnym;
   3) sprawdza prawidłowość funkcjonowania sprzętu komputerowego i systemów, na swoim stanowisku pracy;

   4) w przypadku niestandardowego zachowania aplikacji przetwarzającej dane osobowe użytkownik natychmiast powiadamia o zaistniałym fakcie Inspektora Ochrony Danych lub Administratora Systemów Informatycznych;

   5) w razie stwierdzenia naruszenia zabezpieczenia systemu informatycznego lub stanu wskazującego na istnienie takiej możliwości, jest zobowiązany do podjęcia odpowiednich kroków stosownie do zasad postępowania w sytuacji naruszenia zabezpieczenia danych osobowych opisanych w Instrukcji postępowania w przypadku stwierdzenia naruszenia ochrony danych osobowych.

2. Przerywając pracę w systemie informatycznym użytkownik powinien co najmniej: aktywować wygaszasz ekranu lub w inny sposób zablokować możliwość korzystania ze swego konta użytkownika przez inne osoby. Zalecane jest w takich przypadkach:
   1) skorzystanie z mechanizmu czasowej blokady dostępu do komputera poprzez uruchomienie wygaszacza ekranu z hasłem;
   2) zakończenie pracy w systemie informatycznym – wylogowanie się z systemu.
3. Kończąc pracę w systemie informatycznym, użytkownik:
   1) wylogowuje się ze wszystkich aplikacji, z których korzystał;
   2) wyłącza stację roboczą za wyjątkiem sytuacji serwisowych;
   3) zabezpiecza nośniki informacji oraz wydruki z danymi osobowymi, które nie są przeznaczone do udostępnienia w warunkach uniemożliwiających dostęp do nich osobom nieuprawnionym;
   4) zamyka szafy, w których przechowuje się nośniki, na których utrwalone są dane osobowe oraz wydruki z danymi osobowymi;
   5) gdy jest ostatnią osobą opuszczającą pomieszczenie, sprawdza zamknięcie okien oraz zamyka na klucz drzwi do pomieszczenia.

Rozdział 5
Kopie bezpieczeństwa

§ 25

1. Urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, zasilane energią elektryczną, powinny być w miarę możliwości zabezpieczone przed utratą tych danych wskutek awarii zasilania lub zakłóceń w sieci zasilającej.

2. Kopia zapasowa jest tworzona każdego dnia na serwerach NAS (RAID 5) zlokalizowanych w budynku Urzędu, w pomieszczeniu serwerowni. W razie potrzeby możliwe jest utworzenie dodatkowych kopii na innych nośnikach zewnętrznych.

3. Za tworzenie i przechowywanie kopii zapasowych odpowiedzialny jest Administrator Systemów Informatycznych lub wyznaczony przez niego Informatyk Urzędu.

§ 26

1. Tworzone kopie bezpieczeństwa powinny być opisane w sposób pozwalający na określenie ich zawartości, daty utworzenia kopii oraz nazwy systemu.
2. Jeśli to możliwe, kopie bezpieczeństwa nie powinny być przechowywane w tych samych pomieszczeniach, w których przechowywane są zbiory danych osobowych eksploatowane na bieżąco.
3. Kopie bezpieczeństwa, tworzone na innych urządzeniach niż NAS (RAID 5) powinny być przechowywane w sejfie lub w przypadku braku takiej możliwości w zamkniętych szafach, znajdujących się w pomieszczeniach, które również są zamykane na klucz.
4. Kopie bezpieczeństwa należy okresowo sprawdzać pod kątem ich dalszej przydatności do odtworzenia danych w przypadku awarii systemu oraz bezzwłocznie usuwać po ustaniu ich użyteczności.
5. Kopie bezpieczeństwa, które uległy uszkodzeniu lub stały się niepotrzebne pozbawia się zapisu danych w sposób uniemożliwiający ich odtworzenie.

6. Jeżeli pozbawienie zapisu nie jest możliwe, kopie są niszczone w sposób uniemożliwiający odczytanie bądź odtworzenie danych zawartych na nośniku kopii.
7. Za realizację działań odtworzeniowych w przypadku konieczności podjęcia takich działań w związku z awarią systemu informatycznego Urzędu odpowiedzialny jest Administrator Systemów Informatycznych lub wyznaczony przez niego Informatyk Urzędu. Po odtworzeniu systemu informatycznego Administrator Systemów Informatycznych lub wyznaczony przez niego Informatyk Urzędu odpowiedzialny jest za przeprowadzenie testów poprawności działania systemu przed jego oddaniem do użytkowania.

Rozdział 6
Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz zasady ich likwidacji

§ 27

1. Dane osobowe przechowywane są w postaci elektronicznej na:
   1) nośnikach elektronicznych, wbudowanych w sprzęt informatyczny lub stanowiących element tego systemu,
   2) przenośnych nośnikach elektronicznych.
2. Do miejsca przechowywania nośników informacji i kopii zapasowych dostęp mają tylko osoby upoważnione.

3. Dane przechowywane są na nośnikach przenośnych jedynie w przypadkach, gdy jest to konieczne przez czas niezbędny do spełnienia celu, w jakim zostały one na nośniku zapisane. Po ustaniu czasu przechowywania zawartość nośnika podlega skasowaniu przy użyciu narzędzi zaakceptowanych do użycia w Urzędzie, a w przypadku nośników optycznych stosuje się niszczenie w niszczarkach umożliwiających niszczenie tego typu dokumentów.

4. Przenośne elektroniczne nośniki informacji zawierające dane osobowe są przechowywane przez pracowników w sposób minimalizujący ryzyko ich uszkodzenia lub zniszczenia, w szczególności w zamykanych szafach i meblach biurowych.

5. Likwidacja wydruków z systemu, zawierających dane osobowe odbywa się za pomocą niszczarki do dokumentów lub w inny sposób, trwale uniemożliwiający odczytanie danych.

6. Z urządzeń, dysków lub innych nośników informatycznych, które zostały przeznaczone do przekazania innemu podmiotowi, usuwa się zapisane na nich dane, a w sytuacjach, w których usunięcie danych nie jest możliwe zapewnia się ochronę danych osobowych poprzez odpowiednie zapisy umowne.
7. Dyski i inne informatyczne nośniki danych zawierające dane osobowe przeznaczone do likwidacji, należy pozbawić zapisu tych danych, a w przypadku, gdy nie jest to możliwe należy uszkodzić w sposób uniemożliwiający ich odczyt, a w sytuacjach, w których usunięcie danych nie jest możliwe zapewnić ochronę danych osobowych poprzez odpowiednie zapisy umowne.
8. W przypadku wycofania sprzętu komputerowego z użycia dane osobowe na nim zapisane są kasowane przy użyciu oprogramowania do bezpiecznego usuwania danych. W przypadku braku możliwości programowego usunięcia danych dysk podlega fizycznemu zniszczeniu.
9. Dopuszcza się powierzenie niszczenia nośników danych wyspecjalizowanym podmiotom zewnętrznym, przy odpowiednim zapewnieniu ochrony danych osobowych poprzez odpowiednie zapisy umowne (umowa powierzenia przetwarzania danych).

Rozdział 7
Sposób zabezpieczenia systemu informatycznego przed działalnością niebezpiecznego oprogramowania

§ 28

1. W celu zabezpieczenia systemu informatycznego przed działaniem niebezpiecznego oprogramowania zabrania się:
   1) uruchamiania jakiegokolwiek oprogramowania, które nie zostało zatwierdzone do użytku w urzędzie;
   2) samowolnego korzystania z nośników przenośnych, niewiadomego pochodzenia;
   3) używania nośników przenośnych bez ich uprzedniego przeskanowania przez program antywirusowy;
   4) otwierania poczty elektronicznej, której tytuł nie sugeruje związku z pełnionymi obowiązkami służbowymi; w razie wątpliwości należy skonsultować się z Administratorem Systemów Informatycznych lub Informatykiem Urzędu;
   5) podłączania stacji roboczych do sieci zewnętrznych.

2. W przypadku odnotowania objawów mogących wskazywać na obecność niebezpiecznego oprogramowania użytkownik jest zobowiązany powiadomić Administratora Systemów Informatycznych lub Inspektora Ochrony Danych. Do powyższych objawów można zaliczyć:

   1) istotne spowolnienie działania systemu informatycznego;
   2) nietypowe działanie aplikacji;
   3) nietypowe komunikaty;
   4) utrata lub modyfikacja danych.
3. System informatyczny jest zabezpieczony przed działaniem niebezpiecznego oprogramowania poprzez:
   1) oprogramowanie antywirusowe;
   2) zaporę sieciową;
   3) aktualizację oprogramowania systemowego.
4. Ochrona antywirusowa jest realizowana poprzez zainstalowanie odpowiedniego licencjonowanego oprogramowania antywirusowego.
5. System informatyczny podlega bieżącej kontroli pod kątem obecności wirusów komputerowych.
6. Wykryte zagrożenia usuwa się niezwłocznie z systemu informatycznego.
7. Przed przystąpieniem do unieszkodliwienia wirusa, jeżeli jest to możliwe, należy zabezpieczyć dane zawarte w systemie przed ich utratą.
8. Osobą odpowiedzialną za działania związane z zabezpieczeniem systemu informatycznego jest Administrator Systemów Informatycznych lub wyznaczony przez niego Informatyk Urzędu.

Rozdział 8
Sposoby postępowania w zakresie komunikacji w sieci komputerowej

§ 29

1. Wszelkie pliki zawierające kopie danych osobowych zawartych w systemie, wysyłanych poza system, muszą być zabezpieczone co najmniej hasłem.

2. Nieuzasadnione kopiowanie danych z serwera na stacje robocze, bądź na nośniki informatyczne jest zabronione za wyjątkiem skierowania na pracę zdalną jeżeli takie czynności zostały przewidziane w regulaminie bądź zarządzeniu dotyczącym pracy zdalnej.

