Zarządzenie nr 108/1/2018
z dnia 6 grudnia 2018 roku
Wójta Gminy Waśniów

w sprawie dokumentacji przetwarzania danych osobowych

Na podstawie art. 24 ust. 1 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) z dnia 27 kwietnia 2016 r. (Dz.Urz.UE.L Nr 119) oraz art. 33 ust. 1 ustawy z dnia z dnia 8 marca 1990 r. o samorządzie gminnym (Dz.U. z 2018 poz.994 z póź zm.),

zarządza się co następuje:

§ 1

Wprowadzam do stosowania dokumentację opisującą sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych w Urzędzie Gminy w Waśniowie.

§ 2

Na dokumentację o której mowa w § 1 składają się:

1. Polityka bezpieczeństwa informacji.
2. Instrukcja zarządzania systemem informatycznym.

§ 3

Traci moc zarządzenie Wójta Gminy Waśniów nr 39/2015 z dnia 24.06.2015r.

§ 4

Zarządzenie wchodzi w życie z dniem podjęcia.

WÓJT
Krzysztof Gajewski

POLITYKA BEZPIECZEŃSTWA INFORMACJI

UWAGA:
Dokument wyłącznie
do użytku wewnętrznego

Zatwierdził:	**Data:**
Administrator Danych Osobowych	

Rozdział I
Postanowienia ogólne, definicje

§ 1. 1. Polityka Bezpieczeństwa Informacji w Urzędzie Gminy w Waśniowie jest zbiorem zasad i procedur obowiązujących przy przetwarzaniu i wykorzystywaniu danych osobowych przez Urząd Gminy w Waśniowie.

2. Podstawą do opracowania i wdrożenia dokumentu są:
   1) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 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.
   2) Ustawa z dnia 10 maja 2018 roku o ochronie danych osobowych.

3. Przetwarzanie danych osobowych w Urzędzie Gminy w Waśniowie jest dopuszczalne wyłącznie pod warunkiem przestrzegania zasad wynikających z aktualnie obowiązujących przepisów prawa w tym niniejszej polityki i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

4. Polityka Bezpieczeństwa ma zastosowanie do ochrony zbiorów danych osobowych przetwarzanych w Urzędzie Gminy w Waśniowie, w celu ich bezpiecznego wykorzystania oraz określa zasady korzystania z systemów informatycznych.

§ 2. Określenia i skróty użyte w Polityce Bezpieczeństwa Informacji oznaczają:
1) Rozporządzenie – Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 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;
2) Ustawa – ustawę z dnia 10 maja 2018 roku o ochronie danych osobowych;
3) Urząd – Urząd Gminy w Waśniowie;
4) Administrator Danych Osobowych – Urząd Gminy w Waśniowie w imieniu której działa Wójt Gminy;
5) Inspektor Ochrony Danych – osobę wyznaczoną przez Administratora Danych Osobowych, zwaną dalej „IOD";
6) Administrator Systemów Informatycznych – osobę odpowiedzialną za sprawność i konserwację oraz wdrażanie technicznych zabezpieczeń systemów informatycznych przetwarzających zbiory danych osobowych zwaną dalej „ASI";
7) identyfikator - rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym,
8) hasło – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie użytkownikowi;
9) osoba upoważniona do przetwarzania danych osobowych – rozumie się przez to osobę, która upoważniona została do przetwarzania danych osobowych przez Administratora Danych Osobowych na piśmie. Dotyczy to zarówno zatrudnionych, świadczących usługi na podstawie umów cywilno-prawnych jak i innych, np. stażystów, wolontariuszy, praktykantów;
10) użytkownik systemu - osoba posiadająca upoważnienie wydane przez Administratora Danych Osobowych i dopuszczona jako użytkownik do przetwarzania danych osobowych w systemie informatycznym w zakresie wskazanym w upoważnieniu.

Rozdział II
Obszary i procesy przetwarzania danych osobowych

§ 3. 1. Obszar przetwarzania danych osobowych w Urzędzie Gminy w Waśniowie obejmuje budynki, pomieszczenia i części pomieszczeń, w których przetwarzane są dane osobowe oraz miejsca, gdzie przechowuje się nośniki informacji zawierające dane osobowe.

2. W szczególnie uzasadnionych przypadkach, za zgodą Administratora Danych Osobowych, może dochodzić do przetwarzania danych osobowych poza obszarem przetwarzania danych, jednakże osoba dokonująca takiego przetwarzania musi stosować zabezpieczenia wynikające z niniejszego dokumentu.

§ 4. 1. Dane osobowe, których administratorem jest Urząd Gminy w Waśniowie gromadzone są w zbiorach danych.
2. Administrator danych nie podejmuje czynności przetwarzania, które mogłyby się wiązać z poważnym prawdopodobieństwem wystąpienia wysokiego ryzyka dla praw i wolności osób. W przypadku planowania takiego działania Administrator wykona czynności określone w art. 35 rozporządzenia.
3. W przypadku planowania nowych czynności przetwarzania Administrator dokonuje analizy ich skutków dla ochrony danych osobowych oraz uwzględnia kwestie ochrony danych w fazie ich projektowania.
4. Administrator danych prowadzi rejestr czynności przetwarzania. Wzór rejestru czynności przetwarzania stanowi załącznik nr 1 do niniejszej polityki.
5. W przypadku, gdy podstawą przetwarzania danych osobowych jest umowa zawarta pomiędzy administratorem danych a Urzędem, który będzie podmiotem przetwarzającym (procesorem) prowadzi się rejestr czynności przetwarzania, który stanowi załącznik nr 2 do niniejszej polityki.

Rozdział III
Organizacja systemu ochrony danych osobowych

§ 5. Administrator danych osobowych realizuje zadania w zakresie organizacji systemu ochrony danych osobowych, w szczególności:

1) podejmuje decyzje o celach i środkach przetwarzania danych osobowych;
2) upoważnia osoby do przetwarzania danych osobowych w określonym indywidualnie zakresie;
3) wyznacza Inspektora Ochrony Danych oraz określa zakres jego zadań;
4) zapewnia użytkownikom odpowiednie stanowiska pracy umożliwiające bezpieczne przetwarzanie danych;
5) podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia procedur bezpiecznego przetwarzania danych osobowych.

