WÓJT GMINY
Zbójno
woj. kujawsko-pomorskie

Zarządzenie nr 1/2016
Wójta Gminy Zbójno

z dnia 5 stycznia 2016 r.

w sprawie przyjęcia polityki bezpieczeństwa danych osobowych przetwarzanych w Urzędzie Gminy Zbójno oraz instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Zbójno

Na podstawie §3 ust.1, 2 i 3 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz.1024), zarządzam:

§1.1. Przyjąć politykę bezpieczeństwa danych osobowych przetwarzanych w Urzędzie Gminy Zbójno (*zwaną dalej polityką bezpieczeństwa*) stanowiącą załącznik nr 1 do niniejszego zarządzenia, z wyjątkiem załączników nr 3, pn. „ Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych" oraz nr 8, pn." Struktura zbiorów danych oraz sposób przepływu danych w systemie", stanowiących załączniki do polityki bezpieczeństwa.

2. Załączniki nr 3 i nr 8 do polityki bezpieczeństwa, o których mowa w ust. 1, zostaną opracowane i przyjęte odrębnym zarządzeniem w terminie do dnia 29 lutego 2016 r.

§2. Przyjąć instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Zbójno (*zwaną dalej instrukcją*) stanowiącą załącznik nr 2 do niniejszego zarządzenia.

§3. Zobowiązuję wszystkich pracowników Urzędu Gminy Zbójno do zapoznania się z treścią polityki bezpieczeństwa i instrukcji oraz zobowiązuje ich do przestrzegania ich postanowień.

§4. Monitorowanie i nadzorowanie wykonania niniejszego zarządzenia powierzam administratorowi bezpieczeństwa informacji.

§5. Zarządzenie wchodzi w życie w dniu 18 stycznia 2016 r.

§6. Z dniem wejścia w życie niniejszego zarządzenia tracą moc wszystkie obowiązujące w Urzędzie Gminy Zbójno procedury wewnętrzne dotyczące ochrony danych osobowych, w tym polityka bezpieczeństwa oraz instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

WÓJT
mgr Katarzyna Kukielska

Załącznik nr 1 do zarządzenia nr 1/2016 Wójta Gminy Zbójno z dnia 5 stycznia 2016 r. w sprawie przyjęcia polityki bezpieczeństwa danych osobowych przetwarzanych w Urzędzie Gminy Zbójno oraz instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Zbójno.

Polityka bezpieczeństwa danych osobowych przetwarzanych w Urzędzie Gminy Zbójno

ROZDZIAŁ I
Wstęp

Wójt Gminy Zbójno, świadomy wagi zagrożeń prywatności, w tym zwłaszcza zagrożeń dla danych osobowych przetwarzanych w związku z wykonywaniem zadań administratora danych osobowych, deklaruje podejmowanie wszelkich możliwych działań koniecznych do zapobiegania zagrożeniom, m. in. takim jak:

1) sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu, jak np. pożar, zalanie pomieszczeń, katastrofa budowlana, napad, kradzież, włamanie, działania terrorystyczne, niepożądana ingerencja ekipy remontowej;

2) niewłaściwe parametry środowiska zakłócające pracę urządzeń komputerowych (nadmierna wilgotność lub bardzo wysoka temperatura, oddziaływanie pola elektromagnetycznego i inne);

3) awarie sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne naruszenia ochrony danych, niewłaściwe działanie serwisantów, w tym pozostawienie serwisantów bez nadzoru, a także przyzwolenie na naprawę sprzętu zawierającego dane poza siedzibą administratora danych;

4) podejmowanie pracy w systemie z przełamaniem lub zaniechaniem stosowania procedur ochrony danych, np. praca osoby, która nie jest upoważniona do przetwarzania danych osobowych, próby stosowania nie swojego hasła i identyfikatora przez osoby upoważnione;

5) celowe lub przypadkowe rozproszenie danych w Internecie z ominięciem zabezpieczeń systemu lub wykorzystaniem błędów systemu informatycznego administratora danych;

6) ataki z Internetu;