Rozdział 9
Procedura wykonywania przeglądu i konserwacji systemów oraz nośników informacji służących do przetwarzania danych osobowych.

§ 30

1. Przegląd i konserwacja sprzętu informatycznego realizowane są przez upoważnionych pracowników Urzędu oraz w miarę potrzeby przez podmioty zewnętrzne.
2. Prace serwisowe wykonywane na terenie Urzędu przez podmioty zewnętrzne podlegają bezpośredniemu nadzorowi Administratora Systemów Informatycznych.
3. Przekazanie sprzętu informatycznego do naprawy poza teren urzędu jest dopuszczane, jeżeli spełnione zostaną poniższe warunki:
   1) sprzęt przekazywany jest bez nośników zawierających dane osobowe;
   2) przekazanie sprzętu potwierdzone jest stosowną dokumentacją;
   3) zawarta zostanie umowa powierzenia przetwarzania danych osobowych jeżeli pozbawienie sprzętu nośników danych nie jest możliwe lub znacznie utrudnione.
4. Dokumentacja, o której mowa w ust. 3 pkt 2 i 3 przechowywana jest przez Administratora Systemów Informatycznych.
5. Wszelkie pozostałe prace serwisowe wykonywane przez podmioty zewnętrzne wymagają sporządzenia dokumentacji zawierającej co najmniej poniże informacje:
   1) informacje o osobie przeprowadzającej prace serwisowe oraz podmiocie, którego osoba ta jest pracownikiem;
   2) wskazanie osoby nadzorującej przebieg prac serwisowych (dotyczy sytuacji, gdy prace realizowane są w siedzibie Urzędu);
   3) przedmiot prac serwisowych wraz z oznaczeniem sprzętu, którego prace obejmują;
   4) zakres prac serwisowych i ich wynik;
   5) czas przeprowadzonych prac serwisowych.
6. Dokumentacja, o której mowa w ust. 5 przechowywana jest przez Administratora Systemów Informatycznych.

Rozdział 10
Zasady korzystania z poczty elektronicznej oraz internetu

§ 31

1. Adres indywidualny służbowej poczty elektronicznej pracownika tworzy się według wzorca: “pierwsza litera imienia, nazwisko @ugwejherowo.pl”.
2. Dopuszcza tworzenie poczty elektronicznej z użyciem stanowiska, nazwy referatu lub innego określenia odnoszącego się do przeznaczenia poczty elektronicznej według przykładowego wzorca: sekretarz@ugwejherowo.pl, zk@ugwejherowo.pl, woda@ugwejherowo.pl.
3. Adres firmowej poczty elektronicznej zostaje utworzony w domenie pocztowej, z której korzysta pracodawca.
4. Zabrania się tworzenia i używania adresów firmowej poczty elektronicznej korzystając z innych serwerów/domen niż te, z których korzysta pracodawca.
5. Administrator systemów informatyczych przekazuje pracownikowi szczegóły dotyczace pierwszego logowania.
6. Pracownik jest zobowiązany do nieujawniania hasła do firmowej poczty elektronicznej osobom trzecim.
7. Pracownik zobowiązany jest korzystać z firmowej poczty elektronicznej zgodnie z zakresem powierzonych zadań i posiadanych kompetencji.
8. Pracownik jest zobowiązany do korzystania z przyznanego adresu mailowego do prowadzenia wszelkiej korespondencji z przełożonymi, podwładnymi i innymi pracownikami jak również z petentami urzędu w uzasadnionych przypadkach.
9. W przypadku udostepniania danych osobowych poza organizację Urzędu Gminy należy wykorzystywać mechanizmy kryptograficzne (np. Spakować dane z wykorzystaniem hasła za pomocą programów takich jak: 7-zip, Winrar lub innych) a hasło przekazać innym kanałem komunikacji, np. w kolejnej wiadomości mailowej lub telefonicznie.
10. Użytkownik poczty elektronicznej zobowiązany jest zwracać szczególną uwagę na poprawność adresu odbiorcy.
11. W przypadku przesyłania wiadomości do większej liczby odbiorców zewnętrznych użytkownik zobowiązny jest stosować pole UDW (kopia ukryta).
12. W przypadku korzystania z poczty elektronicznej użytkownik zobowiązany jest zwracać szczególną uwagę na otrzymywane załączniki dołączane do wiadomości. Zabronione jest otwieranie załączników i wiadomości poczty elektronicznej od “niezufanych” nadawców. W przypadku wątpliwśći użytkownik powinien skontaktować się z Administratorem Systemów Informatycznych.
13. Zabronione jest wykorzystywanie poczty elektronicznej do przesyłania spamu oraz używanie kont służbowych do korespondencji prywatnej.
14. Pracodawca ma prawo do kontroli przestrzegania przez użytkownika zasad korzystania z firmowej poczty elektronicznej.
15. Podczas korzystania z sieci Internet użytkownik powinien zachować szczególną ostrożność zwłaszcza w sytuacji

DZIAŁ IV
Postanowienia końcowe

§ 32

1. Polityka Bezpieczeństwa Informacji jest dokumentem wewnętrznym i nie może być udostępniona osobom postronnym w jakiejkolwiek formie.
2. Wszyscy pracownicy oraz osoby upoważnione do przetwarzania danych zobowiązani są do zapoznania się z niniejszym dokumentem oraz do stosowania zawartych w nim reguł.
3. Naruszenie niniejszej Instrukcji może zostać potraktowane jako naruszenie obowiązków pracowniczych i powodować określoną przepisami Kodeksu Pracy, Kodeksu Cywilnego i Kodeksu Karnego odpowiedzialność pracownika.
4. W sprawach nieuregulowanych w niniejszym dokumencie mają zastosowanie przepisy Rozporządzenia oraz ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych.
5. Dokumentem powiązanym z niniejszą Polityką jest Instrukcja postępowania w przypadku naruszenia ochrony danych osobowych, Instrukcja zabezpieczenia pomieszczeń Urzędu Gminy Wejherowo oraz postępowania z kluczami, a także inne regulaminy odnoszące się do zasad ochrony bezpieczeństwa wprowadzone przez Administratora.

UPOWAŻNIENIE DLA INSPEKTORA OCHRONY DANYCH

Administratorzy Danych Osobowych dnia .....
powołują na podstawie art. 37 ust. Rozporządzenia Ogólnego PE i Rady UE o ochronie danych osobowych - **Inspektora Ochrony Danych w osobie …….**
i jednocześnie nadają upoważnienie do przetwarzania danych w zbiorach danych osobowych prowadzonych przez Administratorów. Upoważnienie jest ważne od chwili podpisania przez strony do dnia odwołania Inspektora Ochrony Danych przez Administratora Danych Osobowych.

Do zadań Inspektora Ochrony Danych należy:
1) informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;
2) monitorowanie przestrzegania niniejszego rozporządzenia, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
3) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35;
4) współpraca z organem nadzorczym;
5) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.

Administrator Danych zapewnia środki i organizacyjną odrębność Inspektora Ochrony Danych, niezbędne do należytego wykonywania przez niego zadań wynikających z niniejszego upoważnienia i przepisów ustawy.

Administratorzy Danych Osobowych:	
Wójt Gminy Wejherowo	
Urząd Gminy Wejherowo	
Przewodniczący Rady Gminy Wejherowo	

OŚWIADCZENIE IOD

Oświadczam, że zapoznałem/am się z treścią i obowiązkami wynikającymi z tego upoważnienia oraz że jako Inspektor Ochrony Danych będę nadzorował/a przestrzeganie zasad ochrony danych zgodnie z obowiązkami wynikającymi z zapisów Polityki Bezpieczeństwa Informacji i Ochrony Danych obowiązującej w Urzędzie, Instrukcji zabezpieczenia pomieszczeń oraz postępowania z kluczami, Instrukcji postępowania w przypadku naruszenia zasad ochrony danych, ustawy o ochronie danych osobowych oraz Rozporządzenia w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r.

Oświadczam, że posiadam odpowiednią wiedzę z zakresu ochrony danych osobowych.

Inspektor Ochrony Danych	

UPOWAŻNIENIE DLA ZASTĘPCY INSPEKTORA OCHRONY DANYCH

Administratorzy Danych Osobowych na podstawie art. 11a ust. 1 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. poz. 1000 z późn. zm.) w zw. z art. 37 ust. 5 i 6 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia ……. r powołują:

Zastępcę Inspektora Ochrony Danych w osobie – ……..

i jednocześnie nadaje upoważnienie do przetwarzana danych w zbiorach danych osobowych prowadzonych przez administratora danych przetwarzanych zarówno w formie tradycyjnej jak i przetwarzanych w systemach informatycznych.
Upoważnienie jest ważne od chwili podpisania przez strony do dnia odwołania zastępcy Inspektora Ochrony Danych przez Administratora Danych Osobowych.
Do zadań Zastępcy Inspektora Ochrony Danych należy:

1. Wykonywanie obowiązków Inspektora Ochrony Danych przez czas usprawiedliwionej nieobecności pracownika pełniącego funkcję Inspektora Ochrony Danych jego bieżących czynności;
2. Pomoc Inspektorowi Danych Osobowych przy wykonywaniu bieżących obowiązków.

Administrator Danych zapewnia środki i organizacyjną odrębność zastępcy Inspektora Ochrony Danych Osobowych niezbędną do wykonywania przez niego zadań wynikających z niniejszego upoważnienia oraz przepisów Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.