§ 6.1. Inspektor Ochrony Danych realizuje zadania w zakresie nadzoru nad przestrzeganiem zasad ochrony danych osobowych, w szczególności:

1) sprawuje nadzór na wdrożeniem i funkcjonowaniem stosownych środków organizacyjnych, technicznych i fizycznych w celu zapewnienia bezpieczeństwa danych;
2) monitoruje przestrzeganie przepisów w zakresie danych osobowych oraz nadzoruje działania pod względem zgodności przetwarzania danych z przepisami o ochronie danych osobowych;
3) prowadzi oraz aktualizuje dokumentację opisującą sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych;
4) prowadzi dokumentację z zakresu ochrony danych;
5) podejmuje odpowiednie działania w wypadku naruszenia systemu ochrony danych osobowych;
6) inicjuje i podejmuje przedsięwzięcia w zakresie doskonalenia systemu ochrony danych osobowych;
7) prowadzi szkolenia osób upoważnionych do przetwarzania danych osobowych;
8) współpracuje z organem nadzorczym oraz pełni funkcję punktu kontaktowego dla organu nadzorczego w szczególności w sprawach związanych z przetwarzaniem danych osobowych;
9) prowadzi rejestr czynności przetwarzania;
10) prowadzi rejestr kategorii czynności przetwarzania.

2. Inspektora Ochrony Danych wyznacza administrator danych osobowych.

§ 7.1. Administrator systemu informatycznego realizuje zadania w zakresie zarządzania i bieżącego nadzoru nad systemem informatycznym administratora danych, w szczególności:

1) zarządza systemem informatycznym, w którym przetwarzane są dane osobowe;
2) przeciwdziała dostępowi osób niepowołanych do systemu informatycznego, w którym przetwarzane są dane osobowe;
3) dokonuje wszelkich czynności związanych z przydzieleniem użytkownikom identyfikatorów i haseł dostępu do systemu informatycznego zgodnie z wydanym przez administratora danych osobowych upoważnieniem oraz dokonuje modyfikacji tych uprawnień, a także blokuje konta użytkowników zgodnie z zasadami określonymi w instrukcji zarządzania systemem informatycznym;
4) sprawuje nadzór nad funkcjonowaniem mechanizmów uwierzytelniania użytkowników oraz kontroli dostępu do danych osobowych przetwarzanych w systemach informatycznych;
5) w sytuacji stwierdzenia naruszenia zabezpieczeń systemu informatycznego niezwłocznie informuje IOD o naruszeniu i współdziała z nim przy usuwaniu skutków naruszenia;
6) sprawuje nadzór nad wykonywaniem napraw, konserwacją oraz likwidacją urządzeń i komputerów, na których zapisane są dane osobowe;
7) podejmuje działania służące zapewnieniu niezawodności zasilania komputerów, innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych oraz zapewnieniu bezpiecznej wymiany danych w sieci wewnętrznej i bezpiecznej teletransmisji;
8) odpowiada za wykonywanie kopii zapasowych, ich odpowiednie przechowywanie oraz okresowe sprawdzanie pod kątem ich dalszej przydatności;
9) wykonuje wszelkie czynności przewidziane w Instrukcji Zarządzania Systemem Informatycznym.

2. Administratora systemu informatycznego wyznacza administrator danych osobowych.

§ 8. Osoba upoważniona do przetwarzania danych osobowych jest zobowiązana przestrzegać zasad wynikających z wewnętrznych aktów prawnych, w szczególności:

1) może przetwarzać dane osobowe wyłącznie w zakresie ustalonym indywidualnie przez administratora danych w upoważnieniu i tylko w celu wykonywania nałożonych na nią obowiązków;
2) zachowuje w tajemnicy dane osobowe oraz stosowane metody ich zabezpieczeń. Przestrzeganie tajemnicy danych osobowych obowiązuje przez cały okres zatrudnienia u administratora danych, a także po ustaniu stosunku pracy lub odwołaniu z pełnionej funkcji;
3) stosuje określone przez administratora danych oraz IOD procedury oraz wytyczne mające na celu zgodne z prawem, w tym zwłaszcza adekwatne, przetwarzanie danych;
4) zabezpiecza dane przed ich udostępnianiem osobom nieupoważnionym oraz uniemożliwia dostęp do danych osobowych przez osoby nieuprawnione.

§ 9.1. Do przetwarzania danych osobowych mogą być dopuszczone wyłączenie osoby posiadające imienne upoważnienie podpisane przez Administratora Danych Osobowych. Wzór upoważnienia stanowi załącznik nr 3 do Polityki Bezpieczeństwa Informacji.

2. Inspektor Ochrony Danych prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych. Wzór ewidencji stanowi załącznik nr 4 do Polityki Bezpieczeństwa Informacji.

3. Upoważnione dostępu do danych osobowych przetwarzanych w Urzędzie Gminy w Waśniowie może zostać wydane:

1) osobie zatrudnionej;
2) osobie związanej umową o świadczenie usług;
3) stażyście realizującym staż zawodowy;
4) praktykantowi odbywającemu praktyki zawodowe.

4. Za przygotowanie upoważnienia dostępu do danych osobowych odpowiadają:
   1) bezpośredni przełożony, w przypadku osoby zatrudnionej;
   2) osoba nadzorująca wykonywane prace, w przypadku osoby związanej umową o świadczenie usług;
   3) opiekun stażu, w przypadku stażysty;
   4) opiekun praktyki, w przypadku praktykanta.
5. Administrator Danych Osobowych przekazuje podpisane upoważnienie Inspektorowi Ochrony Danych celem wpisania do ewidencji o której mowa w pkt. 2.
6. W przypadku osób, których zakres upoważnienia obejmuje jednocześnie dostęp do systemu informatycznego upoważnienie przekazuje się również Administratorowi Systemu Informatycznego celem zarejestrowania użytkownika w systemie.
7. Oryginał upoważnienia przechowuje się w aktach osobowych pracownika.
8. Procedurę opisaną w pkt. 3-7 stosuje się również w przypadku cofnięcia upoważnienia dostępu do danych osobowych.