7) naruszenia zasad i procedur określonych w dokumentacji z zakresu ochrony danych osobowych przez osoby upoważnione do przetwarzania danych osobowych, związane z nieprzestrzeganiem procedur ochrony danych, w tym zwłaszcza:

a) niezgodne z procedurami zakończenie pracy lub opuszczenie stanowiska pracy (nieprawidłowe wyłączenie komputera, niezablokowanie wyświetlenia treści pracy na ekranie komputera przed tymczasowym opuszczeniem stanowiska pracy, pozostawienie po zakończeniu pracy nieschowanych do zamykanych na klucz szaf i biurek dokumentów zawierających dane osobowe, niezamknięcie na klucz biura po jego opuszczeniu, nieoddanie klucza do sekretariatu);

b) naruszenie bezpieczeństwa danych osobowych przez nieautoryzowane ich przetwarzanie;

c) ujawnienie osobom nieupoważnionym procedur ochrony danych osobowych stosowanych u administratora danych;

d) ujawnienie osobom nieupoważnionym danych przetwarzanych przez administratora danych, w

tym również nieumyślne ujawnienie danych osobom postronnym, przebywającym bez nadzoru lub niedostatecznie nadzorowanym w pomieszczeniach administratora danych;

e) niewykonywanie stosownych kopii zapasowych;

trona | 2 f) przetwarzanie danych osobowych w celach prywatnych;

g) wprowadzanie zmian do systemu informatycznego administratora danych i instalowanie programów bez zgody administratora systemu.

ROZDZIAŁ II

Postanowienia ogólne

1. Definicje.

Ilekroć w polityce bezpieczeństwa danych osobowych przetwarzanych w Urzędzie Gminy Zbójno mowa jest o:

1) **polityce bezpieczeństwa** – rozumie się przez to politykę bezpieczeństwa danych osobowych przetwarzanych w Urzędzie Gminy Zbójno;

2) **instrukcji** – rozumie się przez to instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Zbójno;

3) **administratorze danych osobowych** – rozumie się przez to Gminę Zbójno reprezentowaną przez Wójta Gminy Zbójno;

4) **urzędzie** – rozumie się przez to Urząd Gminy Zbójno;

5) **administratorze bezpieczeństwa informacji** – rozumie się przez to osobę, którą administrator danych osobowych wyznaczył na administratora bezpieczeństwa informacji w Urzędzie Gminy Zbójno;

6) **administratorze systemu** – rozumie się przez to osobę, którą administrator danych osobowych wyznaczył na administratora systemu informatycznego w Urzędzie Gminy Zbójno;

7) **haśle** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znanych jedynie osobie uprawnionej do pracy w systemie informatycznym;

8) **identyfikatorze użytkownika** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;

9) **integralności danych** – rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;

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

a) osoby, której dane dotyczą,

b) osoby upoważnionej do przetwarzania danych,

c) przedstawiciela, o którym mowa w art. 31a ustawy,

d) podmiotu, o którym mowa w art. 31 ustawy,

e) organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem;

11) **osobie upoważnionej do przetwarzania danych osobowych** – rozumie się przez to osobę

Lub

zarówno zatrudnioną na podstawie umowy o pracę, powołania, wyboru, umów cywilno-prawnych, jak i innych, np. praktykantów, stażystów, pracowników interwencyjnych, którzy upoważnieni zostali pisemnie przez administratora danych osobowych do przetwarzania danych osobowych;

12) **kierownikach działów** – rozumie się przez to kierowników wydziałów lub innych wewnętrznych komórek organizacyjnych oraz pracowników zatrudnionych na samodzielnych stanowiskach pracy w Urzędzie Gminy Zbójno;

13) **osoby sprzątające po godzinach pracy urząd** – rozumie się przez to sprzątaczki, pracowników gospodarczych i stażystów zajmujących się utrzymaniem czystości i porządku w Urzędzie Gminy Zbójno;

14) **poufności danych** – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom;

15) **raporcie** – rozumie się przez to przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzanych danych;

16) **rozliczalności** – rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;

17) **rozporządzeniu** – rozumie się przez to rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U nr 100, poz. 1024);

18) **sieci publicznej** – rozumie się przez to sieć publiczną w rozumieniu ustawy Prawo telekomunikacyjne;

19) **sieci telekomunikacyjnej** – rozumie się przez to sieć telekomunikacyjną w rozumieniu ustawy Prawo telekomunikacyjne;

20) **serwisancie** – rozumie się przez to firmę lub pracownika firmy zajmującej się sprzedażą, instalacją, naprawą i konserwacją sprzętu komputerowego;

21) **systemie informatycznym administratora danych osobowych** – rozumie się przez to sprzęt komputerowy, oprogramowanie, dane eksploatowane w zespole współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych;

22) **teletransmisji** – rozumie się przez to przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej;

23) **ustawie** – rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jedn. Dz. U z 2002 r. nr 101, poz. 926 ze zm.);

24) **uwierzytelnianiu** – rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;