Administratorzy Danych Osobowych:	
Wójt Gminy Wejherowo	
Urząd Gminy Wejherowo	
Przewodniczący Rady Gminy Wejherowo	

OŚWIADCZENIE ZASTĘPCY INSPEKTORA OCHRONY DANYCH

Oświadczam, że zapoznałem/am się z treścią i obowiązkami wynikającymi z tego upoważnienia oraz że jako Inspektor Ochrony Danych będę nadzorował/a przestrzeganie zasad ochrony danych zgodnie z obowiązkami wynikającymi z zapisów Polityki Bezpieczeństwa Informacji i Ochrony Danych obowiązującej w Urzędzie, Instrukcji zabezpieczenia pomieszczeń oraz postępowania z kluczami, Instrukcji postępowania w przypadku naruszenia zasad ochrony danych, ustawy o ochronie danych osobowych oraz Rozporządzenia w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r.

Oświadczam, że posiadam odpowiednią wiedzę z zakresu ochrony danych osobowych.

Zastępca Inspektora Ochrony Danych	

UPOWAŻNIENIE DLA ADMINISTRATORA SYSTEMÓW INFORMATYCZNYCH

Administratorzy Danych Osobowych dnia……powołują

Administratora systemów informatycznych w osobie:……
i jednocześnie nadają mu upoważnienie do przetwarzania danych w zbiorach danych osobowych prowadzonych przez administratora danych przetwarzanych za pomocą systemów informatycznych.

Upoważnienie jest ważne od chwili podpisania przez strony do dnia odwołania systemów informatycznych przez Administratora.

ASI jest odpowiedzialny w szczególności za:

1. wdrażanie nowych systemów informatycznych,
2. nadzorowanie poprawności przetwarzania danych w systemach informatycznych,
3. bieżący monitoring i zapewnienie ciągłości działania systemu informatycznego oraz baz danych,
4. optymalizację wydajności systemu informatycznego, baz danych,
5. instalację i konfigurację sprzętu sieciowego i serwerowego,
6. instalację i konfigurację oprogramowania systemowego, sieciowego, oprogramowania bazodanowego, konfigurację i administrację oprogramowaniem systemowym, sieciowym oraz bazodanowym zabezpieczającym dane chronione przed nieupoważnionym dostępem,
7. współpracę z dostawcami usług oraz sprzętu sieciowego i serwerowego,
8. zarządzanie kopiami awaryjnymi konfiguracji oprogramowania systemowego, sieciowego,
9. zarządzanie kopiami awaryjnymi danych, w tym danych osobowych oraz zasobów umożliwiających ich przetwarzanie,
10. zarządzanie licencjami oraz procedurami ich dotyczącymi,
11. prowadzenie profilaktyki antywirusowej,
12. sprawowanie nadzoru nad zapewnieniem awaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych,
13. sprawowanie nadzoru nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są dane osobowe, zlecanymi firmom.

Administratorzy Danych Osobowych:	
Wójt Gminy Wejherowo	
Urząd Gminy Wejherowo	
Przewodniczący Rady Gminy Wejherowo	

OŚWIADCZENIE ASI

Oświadczam, że zapoznałem/am się z treścią i obowiązkami wynikającymi z tego upoważnienia oraz że jako Administrator Systemów Informatycznych będę nadzorował/a przestrzeganie zasad ochrony danych zgodnie z obowiązkami wynikającymi z zapisów Polityki Bezpieczeństwa Informacji i Ochrony Danych obowiązującej w Urzędzie, Instrukcji zabezpieczenia pomieszczeń oraz postępowania z kluczami, Instrukcji postępowania w przypadku naruszenia zasad ochrony danych, ustawy o ochronie danych osobowych oraz Rozporządzenia w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r.

Administrator Systemów Informatycznych	

Wykaz budynków i pomieszczeń

Dane osobowe przetwarzane są w następujących pomieszczeniach:

L.p.	Stanowiska organizacyjne	Nr pomieszczenia	Rodzaj zabezpieczenia
URZĄD GMINY WEJHEROWO ul. Transportowa 1, 84-200 Wejherowo **Urząd objęty jest systemem alarmowym i ochroną grupy interwencyjnej.**			
1)	**Biuro Podawcze**	1	Zamek patentowy
2)	**Referat Finansowy - Kasa**	2	Zamek patentowy
3)	**Referat Finansowy**	3	Zamek patentowy
4)	**Referat Finansowy**	4	Zamek patentowy
5)	**Referat Finansowy - Podatki**	5	Zamek patentowy
6)	**Referat Finansowy - Podatki**	6	Zamek patentowy
7)	**Inspektor Ochrony Danych**	6	Zamek patentowy
8)	**Referat Finansowy - Skarbnik**	7	Zamek patentowy
9)	**Referat Finansowy**	8	Zamek patentowy
10)	**Referat Finansowy – Audytor Wewnętrzny**	9	Zamek patentowy
11)	**Sala Narad**	11	Zamek patentowy
12)	**Informatyk, Serwerownia**	12	Kraty w oknach, zamki patentowe
13)	**Referat Gospodarki Odpadami i Środowiska**	14	Zamek patentowy
14)	**Referat Gospodarki Odpadami i Środowiska**	14A	Zamek patentowy
15)	**Referat Gospodarki Odpadami i Środowiska**	15	Zamek patentowy
16)	**Referat Gospodarki Odpadami i Środowiska**	15A	Zamek patentowy
17)	**Referat Gospodarki Odpadami i Środowiska**	16	Zamek patentowy
18)	**Referat Spraw Obywatelskich - Kierownik**	17A	Zamek patentowy

19)	**Referat Spraw Obywatelskich**	17B	Zamek patentowy
20)	**Referat Bezpieczeństwa i Zarządzania Kryzysowego**	19	Zamek patentowy
21)	**Sekretariat, Wójt, Z-ca Wójta**	20	Zamki patentowe
22)	**Sekretarz Gminy Wejherowo**	21	Zamek patentowy
23)	**Radca Prawny**	22	Zamek patentowy
24)	**Referat Organizacyjny i Kadr**	23	Zamek patentowy
25)	**Referat Organizacyjny i Kadr – Kierownik**	24	Zamek patentowy
26)	**Referat Zamówień Publicznych i Funduszy Zewnętrznych**	25	Zamek patentowy
27)	**Biuro Rady**	26	Zamek patentowy
28)	**Referat Zamówień Publicznych i Funduszy Zewnętrznych**	27	Zamek patentowy
29)	**Referat Zamówień Publicznych i Funduszy Zewnętrznych - Kierownik**	28	Zamek patentowy
30)	**Referat Inwestycji i Gospodarki Komunalnej**	29	Zamek patentowy
31)	**Referat Inwestycji i Gospodarki Komunalnej - z-ca Kierownika**	30	Zamek patentowy
32)	**Referat Inwestycji i Gospodarki Komunalnej**	31	Zamek patentowy
33)	**Referat Inwestycji i Gospodarki Komunalnej**	32	Zamek patentowy
34)	**Referat Inwestycji i Gospodarki Komunalnej - Kierownik**	34	Zamek patentowy
35)	**Referat Inwestycji i Gospodarki Komunalnej**	36	Zamek patentowy
36)	**Referat Inwestycji i Gospodarki Komunalnej**	37	Zamek patentowy
37)	**Pomieszczenie techniczne (Drukarka, skaner)**	38	Zamek patentowy
38)	**Referat Oświaty i Spraw Społecznych**	39	Zamek patentowy,
39)	**Referat Oświaty i Spraw Społecznych - Kierownik**	40	Zamek patentowy
40)	**Referat Inżynierii Środowiska**	41 A	Zamek patentowy
41)	**Referat Inżynierii Środowiska**	41 B	Zamek patentowy
42)	**Referat Inżynierii Środowiska**	41 C	Zamek patentowy

43)	**Referat Inżynierii Środowiska**	42	Zamek patentowy
44)	**Referat Gospodarki Przestrzennej i nieruchomości**	43	Zamek patentowy
45)	**Referat Oświaty i Spraw Społecznych – Za-ca Kierownika**	44	Zamek patentowy
46)	**Referat Gospodarki Przestrzennej i nieruchomości**	46	Zamek patentowy
47)	**Referat Gospodarki Przestrzennej i nieruchomości**	47	Zamek patentowy
48)	**Referat Gospodarki Przestrzennej i nieruchomości – za-ca kierownika**	48	Zamek patentowy
49)	**Referat Gospodarki Przestrzennej i nieruchomości - kierownik**	50	Zamek patentowy

ul. Leśna 35, 84-239 Bolszewo (budynek Szkoły Podstawowej im. Mikołaja Kopernika)			
50)	Archiwum	-	System alarmowy, monitoring wizyjny, zamek patentowy, potrójne drzwi, krata zabezpieczająca

HALA WIDOWISKOWO-SPORTOWA **ul. Leśna 35 A, 84-239 Bolszewo**			
51)	**Referat Oświaty i Spraw Społecznych**	**266**	**Zamek patentowy, monitoring wizyjny, grupa interwencyjna**

REJESTR CZYNNOŚCI PRZETWARZANIA											
Administrator: **Dane kontaktowe:** **Dane inspektora ochrony danych:** **Dane zastępcy inspektora ochrony danych:**											
Lp.	**Nazwa czynności przetwarzania**	**Nazwa zbioru danych**	**cel przetwarzania**	**nazwa systemu lub oprogramowania**	**podstawa prawna**	**źródło danych**	**Kategorie danych**	**Opis kategorii osób, których dane dotyczą**	**Kategorie odbiorców, którym dane zostały lub zostaną ujawnione**	**Planowane terminy usunięcia poszczególnych kategorii danych**	**Opis środków bezpieczeństwa**
1.											

*dopuszcza się prowadzenie dokumentu w formie elektronicznej

REJESTR WSZYSTKICH KATEGORII CZYNNOŚCI PRZETWARZANIA						
Nazwa podmiotu przetwarzającego: **Dane kontaktowe:** **Dane inspektora ochrony danych:** **Dane zastępcy inspektora ochrony danych:**						
L.P.	**Nazwa czynności przetwarzania**	**Imię i nazwisko lub nazwa administratora, w imieniu którego działa podmiot przetwarzający**	**Kategoria przetwarzań**	**Przekazywanie danych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji oraz stosowane zabezpieczenia**	**Podstawa przetwarzania**	**Opis technicznych i organizacyjnych środków bezpieczeństwa**
1.						