§ 10. Przed dopuszczeniem do pracy przy przetwarzaniu danych osobowych, każdy osoba powinna być zaznajomiona z przepisami dotyczącymi danych osobowych.

Rozdział IV
Zasady ochrony danych osobowych

§ 11. 1. W siedzibie Urzędu Gminy w Waśniowie na podstawie przeprowadzonej analizy ryzyka zastosowano poziom zabezpieczeń fizycznych i organizacyjnych adekwatny do mogących wystąpić zagrożeń.
2. Nad bezpieczeństwem obiektów wchodzących w skład obszaru przetwarzania danych czuwa na podstawie podpisanych umów firma zewnętrzna posiadająca stosowne uprawnienia do prowadzenia działalności ochroniarskiej.
3. Budynki wchodzące w skład obszaru przetwarzania danych zabezpieczono instalacją alarmową informującą zewnętrznym i wewnętrznym sygnałem dźwiękowym o próbie włamania.
4. W przypadku zaistnienia pożaru w oznaczonych miejscach znajdują się hydranty i przenośne gaśnice przeciwpożarowe.
5. Drzwi wejściowe do budynku zamykane są na zamek patentowy dzięki czemu dostęp do pomieszczeń dla osób postronnych po zakończeniu pracy jest niemożliwy.
6. Dostęp do pomieszczeń poza wyznaczonymi godzinami pracy mają wyłącznie osoby upoważnione przez Administratora Danych Osobowych.

§. 12. 1. W celu właściwego zabezpieczenia danych osobowych każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest do:
   1) ustawiania ekranów komputerowych w sposób uniemożliwiający odczyt informacji przez osoby nieupoważnione;
   2) niepozostawiania bez kontroli dokumentów, nośników danych i sprzętu zwłaszcza w trakcie przenoszenia lub przetwarzania danych osobowych poza siedzibą administratora danych;
   3) niepozostawiania bez nadzoru akt, pamięci przenośnych i komputerów przenośnych;
   4) kasowania po wykorzystaniu danych na dyskach przenośnych;
   5) niezapisywania hasła wymaganego do uwierzytelnienia się w systemie na papierze lub innym nośniku;
   6) niepodłączania do listew podtrzymujących napięcie przeznaczonych dla sprzętu komputerowego innych urządzeń;
   7) niedokonywania samodzielnej ingerencji w oprogramowanie i konfigurację powierzonego sprzętu;
   8) opuszczania stanowiska pracy dopiero po aktywowaniu wygaszacza ekranu lub po zablokowaniu stacji roboczej w inny sposób;

9) przesyłania danych osobowych poprzez sieć publiczną wyłącznie w postaci zaszyfrowanej;
10) niszczenia w niszczarce niewykorzystanych lub zbędnych dokumentów zawierających dane osobowe;
11) niszczenia w niszczarce zbędnych lub uszkodzonych nośników informacji zawierających dane osobowe;
12) niepozostawiania osób postronnych w pomieszczeniu, w którym przetwarzane są dane osobowe, bez obecności osoby upoważnionej do przetwarzania danych osobowych;
13) zachowania w tajemnicy wszelkich informacji pozyskanych w trakcie wykonywania obowiązków służbowych;
14) chowania do zamykanych na klucz szaf wszelkich dokumentów zawierających dane osobowe przed opuszczeniem miejsca pracy oraz po zakończeniu dnia pracy;
15) umieszczania kluczy do szaf w ustalonym, przeznaczonym do tego miejscu po zakończeniu dnia pracy;
16) zamykania okien w razie opuszczania pomieszczenia, w tym zwłaszcza po zakończeniu dnia pracy;
17) zamykania drzwi na klucz po zakończeniu pracy w danym dniu i złożenia klucza w wyznaczonym do tego i zabezpieczonym miejscu.

Rozdział V
Gromadzenie danych osobowych

§ 13.1. Dane osobowe przetwarzane w Urzędzie Gminy w Waśniowie mogą być pozyskiwane bezpośrednio od osób, których te dane dotyczą, lub z innych źródeł, w granicach dozwolonych przepisami obowiązującego prawa.
2. Kierownik komórki organizacyjnej zobowiązany jest poinformować Inspektora Ochrony Danych o zamiarze utworzenia nowego zbioru danych osobowych.

§ 14. 1. Zebrane dane osobowe mogą być wykorzystane wyłącznie do celów, dla jakich zostały zebrane. Po wykorzystaniu dane osobowe powinny być przechowywane w formie uniemożliwiającej identyfikację osób, których dotyczą.
2. W przypadku konieczności udostępnienia dokumentów, w których znajdują się dane osobowe niemające bezpośredniego związku z celem udostępnienia, należy bezwzględnie dokonać anonimizacji tych danych osobowych.

§ 15.1. W przypadku gdy dane osobowe są niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem przepisów albo są zbędne do realizacji celu, dla którego zostały zebrane, ADO jest zobowiązany do ich uzupełnienia, uaktualnienia, sprostowania lub usunięcia.
2. Inspektor Ochrony Danych przeprowadza raz w roku przegląd przetwarzanych zbiorów danych osobowych pod kątem celowości ich dalszego przetwarzania. Osoby upoważnione do przetwarzania danych osobowych są obowiązane współpracować z IOD w tym zakresie i wskazywać mu zbiory danych osobowych oraz dane osobowe, które powinny zostać usunięte ze względu na zrealizowanie celu przetwarzania danych osobowych lub brak ich adekwatności do realizowanego celu.

Rozdział VI
Obowiązek informacyjny

§ 16. 1. Kierownicy komórek organizacyjnych, w których są zbieranie i przetwarzane dane osobowe, są

odpowiedzialni za spełnienie obowiązku informacyjnego o którym mowa w art. 13 RODO.
2. Klauzule informacyjne kierownicy komórek organizacyjnych uzgadniają z Inspektorem Ochrony Danych.