25) **użytkowniku** – rozumie się przez to osobę upoważnioną do przetwarzania danych osobowych, której nadano identyfikator i przyznano hasło;

26) **przetwarzaniu danych** – rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych;

27) **zabezpieczeniu danych w systemie informatycznym** – rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;

28) **zbiorze danych** – rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępny według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie;

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

a) osoby, której dane dotyczą,

b) osoby upoważnionej do przetwarzania danych,

c) przedstawiciela, o którym mowa w art. 31a ustawy,

d) podmiotu, o którym mowa w art. 31 ustawy,

e) organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem;

30) **zasadach ochrony danych osobowych** – rozumie się przez to zasady i przepisy w zakresie ochrony danych osobowych wynikające z ustawy, rozporządzenia, polityki bezpieczeństwa oraz instrukcji.

2. Cel.

1.Wdrożenie polityki bezpieczeństwa u administratora danych osobowych ma na celu zabezpieczenie przetwarzanych przez niego danych osobowych, w tym danych przetwarzanych w systemie informatycznym i poza nim, poprzez wykonanie obowiązków wynikających z ustawy i rozporządzenia.

2. W związku z tym, że system informatyczny administratora danych osobowych jest połączony z siecią publiczną, niniejsza polityka bezpieczeństwa służy zapewnieniu wysokiego poziomu bezpieczeństwa danych w rozumieniu §6 rozporządzenia. Niniejszy dokument opisuje niezbędny do uzyskania tego bezpieczeństwa zbiór procedur i zasad dotyczących przetwarzania danych osobowych oraz ich zabezpieczenia.

3. Zakres stosowania.

1. Polityka bezpieczeństwa dotyczy zarówno danych osobowych przetwarzanych w sposób tradycyjny, tj. w formie papierowej jak i w systemach informatycznych.

2. Polityka bezpieczeństwa obowiązuje w Urzędzie Gminy Zbójno.

3. Procedury i zasady określone w polityce bezpieczeństwa stosuje się do wszystkich osób, zarówno zatrudnionych na podstawie umowy o pracę, powołania, wyboru, umów cywilno-prawnych, jak i innych, np. praktykantów, stażystów, pracowników interwencyjnych i robotników publicznych.

ROZDZIAŁ III

Organizacja ochrony danych osobowych

1. Administrator danych osobowych.

Administrator danych osobowych realizuje zadania w zakresie ochrony danych osobowych, w tym

zwłaszcza:

1) stosuje środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności zabezpiecza dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem;

2) podejmuje decyzje o celach i środkach przetwarzania danych osobowych z uwzględnieniem, przede wszystkim, zmian w obowiązującym prawie, organizacji administratora danych osobowych oraz technik zabezpieczenia danych osobowych;

3) upoważnia poszczególne osoby do przetwarzania danych osobowych w określonym indywidualnie zakresie, odpowiadającym zakresowi ich zadań i obowiązków, według wzoru stanowiącego załącznik nr 1 do polityki bezpieczeństwa;

4) wyznacza administratora bezpieczeństwa informacji i administratora systemu oraz ich zastępców, w tym określa zakres ich zadań i obowiązków;

5) zleca administratorowi bezpieczeństwa informacji i administratorowi systemu by zapewnili użytkownikom odpowiednie stanowiska pracy umożliwiające bezpieczne przetwarzanie danych osobowych;

6) podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia procedur bezpiecznego przetwarzania danych osobowych.

2. Administrator bezpieczeństwa informacji.

Administrator bezpieczeństwa informacji zapewnia przestrzeganie przepisów o ochronie danych osobowych w urzędzie, w szczególności przez:

1) sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania dla administratora danych osobowych;

2) nadzorowanie opracowania i aktualizowania dokumentacji, opisującej sposób przetwarzania danych osobowych oraz stosowane środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną;

3) zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych;

4) prowadzenie rejestru zbiorów danych osobowych przetwarzanych przez administratora danych osobowych, z wyjątkiem zbiorów, o których mowa w art. 43 ust. 1 ustawy;

5) prowadzenie szkoleń dla osób upoważnianych do przetwarzania danych osobowych;

6) wystawianie zaświadczeń potwierdzających odbycie szkoleń, o których mowa w pkt 5, według wzoru stanowiącego załącznik nr 2 do polityki bezpieczeństwa.