*dopuszcza się prowadzenie dokumentu w formie elektronicznej

Potwierdzenie uczestnictwa w szkoleniu z zakresu ochrony danych osobowych z uwzględnieniem przepisów RODO

Ja, niżej podpisana/y……
(imię, nazwisko, stanowisko służbowe)
oświadczam niniejszym, że dnia……uczestniczyłam/em w szkoleniu dotyczącym zasad przetwarzania i ochrony danych osobowych obowiązujących w Urzędzie Gminy Wejherowo, (ul. Transportowa 1, 84-200 Wejherowo) z uwzględnieniem przepisów Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), które przeprowadzone zostało przez ……..

Oświadczam jednocześnie, iż zasady przetwarzania danych osobowych oraz sposób postępowania w przypadku stwierdzenia naruszenia przedstawione zarówno w trakcie szkolenia jak i wynikające z Polityki Bezpieczeństwa Informacji i Ochrony Danych Osobowych, Instrukcji zabezpieczenia pomieszczeń Urzędu Gminy oraz postępowania z kluczami, są dla mnie zrozumiałe i zobowiązuję się do ich przestrzegania.

Podpis osoby biorącej udział w szkoleniu:	
Podpis osoby przeprowadzającej szkolenie:	

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH NR……

Na podstawie art. 29 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (zwanego dalej RODO), dnia……..upoważniam:

IMIĘ I NAZWISKO OSOBY UPOWAŻNIONEJ

ZAKRES UPOWAŻNIENIA DO PRZETWARZANIA DANYCH OSOBOWYCH	Upoważnienie	
	TAK	NIE
Do przetwarzania danych osobowych w dowolnej formie, w zakresie realizowanych czynności (zakresu obowiązków) w celach związanych z wykonywaniem obowiązków służbowych.	☐	☐
Na podstawie art. 22^{1b} **ustawy z dnia 26 czerwca 1974 r. – Kodeks pracy**, upoważniam do przetwarzania danych osobowych, o których mowa w art. 9 ust. 1 RODO tj. danych szczególnych kategorii, w dowolnej formie, w zakresie realizowanych czynności.	☐	☐
Na podstawie art. 8, ust 1b ustawy z dnia 4 marca 1994 r. **o zakładowym funduszu świadczeń socjalnych**, upoważniam do przetwarzania danych osobowych dotyczących zdrowia, o których mowa w art. 9 ust. 1 RODO, w dowolnej formie, w zakresie realizacji zadań wynikających z Regulaminu Zakładowego Funduszu Świadczeń Socjalnych.	☐	☐
Na podstawie art. 2b, ust 6 **ustawy z dnia 27 sierpnia 1997 r. o rehabilitacji zawodowej i społecznej oraz zatrudnianiu osób niepełnosprawnych**, upoważniam do przetwarzania danych osobowych, których przetwarzanie wynika z ww. ustawy, w dowolnej formie, w zakresie realizowanych czynności.	☐	☐

Na podstawie **art. 8a ustawy z dnia 27 marca 2003 r. o planowaniu i zagospodarowaniu przestrzennym,** upoważnienie ma obejmować przetwarzanie danych osobowych, których przetwarzanie wynika z ww. ustawy, w dowolnej formie, w zakresie realizowanych czynności.	☐	☐

Nazwa systemów informatycznych, do których upoważniony otrzymuje dostęp:

Z dniem …… r. nadaje się identyfikator do pracy w systemie informatycznym: **……**

Upoważnienie nadaje się na okres zatrudnienia.

OŚWIADCZENIE UPOWAŻNIONEGO

Ja niżej podpisany/a, oświadczam, że zostałem/am zaznajomiony/a z przepisami dotyczącymi ochrony danych osobowych zapisanymi w Polityce Bezpieczeństwa Informacji i Ochrony Danych Osobowych, Instrukcji zabezpieczenia pomieszczeń Urzędu Gminy Wejherowo oraz postepowania z kluczami, Instrukcji postępowania w przypadku naruszenia ochrony danych osobowych obowiązującymi w Urzędzie Gminy Wejherowo i zobowiązuję się do ich przestrzegania.

Jednocześnie oświadczam że :

- Zobowiązuję się do zachowania w tajemnicy danych osobowych, do których mam lub będę miał/a dostęp w związku z wykonywaniem powierzonych zadań i obowiązków, zarówno w trakcie ich wykonywania jak i po zakończeniu stosunku prawnego, na podstawie którego nadane zostało upoważnienie.
- Zapewnię ochronę danym przetwarzanym, a w szczególności zabezpieczę je przed dostępem osób nieupoważnionych, zabraniem, uszkodzeniem oraz nieuzasadnioną modyfikacją lub zniszczeniem.
- Natychmiast zgłoszę stwierdzenie próby lub faktu naruszenia zasad ochrony danych osobowych lub bezpieczeństwa systemu informatycznego, w którym przetwarzane są dane osobowe, a nadto będę postępował zgodnie z Instrukcją postępowania w przypadku naruszenia zasad ochrony danych osobowych.
- Przyjmuję do wiążącej wiadomości, iż postępowanie rażąco sprzeczne z wyżej wskazanymi obowiązkami, przepisami prawa oraz wewnętrznymi regulacjami może być uznane za ciężkie naruszenie obowiązków pracowniczych.
- Jestem świadomy, że naruszenie zasad dotyczących przetwarzania danych osobowych może skutkować odpowiedzialnością administracyjną, cywilnoprawną oraz karną.

Administrator Danych Osobowych — Upoważniony do przetwarzania danych

…… …….

1. Pan/i ……..
2. Kierownik Referatu Organizacyjnego i Kadr
3. a/a

Załącznik nr 9
do Polityki Bezpieczeństwa Informacji i Ochrony Danych Osobowych
w Urzędzie Gminy Wejherowo

WNIOSEK O NADANIE UPOWAŻNIENIA DO PRZETWARZANIA DANYCH OSOBOWYCH

Wejherowo, dnia ……

Proszę o wydanie upoważnienia Pani/Panu

……

nazwisko i imię, stanowisko służbowe

……

nazwa referatu, budynek, numer pokoju

ZAKRES UPOWAŻNIENIA DO PRZETWARZANIA DANYCH OSOBOWYCH	Upoważnienie	
	TAK	NIE
Przetwarzanie danych osobowych w dowolnej formie, w zakresie realizowanych czynności (zakresu obowiązków) w celach związanych z wykonywaniem obowiązków służbowych.	☐	☐
Na podstawie art. 22^{1b} **ustawy z dnia 26 czerwca 1974 r. – Kodeks pracy**, upoważnienie obejmować ma dane osobowe, o których mowa w art. 9 ust. 1 RODO tj. danych szczególnych kategorii, w dowolnej formie, w zakresie realizowanych czynności.	☐	☐
Na podstawie art. 8, ust 1b ustawy z dnia 4 marca 1994 r. o zakładowym funduszu świadczeń socjalnych, upoważnienie obejmować ma dane osobowe dotyczące zdrowia, o których mowa w art. 9 ust. 1 RODO, w dowolnej formie, w zakresie realizacji zadań wynikających z Regulaminu Zakładowego Funduszu Świadczeń Socjalnych.	☐	☐
Na podstawie art. 2b, ust 6 **ustawy z dnia 27 sierpnia 1997 r. o rehabilitacji zawodowej i społecznej oraz zatrudnianiu osób niepełnosprawnych**, upoważnienie ma obejmować przetwarzanie danych osobowych, których	☐	☐

przetwarzanie wynika z ww. ustawy, w dowolnej formie, w zakresie realizowanych czynności.		

Na podstawie art. 8a Ustawy z dnia 27 marca 2003 r. o planowaniu i zagospodarowaniu przestrzennym, upoważnienie ma obejmować przetwarzanie danych osobowych, których przetwarzanie wynika z ww. ustawy, w dowolnej formie, w zakresie realizowanych czynności.	☐	☐

Nazwa systemów informatycznych, do których upoważniony ma otrzymać dostęp:

……

……

…….

- na okres
  - od ……. do …….
  - Bezterminowo*.

*niepotrzebne skreślić

……

EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH							
Numer upoważnienia	**Imię i nazwisko**	**Zakres upoważnienia do przetwarzania danych osobowych w systemie papierowym**	**Zakres upoważnienia do przetwarzania danych osobowych w systemie informatycznym**	**Data nadania uprawnień w systemie**	**Identyfikator**	**Aktualne stanowisko**	**Uwagi**

*dopuszcza się prowadzenie dokumentu w formie elektronicznej

OŚWIADCZENIE O ZACHOWANIU DANYCH W POUFNOŚCI

Zgodnie z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) zobowiązuję się do:

1. Ochrony przetwarzanych danych osobowych w Urzędzie Gminy Wejherowo do których mam lub będę miał/a dostęp w związku z wykonywaniem powierzonych zadań i obowiązków, zarówno w trakcie ich wykonywania jak i po zakończeniu stosunku prawnego, na podstawie którego zadania i obowiązki są wykonywane w szczególności poprzez:

   1) nieprzekazywanie danych osobowych, do których uzyskam dostęp przy okazji wykonywania obowiązków służbowych osobom nieupoważnionym;
   2) uniemożliwianie dostępu do danych osobowych osobom nieuprawnionym;
   3) niedopuszczanie do nielegalnego ujawnienia lub pozyskania danych osobowych;
   4) przestrzeganie przepisów o ochronie danych osobowych oraz zarządzeń, regulaminów i instrukcji wydanych przez Administratora Danych Osobowych dotyczących ochrony tych danych;

2. Zachowania w tajemnicy wszelkich danych osobowych, do których uzyskam dostęp przy okazji wykonywania obowiązków służbowych niezależnie od formy przekazania informacji dotyczących danych osobowych, ani ich źródła.