§ 17. 1. Zabrania się wykorzystywania danych osobowych do prowadzenia działalności marketingowej.
2. Wykorzystywania danych osobowych do działalności marketingowej możliwe jest wyłącznie, gdy osoba, której dane dotyczą wyrazi na to zgodę.
3. Kandydaci do pracy w procesie rekrutacji są zobowiązani podpisać pisemną zgodę na przetwarzanie ich danych osobowych.
4. Dokumenty złożone w celu określonym w ust. 3 są przechowywane w komórce organizacyjnej, która przetwarza te dane, i są włączane do akt osobowych pracownika.

Rozdział VII
Udostępnianie danych osobowych

§ 18. 1. Administrator Danych Osobowych udostępnia dane osobowe przetwarzane we własnych zbiorach wyłącznie osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa.
2. Dane osobowe mogą być udostępniane w następujących przypadkach:
1) na podstawie wniosku od podmiotu uprawnionego do otrzymywania danych osobowych na podstawie przepisów;
2) na podstawie umowy z innym podmiotem, w ramach której istnieje konieczność udostępnienia danych;
3) na podstawie wniosku osoby, której dane dotyczą.
3. Udostępniając dane osobowe należy zaznaczyć, że można je wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.
4. W przypadku żądania udzielenia informacji na temat przetwarzanych danych osobowych na pisemny wniosek pochodzący od osoby, której dane dotyczą, odpowiedź na wniosek następuje w terminie 30 dni od daty jego otrzymania.

§ 19. Odmowa udostępnienia danych osobowych następuje wówczas, gdy spowodowałoby to istotne naruszenia dóbr osobistych osób, których dane dotyczą, lub innych osób oraz jeżeli dane osobowe nie mają istotnego związku ze wskazanymi we wniosku motywami działania wnioskodawcy.
§ 20. W przypadku wątpliwości przy realizacji wniosku o udostępnienie danych osobowych należy niezwłocznie skontaktować się z Inspektorem Ochrony Danych.

Rozdział VIII
Powierzenie przetwarzania danych osobowych

§ 21. 1. Powierzenie przetwarzania danych osobowych odbywa się zgodnie z obowiązującymi przepisami prawa w drodze umowy zawartej na piśmie pomiędzy Administratorem Danych Osobowych a danym podmiotem, któremu zleca się czynności związane z przetwarzaniem danych osobowych.
2. Inspektor Ochrony Danych prowadzi rejestr umów powierzenia przetwarzania danych osobowych.

Rozdział IX
Postępowanie w przypadku naruszeń

§ 22. 1. Przepisy niniejszego rozdziału stosuje się w przypadku:
1) stwierdzenia naruszenia zabezpieczenia systemu informatycznego w obszarze danych osobowych;

2) podejrzenia naruszenia bezpieczeństwa danych osobowych ze względu na stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci komputerowej.

§ 23. Zasady postępowania przypadku naruszenia bezpieczeństwa danych osobowych obowiązują wszystkie osoby biorące udział w procesie przetwarzania danych osobowych.

§ 24. 1. Naruszeniem zabezpieczenia systemu informatycznego, przetwarzającego dane osobowe jest każdy stwierdzony fakt nieuprawnionego ujawnienia danych osobowych, udostępnienia lub umożliwienia dostępu do nich osobom nieupoważnionym, zabrania danych przez osobę nieupoważnioną, uszkodzenia jakiegokolwiek elementu systemu informatycznego, a w szczególności:

1) nieautoryzowany dostęp do danych;
2) nieautoryzowane modyfikacje lub zniszczenie danych;
3) udostępnienie danych nieautoryzowanym podmiotom;
4) nielegalne ujawnienie danych;
5) pozyskiwanie danych z nielegalnych źródeł.

§ 25. 1. W przypadku stwierdzenia naruszenia zabezpieczenia systemu informatycznego lub zaistnienia sytuacji, które mogą wskazywać na naruszenie zabezpieczenia danych osobowych, każdy pracownik zatrudniony przy przetwarzaniu danych osobowych jest zobowiązany przerwać przetwarzanie danych osobowych i niezwłocznie powiadomić o tym fakcie bezpośredniego przełożonego oraz Inspektora Ochrony Danych.

2. Działania, o których mowa w ust. 1 podejmuje się również, gdy stan urządzeń, zawartość zbioru danych osobowych, ustalone metody pracy i obsługi tych zbiorów, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej, mogą wskazywać na naruszenie zabezpieczenia tych baz lub zbiorów.

3. Inspektor Ochrony Danych wspólnie z Administratorem Systemu Informatycznego w sytuacjach o których mowa w pkt. 1 i 2 podejmują natychmiastowe doraźne działania, sprowadzające się do usunięcia naruszenia.

4. W przypadku stwierdzenia naruszenia ochrony danych osobowych IOD dokonuje oceny, czy zaistniałe naruszenie mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych.

5. W każdej sytuacji, w której zaistniałe naruszenie mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych, IOD informuje o tym niezwłocznie Administratora danych osobowych.

6. Administrator danych osobowych zgłasza fakt naruszenia zasad ochrony danych organowi nadzorczemu bez zbędnej zwłoki – jeżeli to wykonalne, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia.

7. Jeżeli ryzyko naruszenia praw i wolności jest wysokie, Administrator danych osobowych zawiadamia o incydencie także osobę, której dane dotyczą.

Rozdział X
Postanowienia końcowe

§ 26. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest zapoznać się z niniejszym dokumentem oraz złożyć stosowne oświadczenie, potwierdzające znajomość jego treści.

§ 27. Zabrania się udostępniania kopi dokumentu osobom nieuprawnionym bez zgody Inspektora Ochrony Danych.