3. Administrator systemu.

Administrator systemu realizuje zadania w zakresie zarządzania i bieżącego nadzoru nad funkcjonowaniem systemu informatycznego administratora danych osobowych, w tym zwłaszcza:

1) zarządza systemem informatycznym w którym przetwarzane są dane osobowe posługując się

hasłem dostępu do wszystkich stacji roboczych z pozycji administratora;

2) przeciwdziała dostępowi osób niepowołanych do systemu informatycznego, w którym przetwarzane są dane osobowe;

3) na wniosek administratora bezpieczeństwa informacji, przydziela każdemu użytkownikowi identyfikator oraz hasło do systemu informatycznego oraz dokonuje ewentualnych modyfikacji uprawnień, a także usuwa konta użytkowników zgodnie z zasadami określonymi w instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych;

4) nadzoruje działanie mechanizmów uwierzytelniania użytkowników oraz kontroli dostępu do danych osobowych;

5) sprawuje nadzór nad wdrożeniem i funkcjonowaniem stosownych środków technicznych w celu zapewnienia bezpieczeństwa danych;

6) podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia zabezpieczeń systemu informatycznego;

7) podejmuje działania w zakresie ustalania i kontroli identyfikatorów dostępu do systemu informatycznego;

8) wyrejestrowuje użytkowników na polecenie administratora danych osobowych lub administratora bezpieczeństwa informacji;

9) zmienia na poszczególnych stacjach roboczych hasła dostępu ujawniając je wyłącznie danemu użytkownikowi oraz, w razie potrzeby, administratorowi bezpieczeństwa informacji lub administratorowi danych osobowych;

10) w sytuacji stwierdzenia naruszenia zabezpieczeń systemu informatycznego, informuje administratora bezpieczeństwa informacji o naruszeniu i współdziała z nimi przy usuwaniu skutków naruszenia;

11) prowadzi szczegółową dokumentację naruszeń bezpieczeństwa danych osobowych przetwarzanych w systemie informatycznym;

12) sprawuje nadzór nad wykonywaniem napraw, konserwacji oraz likwidacji urządzeń komputerowych i nośników danych na których zapisane są dane osobowe;

13) wykonuje kopie zapasowe, dba o ich właściwe zabezpieczenie i przechowywanie oraz okresowo sprawdza je pod kątem ich dalszej przydatności do odtwarzania;

14) podejmuje działania służące zapewnieniu niezawodności zasilania komputerów, innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych oraz bezpiecznej wymiany danych w sieci wewnętrznej i bezpiecznej teletransmisji.

4. Kierownicy działów.

Kierownicy działów nadzorują i kontrolują przestrzeganie zasad ochrony danych osobowych przez pracowników zatrudnionych w podległym im dziale oraz przez podmioty zewnętrzne realizujące na rzecz urzędu zadania w zakresie spraw prowadzonych przez dział, jeżeli w celu realizacji tych zadań podmioty te przetwarzają dane osobowe powierzone im przez urząd, w tym zwłaszcza:

1) sprawują nadzór nad stosowaniem przez pracowników i podmioty zewnętrzne odpowiednich środków technicznych, fizycznych i organizacyjnych w zakresie ochrony danych osobowych;

2) zgłaszają administratorowi bezpieczeństwa informacji wnioski i uwagi co do sposobu usprawnienia zabezpieczenia danych osobowych przetwarzanych w dziale;

3) kontrolują pracowników w zakresie należytego zabezpieczania szaf i biurek, w których gromadzone są dane osobowe; sprzątania biurek i innego umeblowania z dokumentów zawierających dane osobowe – poprzez ich odpowiednie zabezpieczenie w zamykanych na klucz szafach lub biurkach, lub zniszczenie - w przypadku braku przydatności do dalszego korzystania, w niszczarce;

4) przeciwdziałają dostępowi do zbiorów danych osobowych pracowników i podmiotów zewnętrznych, którzy nie mają odpowiedniego upoważnienia do przetwarzania danych osobowych.

5. Pracownicy upoważnieni do przetwarzania danych osobowych.

Pracownicy upoważnieni do przetwarzania danych osobowych są zobowiązani przestrzegać zasad ochrony danych osobowych, w tym w szczególności:

1) mogą przetwarzać dane osobowe wyłącznie w zakresie ustalonym indywidualnie przez administratora danych osobowych w upoważnieniu i tylko w celu wykonywania nałożonych na nich obowiązków; zakres dostępu do danych przypisany jest do niepowtarzalnego identyfikatora użytkownika, niezbędnego do rozpoczęcia pracy w systemie; rozwiązanie stosunku pracy, odwołanie z pełnionej funkcji powoduje wygaśnięcie upoważnienia do przetwarzania danych osobowych;