3. Jednocześnie oświadczam że :

   1) Natychmiast zgłoszę stwierdzenie próby lub faktu naruszenia zasad ochrony danych osobowych lub bezpieczeństwa systemu informatycznego, w którym przetwarzane są dane osobowe, a nadto będę postępował zgodnie z Instrukcją postępowania w przypadku naruszenia zasad ochrony danych osobowych.

- Przyjmuję do wiadomości, iż postępowanie rażąco sprzeczne z wyżej wskazanymi obowiązkami, przepisami prawa oraz wewnętrznymi regulacjami może być uznane za ciężkie naruszenie obowiązków pracowniczych.
- Jestem świadomy, że naruszenie zasad dotyczących przetwarzania danych osobowych może skutkować odpowiedzialnością administracyjną, cywilnoprawną oraz karną.

Imię i nazwisko	Data	Podpis

EWIDENCJA OSÓB OD KTÓRYCH ODEBRANO OŚWIADCZENIE O ZACHOWANIU DANYCH W POUFNOŚCI			
Lp.	Imię i nazwisko	Stanowisko	Data odbioru oświadczenia

- Dopuszcza się prowadzenie dokumentu w formie elektronicznej

Wniosek o udostępnienie danych ze zbioru danych osobowych

1. Wniosek do: . . . . . .

2. Wnioskodawca: . . . . . .

. . . . . .

(nazwa firmy i jej siedziba albo nazwisko, imię i adres zamieszkania wnioskodawcy)

3. Podstawa prawna upoważniająca do pozyskania danych:

. . . . . .

. . . . . .

4. Wskazanie przeznaczenia dla udostępnionych danych osobowych:

. . . . . .

. . . . . .

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

. . . . . .

. . . . . .

6. Zakres żądanych informacji ze zbioru:

. . . . . .

. . . . . .

7. Informacje umożliwiające wyszukanie w zbiorze żądanych danych osobowych:

. . . . . .

. . . . . .

(data i podpis wnioskodawcy)

WYKAZ PODMIOTÓW KTÓRYM POWIERZONO PRZETWARZANIE DANYCH		
Lp.	**Nazwa podmiotu**	**Data zawarcia umowy powierzenia**
1.		
2.		
3.		

*Dopuszcza się prowadzenie dokumentu w formie elektronicznej

WNIOSEK O UNIEWAŻNIENIE/CZASOWE ZAWIESZENIE/MODYFIKACJĘ UPOWAŻNIENIA DO PRZETWARZANIA DANYCH OSOBOWYCH

Wejherowo, dnia ……

Zwracam się z wnioskiem o unieważnienie/czasowe zawieszenie/modyfikację* upoważnienia do przetwarzania danych osobowych Pani/Panu

……

nazwisko i imię, stanowisko służbowe

……

nazwa referatu, budynek, numer pokoju

z powodu:

……..

……

……

Systemy informatyczne, których wniosek dotyczy:

……

……

- na okres
  - od ……. do …….
  - Bezterminowo*.

*niepotrzebne skreślić

…….

Podpis sekretarza/kierownika referatu/pracownika

UNIEWŻNIENIE/CZASOWE ZAWIESZENIE* UPRAWNIEŃ DO PRZETWARZANIA DANYCH OSOBOWYCH W SYSTEMACH INFORMATYCZNYCH

Dnia ……..**,** unieważnia się/czasowo zawiesza się* upoważnienie nr……. do przetwarzania danych osobowych nadane dnia……... Pani/Panu……

Unieważnienie/czasowe zawieszenie* obejmuje następujące systemy informatyczne:

- identyfikator do pracy w systemie informatycznym służącym do przetwarzania danych osobowych: ……

Czasowe zawieszenie obejmuje okres od……..do……..

*niepotrzebne skreślić

Administrator Danych Osobowych

…….

1. a/a

Załącznik Nr 2 do zarządzenia Nr 122/2021
Wójta Gminy Wejherowo
z dnia 31 sierpnia 2021 r.

INSTRUKCJA POSTĘPOWANIA
W PRZYPADKU NARUSZENIA ZASAD OCHRONY DANYCH OSOBOWYCH

URZĄD GMINY WEJHEROWO

Data	Wersja	Opis zmiany	Autor
18.05.2018 r.	1.0	Stworzenie dokumentu	Podmiot zewnętrzny MBM
19.03.2019 r.	2.0.	Aktualizacja dokumentu	Inspektor Ochrony Danych
31.08.2021 r.	3.0.	Aktualizacja dokumentu	Inspektor Ochrony Danych

Dokument przygotował

Imię i nazwisko	Stanowisko	Podpis
Monika Wegner	Inspektor Ochrony Danych	
Jarosław Domarus	Starszy Informatyk – Administrator Systemów Informatycznych	

Dokument zatwierdził

Data	Podpis
Wójt Gminy Wejherowo	
Przewodniczący Rady Gminy	

ROZDZIAŁ 1
Postanowienia ogólne

§ 1

Celem **Instrukcji postępowania w sytuacji naruszenia ochrony danych osobowych** zwaną dalej „Instrukcją", jest aktywna kontrola nad przypadkami naruszeń i podejrzeniami naruszeń w celu zapewnienia poufności, integralności, rozliczalności i ciągłości przetwarzanych danych osobowych. Przestrzeganie postanowień niniejszej Instrukcji służyć ma wykrywaniu i właściwemu reagowaniu na przypadki naruszenia ochrony danych osobowych.

§ 2

1. Osobą sprawującą nadzór nad przestrzeganiem zasad ochrony danych osobowych oraz odpowiedzialną za nadzorowanie przypadków naruszeń jest Inspektor Ochrony Danych.
2. Osobą sprawującą nadzór nad przetwarzaniem danych w systemach informatycznych oraz sprawującą kontrolę i ocenę funkcjonowania mechanizmów technicznych zabezpieczeń systemów informatycznych służących do przetwarzania danych jest Administrator Systemów Informatycznych we współpracy z Inspektorem Ochrony Danych**.**

ROZDZIAŁ 2
Definicje

§ 3

Przez użyte w Instrukcji określenia należy rozumieć:

1. **Administrator danych osobowych (ADO) –** oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych.
2. **Rozporządzenie** – rozporządzenie Parlamentu Europejskiego i Rady z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych osobowych) (Dz. Urz. UE L 119 z 04.05.2016 , str. 1 oraz Dz. Urz. UE L 127 z 23.05.2018, str. 2) zwana dalej także RODO;
3. **Ustawa** – ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych zwana w dalszej części ustawą.
4. **Inspektor ochrony danych –** rozumie się przez to osobę wyznaczoną przez administratora danych osobowych, posiadającą odpowiednie kwalifikacje zawodowe, wiedzę fachową na temat prawa i praktyk w dziedzinie ochrony danych osobowych oraz umiejętności wymagane do wypełniania zadań związanych z ochroną tych danych powołaną w celu informowania i doradzania Administratorowi, podmiotowi przetwarzającemu oraz pracownikom w zakresie obowiązującego prawa o ochronie

danych oraz niniejszej polityki jak również w celu monitorowania ich przestrzegania oraz działania jako punkt kontaktowy dla podmiotów przetwarzających i organu nadzorczego.

5. **Administrator systemu informatycznego -** pracownik lub podmiot zewnętrzny odpowiedzialny za prawidłową pracę systemów informatycznych, w tym utrzymanie ciągłości działania oraz bezpieczeństwa w infrastrukturze informatycznej, inwentaryzowanie, okresowe sprawdzanie stanu urządzeń oraz sprzętu pozwalającego na obsługę czynności przetwarzania danych osobowych w systemach informatycznych.
6. **Dane osobowe** – informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.
7. **Zbiór danych osobowych** – oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie.
8. **Przetwarzanie danych –** oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.
9. **Podmiot przetwarzający** - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora.
10. **Odbiorca** - osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania.
11. **Osoba upoważniona do przetwarzania danych osobowych lub użytkownik** – każda osoba świadcząca na rzecz Administratora pracę lub usługi w oparciu o jakikolwiek stosunek prawny, jeżeli to świadczenie pracy lub usług wiąże się z przetwarzaniem danych osobowych, posiadająca imienne upoważnienie do przetwarzania danych osobowych wydane przez Administratora, określające imię i nazwisko osoby upoważnionej, datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych, a także identyfikator jeżeli dane są przetwarzane w systemie informatycznym.
12. **Zabezpieczenie danych** – zabezpieczenie danych poprzez wdrożenie i eksploatację środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem.