WÓJT
Krzysztof Gajewski

Załącznik nr 1
do Polityki Bezpieczeństwa Informacji

REJESTR CZYNNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH

Nazwa i dane kontaktowe administratora	
Nazwa	
Adres	
e - mail	
Telefon	

Inspektor Ochrony Danych (jeśli powołano)	
Nazwa	
Adres	
e - mail	
Telefon	

Przedstawiciel (jeśli wyznaczono)	
Nazwa	
Adres	
e - mail	
Telefon	

SPIS TREŚCI:

Nazwa czynności przetwarzania	
Komórka organizacyjna	
Cel przetwarzania (art. 30 ust. 1 pkt b)	
Opis kategorii osób, których dane dotyczą (art. 30 ust. 1 pkt c)	
Opis kategorii danych osobowych (art. 30 ust. 1 pkt c)	
Podstawa prawna przetwarzania danych	
Źródło danych	
Planowany termin usunięcia poszczególnych kategorii danych (jeżeli jest to możliwe) (art. 30 ust. 1 pkt f)	
Nazwa współadministratora i dane kontaktowe (jeśli dotyczy) (art. 30 ust. 1 pkt a)	
Nazwa podmiotu przetwarzającego i dane kontaktowe (jeśli dotyczy) (art. 30 ust. 1 pkt d)	
Kategorie odbiorców (innych niż podmiot przetwarzający) (art.30 ust. 1 pkt d)	
Nazwa systemu lub oprogramowania	
Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa zgodnie z art. 32 ust. 1 (jeżeli jest to możliwe) (Art. 30 ust. 1 pkt g)	
DPIA (jeśli tak, lokalizacja raportu)	
Transfer do kraju trzeciego lub organizacji międzynarodowej (nazwa kraju i podmiotu) (art. 30 ust.1 pkt e)	
Jeśli transfer i art. 49 ust. 1 akapit drugi - dokumentacja odpowiednich zabezpieczeń (art. 30 ust.1 pkt e)	

WÓJT
Krzysztof Gajewski

Załącznik nr 2
do Polityki Bezpieczeństwa Informacji

REJESTR KATEGORII CZYNNOŚCI PRZETWARZANIA

Nazwa i dane kontaktowe administratora	
Nazwa	
Adres	
e - mail	
Telefon	

Inspektor Ochrony Danych (jeśli powołano)	
Nazwa	
Adres	
e - mail	
Telefon	

Przedstawiciel (jeśli wyznaczono)	
Nazwa	
Adres	
e - mail	
Telefon	

WÓJT
Krzysztof Gajewski

SPIS TREŚCI:

WÓJT
Krzysztof Gajewski

Kategoria przetwarzania (art. 30 ust. 2 lit. b)	
Komórka organizacyjna	
Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa (art. 30 ust. 2 lit. d, art. 32 ust. 1)	
Nazwa i dane kontaktowe administratora (art. 30 ust. 2 lit. a)	
Nazwa i dane kontaktowe współadministratora (jeżeli dotyczy)	
Nazwa i dane kontaktowe przedstawiciela administratora (jeśli wyznaczono)	
Inspektor ochrony danych administratora (jeżeli powołano)	
Nazwy państw trzecich lub organizacji międzynarodowych, do których dane są przekazywane (art. 30 ust. 2 lit. c)	
Dokumentacja odpowiednich zabezpieczeń danych osobowych przekazywanych na podstawie art. 49 ust. 1 akapit drugi (art. 30 ust. 2 lit. c)	
Nazwa i dane kontaktowe podprzetwarzającego (podwykonawcy)	
Kategorie podpowierzonych przetwarzań	

WÓJT
Krzysztof Gajewski

Załącznik nr 3
do Polityki Bezpieczeństwa Informacji

.....
(pieczęć jednostki)

UPOWAŻNIENIE/ANULOWANIE UPOWAŻNIENIA*
do przetwarzania danych osobowych

Na podstawie art. 32 ust. 4 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 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) – dalej RODO

Upoważniam/anuluję upoważnienie

Panią/Pana.....
zatrudnionego w: Urzędzie Gminy w Waśniowie
do przetwarzania danych osobowych w zakresie:
pełnionych obowiązków służbowych wynikających z zawartej umowy i zakresu czynności na zajmowanym stanowisku.

oraz obsługi systemu informatycznego:
na zajmowanym stanowisku pracy .....
służącego do przetwarzania danych osobowych.

Upoważnienia udziela się na czas: trwania umowy o pracę
Upoważnienie niniejsze nie upoważnia do udzielania dalszych upoważnień.

.....
(data wydania/cofnięcia upoważnienia)

.....
(pieczęć i podpis ADO)

OŚWIADCZENIE

Oświadczam, że są mi znane obowiązki i odpowiedzialność wynikające z udzielonego mi jak wyżej upoważnienia.

.....
(pieczęć użytkownika)

Wypełnia Administrator Systemu Informatycznego:

Identyfikator użytkownika: .....
Data zarejestrowania w systemie: .....**
Data wyrejestrowania użytkownika z systemu: .....***

Podpis Administratora: .....

*) niepotrzebne skreślić
**) wypełnić w przypadku wydania upoważnienia
***) wypełnić w przypadku anulowania upoważnienia

WÓJT
Krzysztof Gajewski

Urząd Gminy w Waśniowie

Załącznik nr 4
do Polityki Bezpieczeństwa Informacji

EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH

Lp.	Imię i nazwisko	Zakres upoważnienia (nazwa zbioru danych)	Identyfikator w systemie informatycznym	Data nadania upoważnienia	Data ustania upoważnienia	UWAGI

WÓJT
Krzysztof Gajewski

.....
podpis IOD

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

UWAGA:
Dokument wyłącznie
do użytku wewnętrznego

Zatwierdził:	**Data:**
Administrator Danych Osobowych	

Rozdział I
Wprowadzenie

§ 1.1 Niniejsza instrukcja określa zasady eksploatacji i zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie Gminy w Waśniowie, zwanym dalej Urzędem.

2. Zasady opisane w niniejszym dokumencie są zgodne z obowiązującymi wymaganiami prawnymi, w szczególności:

1) Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z 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.
2) Ustawą z dnia 10 maja 2018 roku o ochronie danych osobowych.