13. **Naruszenie ochrony danych osobowych** – naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.
14. **System informatyczny** – zespół współpracujących ze sobą urządzeń, programów oraz narzędzi programowych zastosowanych w celu przetwarzania danych.
15. **Elektroniczny nośnik danych** – materiał lub urządzenie służące do zapisywania, przechowywania lub odczytywania danych osobowych w postaci cyfrowej lub analogowej.
16. **System tradycyjny** – rozumie się przez to zespół procedur organizacyjnych, związanych z mechanicznym przewarzaniem informacji oraz wyposażenia i środków trwałych w celu przetwarzania danych osobowych na papierze.
17. **Sieć lokalna** – połączenie systemów informatycznych administratora wyłącznie dla jego własnych potrzeb przy wykorzystaniu urządzeń i sieci telekomunikacyjnych.
18. **Identyfikator** – ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący użytkownika upoważnionego do przetwarzania danych w systemie informatycznym.
19. **Hasło** – ciąg znaków literowych, cyfrowych lub innych, znany jedynie Administratorowi oraz Użytkownikowi upoważnionemu do Przetwarzania Danych w Systemie informatycznym.
20. **Uwierzytelnianie** – proces, którego celem jest weryfikacja tożsamości deklarowanej przez Użytkownika.
21. **Pomieszczenia** – rozumie się przez to budynki, pomieszczenia lub części pomieszczeń określone przez Administratora Danych tworzące obszar, w którym przetwarzane są dane osobowe z użyciem stacjonarnego lub mobilnego sprzętu komputerowego oraz w systemie tradycyjnym.
22. **Uchybienie** - świadome lub nieświadome działania zmierzające do zagrożenia wskutek, których może dojść do utraty danych osobowych, kradzieży danych osobowych lub uszkodzenia nośników danych.
23. **Zagrożenie** - świadome lub nieświadome działania wskutek, których doszło do utraty danych osobowych, kradzieży danych osobowych lub uszkodzenia nośników danych.
24. **Poufność danych –** właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym osobom.
25. **Integralność danych –** właściwość zapewniająca, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
26. **Rozliczalność danych –** właściwość zapewniająca, że działania osoby mogą być przypisane w sposób jednoznaczny tylko tej osobie.
27. **Integralność systemu –** rozumiana jest jako nienaruszalność systemu, niemożność jakiejkolwiek manipulacji, zarówno zamierzonej, jak i przypadkowej.
28. **Dostępność informacji –** zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią zasobów wtedy, gdy jest to potrzebne.
29. **Uchybienie** - świadome lub nieświadome działania zmierzające do zagrożenia wskutek, których może dojść do utraty danych osobowych, kradzieży danych osobowych lub uszkodzenia nośników danych.

30. **Urząd –** Urząd Gminy Wejherowo z siedzibą - ul. Transportowa 1, 84-200 Wejherowo;
31. **Wójt –** Wójt Gminy Wejherowo.
32. **Rada Gminy –** Rada Gminy Wejherowo.

ROZDZIAŁ 3
Identyfikacja naruszeń

§ 4

Do głównych zagrożeń mających wpływ na bezpieczeństwo ochrony danych osobowych należy zaliczyć:

1) **zagrożenia losowe zewnętrzne** (np. klęski żywiołowe, przerwy w zasilaniu, awarie serwerów) – ich występowanie może prowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej systemu informatycznego, zostaje zakłócona ciągłość systemu, ale nie dochodzi do utraty poufności danych;
2) **zagrożenia losowe wewnętrzne** (np. niezamierzone pomyłki informatyczne, pomyłki ludzkie, awarie sprzętowe, błędy oprogramowania, pogorszenie jakości sprzętu lub oprogramowania, niewłaściwe zabezpieczenie pomieszczeń lub sprzętu) – ich występowanie może doprowadzić do zniszczenia danych, zakłócenia ciągłości pracy systemu i może dojść do naruszenia poufności danych;
3) **zagrożenia zamierzone** – (świadome i celowe działania np. włamanie do systemu - nieuprawniony dostęp do systemu z zewnątrz, działanie wirusów komputerowych - nieuprawniony dostęp do systemu z wewnątrz, udostępnienie danych osobie nieupoważnionej, kradzież sprzętu informatycznego zawierającego dane, świadome zniszczenie danych) – ich występowanie powoduje naruszenie poufności danych, ale z reguły nie powoduje uszkodzenia infrastruktury technicznej i zakłócenia ciągłości pracy.

§ 5

Naruszenie ochrony danych osobowych może być spowodowane:

1) oddziaływaniem czynników zewnętrznych, takich jak: temperatura otoczenia, wilgotność, pole elektromagnetyczne, wirusy komputerowe, skutki powodzi, pożaru, itp.;
2) niekontrolowanym działaniem osób trzecich, powodującym zakłócenia systemu podczas włamania, niewłaściwym działaniem zespołów serwisowych, przetwarzaniem danych osobowych bez uprawnień, tworzeniem w zbiorach użytkownika nieautoryzowanych kont dostępu;
3) umyślnym lub nieumyślnym działaniem, a nawet zaniechaniem działania użytkowników przetwarzających dane osobowe.

§ 6

Za naruszenie lub podejrzenie naruszenia bezpieczeństwa danych osobowych uważa się przede wszystkim:

1) losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu (wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej itp.);
2) niewłaściwe parametry środowiska (nadmierna wilgotność, wysoka temperatura, oddziaływanie pola elektromagnetycznego, wibracje lub wstrząsy wywołane urządzeniami przemysłowymi);
3) awarię sprzętu lub oprogramowania, która wyraźnie wskazuje na umyślne działanie w kierunku naruszenia danych, a także niewłaściwe działalnie serwisu, a w tym sam fakt pozostawienia serwisantów bez nadzoru;
4) pojawienie się odpowiedniego komunikatu alarmowego od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu;
5) naruszenie lub próba naruszenia integralności systemu lub bazy danych w tym systemie;
6) stwierdzenie próby modyfikacji lub modyfikację danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia;
7) ujawnienie osobom nieupoważnionym danych osobowych lub objętych tajemnicą procedur ochrony przetwarzania albo innych strzeżonych elementów systemu zabezpieczeń. Ujawnienie osobom nieuprawnionym danych osobowych obejmuje również przesłanie dokumentu lub wiadomości zawierającej dane osobowe do nieuprawnionego adresata;
8) ujawnienie istnienia nieautoryzowanych kont dostępu do systemu informatycznego służącego do przetwarzania danych osobowych;
9) podmienienie lub zniszczenie nośników z danymi osobowymi bez odpowiedniego upoważnienia lub niedozwolone skasowanie lub skopiowanie danych osobowych, w tym stosowanie nieodpowiednich technik usuwania danych;
10) naruszenie dyscypliny pracy w zakresie przestrzegania procedur bezpieczeństwa (np. niewylogowanie się z systemu przed opuszczeniem stanowiska pracy; pozostawienie otwartego pomieszczenia bez nadzoru osób upoważnionych do przetwarzania danych osobowych; brak zmiany hasła do systemów informatycznych przez okres dłuższy niż 3 miesiące; pozostawianie kluczy do pomieszczeń po zakończeniu pracy w sposób umożliwiający dostęp do kluczy przez osoby nieupoważnione do przetwarzania danych osobowych; pozostawianie na wymienniku dokumentów zawierających dane osobowe, co do których dostęp możliwy będzie także dla innych pracowników (nieupoważnionych do przetwarzania danych);
11) brak dostępu do zawartości zbioru danych – zbiór istnieje, lecz nie można go otworzyć;
12) informacja o zainfekowaniu systemu wirusami;
13) brak urządzeń systemu lub nośników informacji, na których zapisane są dane osobowe;
14) utrata możliwości fizycznego dostępu do danych (np. zagubiony klucz do pomieszczenia lub mebli biurowych);
15) próbę lub fakt nieuprawnionego dostępu do zbioru danych lub pomieszczenia, w którym jest przetwarzany np. zmiana ułożenia kolejności dokumentów, otwarte drzwi lub meble biurowe, nietypowe ustawienie sprzętu;
16) zmianę lub utratę danych zapisanych na kopiach awaryjnych lub zapisach archiwalnych.
17) nieuprawnione prace na koncie użytkownika dopuszczonego do przetwarzania danych osobowych przez osobę do tego nieuprawnioną;
18) ujawnienie indywidualnych haseł dostępu użytkowników do systemu;
19) niewykonanie kopii bezpieczeństwa w odpowiednim terminie;
20) pozostawienie bez opieki dokumentacji w miejscu dostępnym dla osób nieupoważnionych do przewarzania danych osobowych.

ROZDZIAŁ 4
Procedury postępowania w przypadku naruszeń

§ 7

1. Każdy użytkownik w przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenie systemu ochrony, o których mowa w § 6 niniejszej Instrukcji, zobowiązany jest do bezzwłocznego powiadomienia o tym fakcie Inspektora Ochrony Danych oraz Administratora Systemów Informatycznych lub Informatyka Urzędu.

2. W razie braku możliwości zawiadomienia Inspektora Ochrony Danych, należy zawiadomić bezpośredniego przełożonego, którego obowiązkiem jest zawiadomienie Administratora Danych Osobowych oraz Administratora Systemów Informatycznych lub Informatyka Urzędu.

3. Do czasu przybycia na miejsce osoby nadzorującej przypadki naruszeń użytkownik powinien:
   1) niezwłocznie podjąć czynności niezbędne do powstrzymania skutków naruszenia ochrony (o ile to jest możliwe), a następnie uwzględnić w działaniu również ustalenie przyczyn lub sprawców;
   2) rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia;
   3) zaniechać – o ile to możliwe - dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić analizę i dokumentację danego przypadku;
   4) podjąć, stosownie do zaistniałej sytuacji działania, które zapobiegną ewentualnej utracie danych osobowych;
   5) podjąć inne działania przewidziane i określone w instrukcjach technicznych i technologicznych stosownie do objawów i komunikatów towarzyszących naruszeniu;
   6) podjąć stosowne działania, jeżeli zaistniały przypadek jest określony w dokumentacji systemu operacyjnego, dokumentacji bazy danych lub aplikacji użytkowej;
   7) zastosować się do innych instrukcji i regulaminów, jeżeli odnoszą się one do zaistniałego przypadku;
   8) ustalić przyczynę i sprawcę naruszenia ochrony oraz zapisać wszelkie informacje i okoliczności związane ze zdarzeniem;
   9) nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia;
   10) zabezpieczyć dostęp do pomieszczenia lub urządzenia.

4. Dokonywanie zmian w miejscu naruszenia ochrony danych osobowych jest dopuszczalne tylko w wypadku konieczności ratowania osób, mienia albo zapobiegania powstaniu innego niebezpieczeństwa zmierzającego do dalszego naruszenia bezpieczeństwa ochrony danych.

5. W przypadku stwierdzenia przez użytkownika naruszenia bezpieczeństwa danych w systemie informatycznym należy dodatkowo:
   1) zabezpieczyć system informatyczny;
   2) zabezpieczyć technicznie stan urządzeń;
   3) zabezpieczyć zawartość zbioru danych osobowych;
   4) fizycznie odłączyć urządzenia i te segmenty sieci, które mogły umożliwić dostęp do bazy danych osobie niepowołanej;

5) wylogować użytkownika podejrzanego o naruszenie bezpieczeństwa zabezpieczenia ochrony danych;
6) w razie potrzeby zmienić hasło dla administratora.

§ 8

W przypadku uszkodzenia urządzeń służących do przetwarzania danych, utraty danych lub ich zniekształcenia, odtwarza się bazy danych osobowych z kopii bezpieczeństwa.

§ 9

1. Po przybyciu na miejsce naruszenia bezpieczeństwa danych osobowych osoba odpowiedzialna za nadzór nad naruszeniami podejmuje następujące kroki:
   1) zapoznaje się z zaistniałą sytuacją i wybiera sposób dalszego postępowania uwzględniając zagrożenie w prawidłowości pracy;
   2) może żądać dokładnej relacji z zaistniałego naruszenia od osoby powiadamiającej lub odpowiedzialnej za naruszenie jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem;
   3) podejmuje niezbędne działania mające na celu uniemożliwienie dalszego naruszenia bezpieczeństwa danych (odłączenie wadliwych urządzeń, zablokowanie dostępu do sieci, programów, zbiorów danych itp.);
   4) zabezpiecza, utrwala wszelkie informacje i dokumenty mogące stanowić pomoc przy ustaleniu przyczyn naruszenia;
   5) dokonuje analizy stanu zabezpieczeń wraz z oszacowaniem rozmiaru szkód powstałych na skutek naruszenia;
   6) rozważa celowość i potrzebę zawiadomienia o zaistniałym naruszeniu Administratora Danych Osobowych;
   7) nawiązuje bezpośredni kontakt ze specjalistami spoza Urzędu (jeśli zachodzi taka potrzeba);
   8) poddaje analizie metody pracy osób upoważnionych do przetwarzania danych osobowych;
   9) po wyczerpaniu niezbędnych środków doraźnych po zaistniałym naruszeniu proponuje działania naprawcze (w tym także ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń, oraz terminu wznowienia przetwarzania danych osobowych);
   10) dokumentuje zaistniały przypadek naruszenia bezpieczeństwa danych osobowych sporządzając raport, którego wzór stanowi **zał. nr 1** do niniejszej Instrukcji;
   11) w przypadku naruszenia ochrony danych osobowych, które skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych zawiadamia o naruszeniu Urząd Ochrony Danych Osobowych;
   12) w przypadku gdy naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych przygotowuje zawiadomienie o takim naruszeniu, które Administrator Danych Osobowych przekazuje osobie, której dane dotyczą.

2. W przypadku naruszenia danych w systemie informatycznym Inspektor Ochrony Danych wraz Administratorem Systemów Informatycznych lub Informatykiem Urzędu dodatkowo:

   1) sprawdza stan urządzeń wykorzystywanych do przetwarzania danych osobowych;

2) w celu powstrzymania lub ograniczenia dostępu do danych osoby nieupoważnionej podejmuje odpowiednie kroki zmierzające do: fizycznego odłączenia urządzeń i segmentów sieci, które mogłyby umożliwić dostęp do zbiorów danych osobie nieupoważnionej, wylogowania użytkownika systemu podejrzewanego o naruszenie zabezpieczenia ochrony danych, zmiany hasła poprzez które uzyskano nielegalny dostęp, aby uniknąć ponownej próby włamania;
3) przywraca prawidłowy stan działania systemu;
4) sprawdza sposób działania programów (w tym obecność wirusów komputerowych);
5) wyraża zgodę na ponowne uruchomienie komputera lub innych urządzeń.

§ 10

1. Inspektor Ochrony Danych oraz Administrator Systemów Informatycznych lub Informatyk Urzędu podejmują niezbędne działania w celu wyeliminowania naruszeń zabezpieczeń danych w przyszłości, a w szczególności:

   1) jeżeli przyczyną zdarzenia był stan techniczny urządzenia, sposób działania programu, uaktywnienie się wirusa komputerowego lub inny atak sieciowy, jakość komunikacji w sieci telekomunikacyjnej, niezwłocznie zlecają przeprowadzenie przeglądów oraz konserwacji urządzeń i programów, ustalenie źródła pochodzenia wirusa komputerowego lub innego ataku sieciowego oraz wdrożenie skuteczniejszego zabezpieczenia antywirusowego, a w miarę potrzeby kontaktują się z dostawcą usług telekomunikacyjnych w celu usprawnienia systemu zabezpieczeń;
   2) jeżeli przyczyną zdarzenia były wadliwe metody pracy, błędy i zaniedbania osób zatrudnionych przy przetwarzaniu danych osobowych, Inspektor Ochrony Danych przeprowadza dodatkowe kursy i szkolenia osób upoważnionych do przetwarzania danych osobowych, a wobec osób winnych zaniedbań wnioskuje o wyciągnięcie konsekwencji przewidzianych prawem;
   3) jeżeli przyczyną zdarzenia było włamanie, w celu nielegalnego pozyskania danych dokonuje szczegółowej analizy wdrożonych środków zabezpieczenia i proponuje wdrożenie skuteczniejszej ochrony fizycznej;
   4) jeżeli przyczyną zdarzenia był czyn zabroniony lub zachodzi jego uzasadnione podejrzenie, zawiadamia organy ścigania.

§ 11

1. Inspektor Ochrony Danych prowadzi rejestr naruszeń, który stanowi **załącznik nr 2** do niniejszej Instrukcji przy czym dopuszcza się możliwość prowadzenia rejestru w formie elektronicznej.
2. Inspektor Ochrony Danych wraz z Administratorem Systemów Informatycznych dokonuje rocznej analizy przypadków naruszeń. Dokument do analizy naruszeń stanowi **załącznik nr 3** do niniejszej Instrukcji.

ROZDZIAŁ 5
Postanowienia końcowe

§ 12

1. Każdy użytkownik przetwarzający dane osobowe w zbiorach danych zobowiązany jest zapoznać się z niniejszą Instrukcją i stosować przepisy w niej zawarte na swoim stanowisku pracy.
2. Nieprzestrzeganie zasad wskazanych w niniejszej Instrukcji stanowi niewykonanie bądź nienależyte wykonanie obowiązków pracowniczych lub niewykonanie bądź nienależyte wykonanie innej niż umowa o pracę umowy stanowiącej podstawę zatrudnienia, co może wiązać się dla osoby zatrudnionej z odpowiedzialnością majątkową wobec administratora danych.
3. Nadużycie przez użytkownika postanowień niniejszej Instrukcji może stanowić podstawę do pociągnięcia go do odpowiedzialności dyscyplinarnej lub karnej, w trybie i na zasadach przewidzianych przepisami prawa.

§ 13

W sprawach nie uregulowanych niniejszą Instrukcją zastosowanie znajdują przepisy Rozporządzenia Parlamentu Europejskiego i Rady z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych osobowych) oraz przepisy ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych.

załącznik nr 1
do Instrukcji postępowania w przypadku
naruszenia zasad ochrony danych osobowych

RAPORT Z NARUSZENIA
BEZPIECZEŃSTWA DANYCH OSOBOWYCH

Nr raportu ……/……. Data i godzina wystąpienia zdarzenia

.....

Miejsce wystąpienia zdarzenia

.....

Osoba zawiadamiająca

……..…….

……..

Opis zdarzenia i rodzaj naruszenia

.....

.....

.....

.....

.....

Przyczyny powstania zdarzenia

.....

.....

.....

.....

Zaistniałe skutki zagrożenia

.....

.....

.....

.....

.....

.....

.....

.....

Podjęte czynności naprawczo-zapobiegawcze

.....

.....

.....

.....

.....

Osoby zaangażowane w wyjaśnienie zdarzenia

……..……

……..

Podpisy:

……..…….

Osoba zgłaszająca

…….

Osoba nadzorująca

załącznik nr 2
do Instrukcji postępowania w przypadku
naruszenia zasad ochrony danych osobowych

REJESTR NARUSZEŃ

L.P	Data i numer raportu	Data i godzina wystąpienia zdarzenia	Rodzaj naruszenia	Informacja o zawiadomieniu UODO

załącznik nr 3
do Instrukcji postępowania w przypadku
naruszenia zasad ochrony danych osobowych

ROCZNA ANALIZA PRZYPADKÓW NARUSZEŃ

Data sporządzenia analizy .....

Osoba nadzorująca

……..……

Ilość naruszeń ……. w tym: uchybienia …… zagrożenia ……..

1) Ocena wdrożonych zabezpieczeń zapobiegających naruszeniom

.....

.....

.....

.....

2) Ocena realizacji działań naprawczo-zapobiegawczych

.....

.....

.....

.....

3) Zadania do realizacji w celu zapobiegania naruszeniom

.....

.....

.....

.....

.....

Podpisy:

……..……

Osoba nadzorująca

……..

Osoba przyjmująca raport

Załącznik Nr 3 do zarządzenia Nr 122/2021
Wójta Gminy Wejherowo
z dnia 31 sierpnia 2021 r.