3. Określenia i skróty użyte w niniejszym dokumencie oznaczają:

1) Rozporządzenie – Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 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;
2) Ustawa – ustawę z dnia 10 maja 2018 roku o ochronie danych osobowych;
3) Administrator Danych Osobowych – Urząd Gminy w Waśniowie w imieniu której działa Wójt Gminy;
4) Inspektor Ochrony Danych – osobę wyznaczoną przez Administratora Danych Osobowych, zwaną dalej „IOD";
5) Administrator Systemów Informatycznych – osobę wyznaczoną przez Administratora Danych Osobowych, odpowiedzialną za sprawność i konserwację oraz wdrażanie technicznych zabezpieczeń systemów informatycznych przetwarzających zbiory danych osobowych zwaną dalej „ASI";
6) identyfikator - rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym,
7) hasło – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie użytkownikowi;
8) osoba upoważniona do przetwarzania danych osobowych – rozumie się przez to osobę, która upoważniona została do przetwarzania danych osobowych przez Administratora Danych Osobowych na piśmie. Dotyczy to zarówno zatrudnionych, świadczących usługi na podstawie umów cywilno-prawnych jak i innych, np. stażystów, wolontariuszy, praktykantów;
9) użytkownik systemu - osoba posiadająca upoważnienie wydane przez Administratora Danych Osobowych i dopuszczona jako użytkownik do przetwarzania danych osobowych w systemie informatycznym w zakresie wskazanym w upoważnieniu.

Rozdział II
Procedura nadawania i odbierania uprawnień do systemów informatycznych

§ 2.1. Podstawą do nadania uprawnień do przetwarzania danych osobowych w systemie informatycznym Urzędu Gminy w Waśniowie jest upoważnienie do przetwarzania danych osobowych wydawane przez Administratora Danych Osobowych według procedury opisanej w § 10 Polityki Bezpieczeństwa Informacji.

2. Za nadanie uprawnień w systemie informatycznym odpowiada Administrator Systemu Informatycznego. Uprawnienia nie mogą być nadane, jeżeli osoba nie posiada upoważnienia do przetwarzania danych osobowych w wymaganym zakresie.

3. W przypadku nadawania użytkownikowi uprawnień do danego systemu informatycznego po raz pierwszy, Administrator Systemu Informatycznego przyznaje użytkownikowi identyfikator, który jest wpisywany do upoważnienia oraz ewidencji osób upoważnionych do przetwarzania danych osobowych.

4. Identyfikator użytkownika w systemie informatycznym musi być unikalny dla każdego użytkownika. Sprawdzenie unikalności identyfikatora odbywa się na podstawie ewidencji osób upoważnionych do przetwarzania danych osobowych.
5. Hasło użytkownika jest przydzielane indywidualnie i znane jest tylko użytkownikowi, który się nim posługuje.
6. Administrator Systemu Informatycznego po wygenerowaniu identyfikatora i hasła dostępu do systemu informatycznego przekazuje je niezwłocznie użytkownikowi.
7. Użytkownik przy pierwszym logowaniu do systemu informatycznego zobowiązany jest do zmiany hasła.

§ 3.1. W przypadku odebrania lub zmiany zakresu upoważnienia dostępu do systemów informatycznych stosuje się procedurę opisaną w § 10 Polityki Bezpieczeństwa Informacji.
2. W przypadku odebrania uprawnień Administrator Systemu Informatycznego niezwłocznie dokonuje zablokowania użytkownika w systemie informatycznym. Niedopuszczalne jest całkowite usunięcie konta użytkownika z systemu informatycznego.

Rozdział III
Stosowane metody i środki uwierzytelnienia

§ 4.1. Użytkownicy systemu informatycznego służącego do przetwarzania danych osobowych wykorzystują w procesie uwierzytelnienia identyfikatory i hasła.
2. Identyfikator jest w sposób jednoznaczny przypisany użytkownikowi oraz nie podlega zmianie.
3. Hasło dostępu do systemów informatycznych jest przekazywane użytkownikowi przez Administratora Systemów Informatycznych.
4. Po zalogowaniu do systemu z wykorzystaniem otrzymanego hasła użytkownik jest zobowiązany do dokonania jego natychmiastowej zmiany, nawet, jeżeli system informatyczny nie wymusza takiego działania.
5. Hasło powinno składać się z zestawu co najmniej ośmiu znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne. Hasło nie może być identyczne z identyfikatorem użytkownika ani z jego imieniem lub nazwiskiem.
6. Hasło jest zmieniane przez użytkownika nie rzadziej niż raz na pół roku lub niezwłocznie w przypadku podejrzenia, iż mogły z nim się zapoznać nieuprawnione osoby.
7. W przypadku systemów informatycznych zastosowano wymuszoną zmianę hasła.
8. W przypadku systemów informatycznych w których nie zastosowano procedury o której mowa w § 4 pkt. 7 za zmianę hasła odpowiada użytkownik.
9. Użytkownik zobowiązany jest do:
   1) nieujawniania hasła innym osobom, w tym innym użytkownikom,
   2) zachowania hasła w tajemnicy, również po jego wygaśnięciu,
   3) niezapisywania hasła,
   4) postępowania z hasłami w sposób uniemożliwiający dostęp do nich osobom trzecim,
   5) przestrzegania zasad dotyczących jakości i częstotliwości zmiany hasła,
   6) wprowadzania hasła do systemu w sposób minimalizujący podejrzenie go przez innych użytkowników systemu.
10. W sytuacjach awaryjnych użytkownik powinien zwrócić się do Administratora Systemów Informatycznych w celu wygenerowanie nowego hasła.
11. W przypadku podejrzenia zapoznania się z hasłem przez osobę nieuprawnioną użytkownik jest zobowiązany do natychmiastowej zmiany hasła oraz powiadomienia o zaistniałym fakcie Administratora Systemów Informatycznych.

§ 5.1. Administrator Systemu Informatycznego zobowiązany jest zmienić główne hasło administratora nie rzadziej niż raz na pół roku.

2. Zabrania się ciągłej pracy na koncie administratora (supervisora).
3. Hasło składa się co najmniej z 8 znaków, zawiera małe i wielkie litery oraz cyfry i znaki specjalne.
4. Niezwłocznie po dokonaniu zmiany haseł administratora, Administrator Systemu Informatycznego spisuje hasło, umieszcza w zamkniętej kopercie i przetrzymuje je w sejfie w pomieszczeniu serwerowni.
5. Zarejestrowane hasła administratora, oprócz treści hasła winny posiadać adnotację o dacie ich wprowadzenia do systemu oraz być przechowywane przez okres 12 miesięcy.
6. W przypadku utraty uprawnień przez osobę administrującą systemem należy niezwłocznie zmienić hasła, do których miała dostęp.

Rozdział IV
Procedura rozpoczęcia, zawieszenia i zakończenia pracy w systemie

§ 6.1. Rozpoczęcie pracy na stacji roboczej następuje po uruchomieniu komputera, a następnie wprowadzeniu indywidualnego identyfikatora i hasła.
2. Przed osobami nieupoważnionymi należy chronić ekrany komputerów, wydruki leżące na biurkach oraz w otwartych szafach.
2. Monitory komputerów są wyposażone we włączające się po 15 minutach od przerwania pracy wygaszacze ekranu. Wznowienie wyświetlenia następuje dopiero po wprowadzeniu hasła użytkownika.
3. W przypadku opuszczenia stanowiska pracy użytkownik zobowiązany jest aktywizować wygaszacz ekranu, wylogować się z sytemu operacyjnego lub zablokować w inny sposób stację roboczą.
4. Zakończenie pracy na stacji roboczej następuje po dokładnym zapisaniu wszystkich danych, a następnie prawidłowym wylogowaniu się użytkownika i wyłączeniu komputera.

Rozdział V
Procedura tworzenia kopii zapasowych oraz sposób postępowania z nośnikami

§ 7.1. Za tworzenie i przechowywanie kopii zapasowych odpowiedzialny jest Administrator Systemu Informatycznego lub osoba wyznaczona według ustalonego harmonogramu.
2. Całościowe kopie zapasowe systemów przetwarzających dane osobowe sporządzane są codziennie. Zapis odbywa się poza godzinami pracy.
3. Kopie o których mowa w § 7.2 sporządzane są w dwóch egzemplarzach i przechowywane w dwóch różnych pomieszczeniach. Kopia nr 1 przechowywana jest w pomieszczeniach serwerowni. Kopia nr 2 przechowywana i zabezpieczona jest w pokojach informatyków.
4. Poszczególne kopie zapasowe oznaczane są w sposób umożliwiający określenie daty utworzenia kopii oraz nazwy systemu.
5. Nośniki z kopiami zapasowymi przechowywane są w szafach metalowych.
6. Administrator Systemu Informatycznego odpowiada za prowadzenie ewidencji wykonania kopii zapasowych. Ewidencja może być prowadzona elektronicznie.
7. Czas przechowywania poszczególnych kopii zapasowych, wynosi nie mniej niż 6 miesięcy.
8. W przypadku awarii systemu informatycznego za realizację działań odtworzeniowych odpowiada Administrator Systemu Informatycznego. Po odtworzeniu systemu informatycznego Administrator Systemu Informatycznego odpowiedzialny jest za przeprowadzenie testów poprawności działania systemu przed jego oddaniem do użytkowania.
9. Przeprowadza się czasową weryfikację możliwości odtworzenia danych zapisanych na kopiach zapasowych nie rzadziej niż raz na rok.
§ 8. 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. 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 specjalistycznych narzędzi, a w przypadku nośników optycznych stosuje się niszczenie w niszczarkach.

3. Przenośne elektroniczne nośniki informacji zawierające dane osobowe są przechowywane przez pracowników w sposób minimalizujący ryzyko ich uszkodzenia lub zniszczenia, w szczególności w zamykanych na klucz szafach.

4. W przypadku wycofania sprzętu komputerowego z użycia dane osobowe na nim zapisane są kasowane przy użyciu dedykowanego oprogramowania do bezpiecznego usuwania danych. W przypadku braku możliwości programowego usunięcia danych dysk podlega fizycznemu zniszczeniu.

5. Niszczenia elektronicznych nośników dokonuje Administrator Systemu. Zniszczenie nośnika potwierdzane jest odpowiednim protokołem przechowywanym przez Administratora Systemu Informatycznego.

6. Dopuszcza się powierzenie niszczenia nośników danych wyspecjalizowanym podmiotom zewnętrznym, pod warunkiem:

1) zawarcia umowy powierzenia przetwarzania danych,
2) zagwarantowania poufności danych przez usługodawcę,
3) umożliwienia prowadzenia nadzoru nad procesem niszczenia nośników przez IOD,
4) udokumentowania faktu zniszczenia nośników protokołem.

Rozdział VI
Sposób zabezpieczenia systemu informatycznego

§ 9.1. W celu zabezpieczenia systemu informatycznego przed działaniem niebezpiecznego oprogramowania zabrania się:

1) instalowania i uruchamiania jakiegokolwiek oprogramowania, które nie zostało zatwierdzone do użytku;
2) samowolnego korzystania z prywatnych nośników przenośnych;
3) otwierania poczty elektronicznej, której tytuł nie sugeruje związku z pełnionymi obowiązkami służbowymi - w przypadkach wątpliwych należy skonsultować się z Administratorem Systemu Informatycznego;
4) korzystania z Internetu w celach nie związanych z pełnionymi obowiązkami służbowymi;
5) podłączania komputerów do sieci zewnętrznych za pośrednictwem modemów.

2. W przypadku zauważenia objawów mogących wskazywać na obecność niebezpiecznego oprogramowania użytkownik zobowiązany jest niezwłocznie powiadomić Administratora Systemu Informatycznego. Do objawów powyższych można w szczególności zaliczyć:

1) istotne spowolnienie działania systemu informatycznego,
2) nietypowe działanie aplikacji,
3) nietypowe komunikaty,
4) utratę danych lub modyfikację danych.