INSTRUKCJA ZABEZPIECZENIA POMIESZCZEŃ URZĘDU GMINY WEJHEROWO ORAZ POSTĘPOWANIA Z KLUCZAMI

URZĄD GMINY WEJHEROWO

Data	Wersja	Opis zmiany	Autor
19.03.2019 r.	1.0.	Utworzenie dokumentu	Inspektor Ochrony Danych
31.08.2021 r.	2.0.	Aktualizacja dokumentu	Inspektor Ochrony Danych

Dokument przygotował

Imię i nazwisko	Stanowisko	Podpis
Monika Wegner	Inspektor Ochrony Danych	

Dokument zatwierdził

Data	Podpis
Wójt Gminy Wejherowo	
Przewodniczący Rady Gminy	

Rozdział 1

Postanowienia ogólne

§ 1

1. Instrukcja postępowania z kluczami oraz zabezpieczania pomieszczeń obowiązuje w siedzibie Urzędu Gminy Wejherowo znajdującego się pod adresem: ul. Transportowa 1, 84-200 Wejherowo.
2. Instrukcja postępowania z kluczami oraz zabezpieczenia pomieszczeń obowiązuje wszystkich pracowników Urzędu Gminy Wejherowo, praktykantów, stażystów oraz wolontariuszy.
3. **Użyte w niniejszej instrukcji określenia oznaczają:**
   1) **Urząd – Urząd Gminy Wejherowo,**
   2) **strefa administracyjna – budynek Urzędu Gminy Wejherowo,**
   3) **pracownik – pracownik Urzędu Gminy Wejherowo, stażysta, praktykant, wolontariusz**
   4) **Wójt – Wójt Gminy Wejherowo.**

Rozdział 2

Ochrona Urzędu

§ 2

1. Budynek Urzędu Gminy Wejherowo podlega ochronie polegającej na całodobowym monitorowaniu przez system alarmowy zainstalowany w budynku, nad którym nadzór świadczy wybrane przez Urząd Biuro Ochrony Mienia.
2. **Szczegółowy zakres obowiązków i ustaleń w zakresie ochrony i dozoru reguluje umowa zawarta pomiędzy Wójtem Gminy Wejherowo a Biurem Ochrony Mienia.**
3. **Z uwagi na publiczny charakter Urzędu w czasie jego pracy nie obowiązuje system przepustek, ani też inny system określający uprawnienia do wejścia, przebywania i wyjścia z budynku Urzędu.**
4. Zobowiązuje się pracowników w godzinach pracy Urzędu do:
   1) zwracania uwagi na zachowanie osób wchodzących i wychodzących z Urzędu;
   2) reagowania na wejście do budynku i przebywanie w nim osób będących pod wpływem alkoholu lub innych środków odurzających;
   3) reagowania na próby niszczenia, wynoszenia lub wywożenia mienia z budynku Urzędu;

4) reagowania na próby wnoszenia do budynku przedmiotów niebezpiecznych, materiałów lub substancji budzących podejrzenie możliwości naruszenia bezpieczeństwa Urzędu oraz pracowników;
5) natychmiastowego reagowania poprzez powiadomienie Wójta, a następnie odpowiednich służb (Policja, Straż Pożarna, Pogotowie Ratunkowe) o zaobserwowanych próbach stworzenia zagrożenia dla życia i zdrowia, a także utraty lub zniszczenia mienia.

5. Zobowiązuje się Kierownika Referatu Organizacyjnego i Kadr do zorganizowania pracy sprzątaczek w strefie administracyjnej poza rozkładem czasu pracy Urzędu w taki sposób, by wykonywały one niżej wymienione czynności:
   1) prowadzenie dozoru strefy administracyjnej w trakcie wykonywania obowiązków;
   2) sprawdzanie zamknięć drzwi i okien oraz stosowanych zabezpieczeń;
   3) sprawdzanie stanu technicznego urządzeń i armatury w pomieszczeniach higieniczno- sanitarnych;
   4) podejmowanie natychmiastowych czynności wyjaśniających w przypadku zaobserwowania obecności w strefie administracyjnej osób nie będących pracownikami Urzędu;
   5) natychmiastowego reagowania poprzez powiadomienie Wójta, a następnie odpowiednich służb (Policja, Straż Pożarna, Pogotowie Ratunkowe) o zaobserwowanych próbach stworzenia zagrożenia dla życia i zdrowia, a także utraty lub zniszczenia mienia.

Rozdział 3
Zabezpieczenie pomieszczeń i procedura postępowania z kluczami oraz kodami cyfrowymi do systemu alarmowego

§ 3.

1. Wójt nadaje pracownikom Biura Ochrony Mienia upoważnienia do otwierania głównych drzwi wejściowych do budynku oraz do rozkodowywania systemu alarmowego przed rozpoczęciem pracy Urzędu.
2. Budynek Urzędu posiada jedno wejście główne oraz jedno wejście pomocnicze.
3. Wójt posiada kody dostępu oraz klucze do pomocniczych drzwi wejściowych do budynku Urzędu. Wójt posiada możliwość otwarcia Urzędu w soboty, niedziele oraz święta.

4. Dostęp do kompletu kluczy wejściowych do głównego wejścia do budynku Urzędu posiadają następujące osoby:
   1) wyznaczony pracownik Referatu Organizacyjnego i Kadr;
   2) pracownicy Biura Ochrony Mienia;
   3) Sprzątaczka**.**
5. Komplet kluczy do pomocniczego wejścia do budynku Urzędu posiadają następujące osoby:
   1) wyznaczony pracownik Referatu Organizacyjnego i Kadr;
   2) Wójt Gminy Wejherowo.
6. Wójt oraz wyznaczony pracownik Referatu Organizacyjnego i Kadr uprawnione są do znajomości kodu cyfrowego systemu alarmowego.
7. Zamknięcia dostępu zewnętrznego do strefy administracyjnej po godzinie 16.30 w poniedziałki oraz po godzinie 15.30 od wtorku do piątku dokonuje sprzątaczka, która po zakończeniu swoich prac porządkowych od poniedziałku do piątku o godz. 20.30 zawiadamia Biuro Ochrony Mienia o konieczności zakodowania systemu alarmowego.
8. Sprzątaczka posiada dostęp do kompletu kluczy do głównych drzwi wejściowych, celem zamknięcia Urzędu na czas wykonywania obowiązków służbowych. Po zakończeniu pracy, pozostawia klucz w skrzynce znajdującej się na parterze budynku.
9. Do otwierania pomieszczeń dla potrzeb wykonania czynności związanych ze sprzątaniem wykorzystywane są klucze zdane przez pracowników po zakończeniu obowiązków służbowych do rąk własnych sprzątaczki bądź koszyka znajdującego się w pokoju nr 38 (piętro budynku Urzędu Gminy) lub w biurze podawczym (parter budynku Urzędu Gminy).
10. Pracownik, któremu zostały powierzone klucze wejściowe do budynku Urzędu zobowiązany jest do:
    1) wykorzystywania ich zgodnie z przeznaczeniem;
    2) nie kopiowania powierzonych kluczy bez zgody Wójta oraz nie udostępniania ich osobom trzecim.
11. Pracownicy Urzędu przed przystąpieniem do pracy pobierają klucze do swoich pomieszczeń biurowych ze skrzynki znajdującej się przy wejściu do Urzędu. Klucz otwierający skrzynkę z kluczami do pomieszczeń biurowych posiadają pracownicy biura ochrony mienia. Po pobraniu klucza, poszczególni pracownicy zapisują na liście obecności numer pobranego klucza.
12. Pracownicy przed rozpoczęciem pracy podpisują listę obecności znajdującą się w Biurze Podawczym (parter budynku Urzędu Gminy).

13. Po otwarciu pomieszczeń biurowych, przed przystąpieniem do pracy, pracownicy sprawdzają stan zastosowanych zabezpieczeń sprzętu biurowego i komputerowego, dokumentacji i innego wyposażenia.
14. W przypadku stwierdzenia nieprawidłowości lub naruszenia stanu zabezpieczeń pomieszczeń Urzędu, pracownik, który to stwierdził, natychmiast powiadamia o tym Inspektora Ochrony Danych lub bezpośredniego przełożonego.
15. Od momentu pobrania kluczy do momentu ich zdania, na pracownikach urzędujących w tych pomieszczeniach spoczywa pełna odpowiedzialność za ich zabezpieczenie.
16. Po zakończeniu pracy pracownicy zobowiązani są do uporządkowania swoich stanowisk pracy oraz wykonania czynności zabezpieczających adekwatnych do zastosowanych rozwiązań technicznych i organizacyjnych polegających na:
    1) zabezpieczeniu dokumentacji i pieczęci urzędowych;
    2) zabezpieczeniu komputerów i nośników informacji;
    3) wyłączeniu wszystkich urządzeń energetycznych zasilanych energią elektryczną (czajniki, wentylatory itp.) zgodnie z zasadami bhp;
    4) zamknięciu okien i drzwi;
    5) oddaniu kluczy od pomieszczeń biurowych do rąk własnych sprzątaczki bądź koszyka znajdującego się w pokoju nr 38 (piętro budynku Urzędu Gminy) lub w biurze podawczym (parter budynku Urzędu Gminy).
17. Klucze od biurek stanowiskowych i szaf biurowych są w posiadaniu pracowników, którzy ponoszą pełną odpowiedzialność za ich należyte zabezpieczenie.
18. Wójt wyznacza osobę odpowiedzialną za należyte przechowywanie, zabezpieczenie oraz udostępnianie kluczy zapasowych. Dostęp do kluczy zapasowych mają wyznaczone osoby Referatu Organizacyjnego i Kadr.
19. Wydawanie kluczy zapasowych (o których mowa w § 3 ust. 18) pracownikom może odbywać się tylko w uzasadnionych sytuacjach oraz w przypadkach awaryjnych za pokwitowaniem. Do wydawania kluczy zapasowych wyznaczony jest pracownik Referatu Organizacyjnego i Kadr.
20. Klucze zapasowe po ich wykorzystaniu należy niezwłocznie zwrócić do depozytu .
21. Otwarcie Urzędu w soboty, niedziele oraz święta możliwe jest wyłącznie za zgodą Wójta bądź osoby przez niego upoważnionej.