3. System informatyczny jest zabezpieczony przed działaniem niebezpiecznego oprogramowania poprzez:

1) oprogramowanie antywirusowe,
2) zaporę sieciową,
3) aktualizację oprogramowania systemowego,
4) konfigurację oprogramowania minimalizującą ryzyko naruszenia bezpieczeństwa,
5) monitoring styku sieci wewnętrznej z ogólnodostępną siecią informatyczną.

4. Administrator Systemu Informatycznego jest odpowiedzialny za nadzór nad działaniem powyższych zabezpieczeń, a w szczególności za:

1) weryfikację aktualności sygnatur systemu antywirusowego i podejmowanie ewentualnych działań korekcyjnych,
2) weryfikację logów systemu antywirusowego i podejmowanie działań korekcyjnych,
3) przegląd logów zapory sieciowej oraz podejmowanie działań mających na celu zablokowanie ataków sieciowych,
4) weryfikację poprawności aktualizacji oprogramowania systemowego.

Rozdział VII
Procedura korzystania z Internetu i poczty elektronicznej

§ 10.1. Użytkownicy posiadający uprawnienia do korzystania z sieci Internetu zobowiązani są do przestrzegania następujących zasad:

1) zakazuje się pobierania przez użytkowników plików lub przeglądania zasobów informacyjnych o treści nie związanej z wykonywaną pracą, w szczególności prawnie zabronionej.
2) do wymiany korespondencji elektronicznej wykorzystywana może być wyłącznie służbowa poczta elektroniczna administratora danych,
3) użytkownik ponosi odpowiedzialność za szkody spowodowane przez oprogramowanie samowolnie przez niego zainstalowane,
4) do korzystania z Internetu użytkownicy mogą wykorzystywać jedynie zaakceptowane przez Administratora Systemu Informatycznego formy dostępu,
5) Administrator Systemu Informatycznego stosuje mechanizmy monitorujące przeglądanie stron internetowych przez użytkowników. Uwzględniają one:
   - blokowanie stron internetowych określonego typu;
   - blokowanie określonych stron internetowych;
   - analizę przesyłanych informacji.

§ 11.1. Użytkownicy poczty elektronicznej zobowiązani są do przestrzegania następujących zasad:

1) przesyłanie informacji za pośrednictwem poczty elektronicznej winno odbywać się zgodnie z uprawnieniami adresatów do korzystania z określonego typu danych,
2) w przypadku wątpliwości nadawca powinien sprawdzić, czy dana osoba ma uprawnienia do korzystania z dokumentów danego typu lub o określonej klauzuli poprzez skonsultowanie się z Administratorem Systemu Informatycznego,
3) użytkownicy powinni zwrócić szczególną uwagę na poprawność adresu odbiorcy dokumentu,
4) w przypadku przesyłania danych osobowych należy wykorzystywać mechanizmy kryptograficzne,
5) zabrania się przesyłania za pośrednictwem poczty elektronicznej informacji niezgodnych z prawem,
6) użytkownicy nie powinni otwierać przesyłek od nieznanych sobie osób, których tytuł nie sugeruje związku z wypełnianymi przez nich obowiązkami służbowymi. W przypadku otrzymania takiej przesyłki, użytkownik powinien ją usunąć lub skontaktować się z Administratorem Systemu Informatycznego,
7) użytkownicy nie powinni uruchamiać wykonywalnych załączników dołączonych do wiadomości przesyłanych pocztą elektroniczną. W takim przypadku użytkownik powinien poinformować o zdarzeniu Administratora Systemu Informatycznego, który winien sprawdzić, czy załącznik stanowi zagrożenie dla przetwarzanych w systemie informatycznym informacji.

§ 12.1. Zabrania się użytkownikom przesyłania jakichkolwiek zbiorów danych za pośrednictwem poczty elektronicznej bez zgody Administratora Systemu Informatycznego.

2. Przesyłanie zbiorów danych za pośrednictwem poczty elektronicznej możliwe jest wyłącznie po zastosowaniu mechanizmów kryptograficznych.

Rozdział VIII
Procedura wykonywania przeglądu i konserwacji systemów

§ 13.1. Przegląd i konserwacja sprzętu informatycznego realizowane są przez Administratora Systemu Informatycznego lub podmioty zewnętrzne.

2. Prace serwisowe wykonywane przez podmioty zewnętrzne podlegają bezpośredniemu nadzorowi Administratora Systemu Informatycznego.

3. Przekazanie sprzętu komputerowego do naprawy poza siedzibę administratora danych jest dopuszczalne, jeżeli spełnione zostaną poniższe warunki:

1) sprzęt przekazywany jest bez nośników zawierających dane osobowe, zaś fakt usunięcia nośników danych lub stwierdzenia braku nośników danych jest potwierdzany protokołem,
2) przekazanie sprzętu potwierdzane jest protokołem, pozwalającym na jednoznaczne wskazanie osoby przekazującej i osoby odbierającej sprzęt.
3) Protokoły, o których mowa w punkcie 3, lub ich kopie przechowywane są przez IOD.

4. Wszelkie prace serwisowe wykonywane przez podmioty zewnętrzne wymagają sporządzenia protokołu serwisowego, zawierającego co najmniej poniższe informacje:

1) wskazanie osoby przeprowadzającej prace serwisowe oraz podmiotu,
2) wskazanie osoby nadzorującej przebieg prac serwisowych,
3) przedmiot prac serwisowych,
4) zakres prac serwisowych i ich wynik,
5) czas przeprowadzania prac serwisowych.

Rozdział IX
Postanowienia końcowe

§. 14. W sprawach nieokreślonych niniejszą instrukcją należy stosować instrukcje obsługi i zalecenia producentów aktualnie wykorzystywanych urządzeń i programów.

§. 15. Każda osoba upoważniona do przetwarzania danych osobowych jest zobowiązana zapoznać się z zasadami wynikającymi z niniejszego dokumentu.

WÓJT
Krzysztof Gajewski