2) muszą zachować tajemnicę danych osobowych oraz przestrzegać procedur ich bezpiecznego przetwarzania; przestrzeganie tajemnicy danych osobowych obowiązuje przez cały okres zatrudnienia u administratora danych, a także po ustaniu stosunku pracy lub odwołaniu z pełnionej funkcji;

3) zapoznają się z przepisami prawa w zakresie ochrony danych osobowych oraz postanowieniami niniejszej polityki bezpieczeństwa i instrukcji;

4) stosują określone przez administratora danych osobowych procedury oraz wytyczne mające na celu zgodne z prawem, w tym zwłaszcza adekwatne, przetwarzanie danych osobowych;

5) korzystają z systemu informatycznego w sposób zgodny ze wskazówkami zawartymi w instrukcjach obsługi urządzeń wchodzących w skład tego systemu;

6) zabezpieczają dane przed ich udostępnianiem osobom nieupoważnionym.

6. Pracownicy sprzątający po godzinach pracy urząd.

Pracownicy sprzątający po godzinach pracy urząd, realizują następujące zadania w zakresie ochrony danych osobowych:

1) sprawdzają czy szafy i biurka, w których gromadzone są zbiory danych osobowych, zamknięte są na klucz; w przypadku braku należytego zabezpieczenia, niezwłocznie zgłaszają ten fakt administratorowi bezpieczeństwa informacji;

2) sprawdzają czy na szafkach i biurkach lub innych ogólnie dostępnych miejscach nie znajdują się pozostawione przez pracowników dokumenty, które mogą zawierać dane osobowe; w przypadku stwierdzenia, że doszło do pozostawienia dokumentów i ich nienależytego zabezpieczenia, zgłaszają ten fakt administratorowi bezpieczeństwa informacji.

7. Pracownik prowadzący rejestr wniosków o udostępnienie danych osobowych.

Pracownik prowadzący rejestr wniosków o udostępnienie danych osobowych wpisuje do rejestru każdy wniosek o udostępnienie danych osobowych wpływający do urzędu oraz udzieloną na nią odpowiedź.

ROZDZIAŁ IV

Infrastruktura przetwarzania danych osobowych

1. Obszar przetwarzania danych osobowych.

Wykaz budynków i pomieszczeń wchodzących w skład obszaru w którym przetwarzane są dane osobowe, stanowi załącznik nr 3 do polityki bezpieczeństwa.

2. Zbiory danych.

Wykaz zbiorów danych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych w urzędzie, stanowi załącznik nr 4 do polityki bezpieczeństwa.

3. System informatyczny.

System informatyczny administratora danych osobowych obsługiwany jest przez trzy serwery główne, oraz jeden serwer na którym gromadzone są kopie zapasowe zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania.

4. Ewidencje.

W ramach struktury organizacyjnej administratora danych osobowych prowadzone są następujące ewidencje wchodzące w skład dokumentacji z zakresu ochrony danych osobowych:

1) administrator bezpieczeństwa informacji prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych, według wzoru stanowiącego załącznik nr 5 do polityki bezpieczeństwa;

2) osoba zajmująca się obsługą sekretariatu prowadzi ewidencję wniosków o udostępnienie danych osobowych wpływający do urzędu, według wzoru stanowiącego załącznik nr 6 do polityki bezpieczeństwa;

3) administrator systemu prowadzi ewidencję:

a) serwerów, komputerów, nośników przenośnych oraz kluczy kryptograficznych,

b) oprogramowania komputerowego,

według wzoru stanowiącego załącznik nr 7 do polityki bezpieczeństwa.

ROZDZIAŁ V

Struktura zbiorów danych oraz sposób przepływu danych w systemie

Struktura zbiorów danych osobowych oraz sposób przepływu danych w systemie, stanowi załącznik nr 8 do polityki bezpieczeństwa.

1. Poziom bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym.

Ze względu na fakt, że system informatyczny administratora danych osobowych połączony jest z siecią publiczną, zgodnie z §6 rozporządzenia, należy zapewnić wysoki poziom bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym. Wynikające z tego konsekwencje trzeba uwzględnić w instrukcji.

2. Strategia zabezpieczenia danych osobowych (działania niezbędne do zapewnienia poufności,

integralności i rozliczalności przetwarzanych danych osobowych).

Bezpieczeństwo osobowe

Zachowanie poufności

1. Administrator danych osobowych przeprowadza nabór na wolne stanowiska w drodze konkursu. Kandydaci na pracowników są dobierani z uwzględnieniem ich kompetencji merytorycznych, a także kwalifikacji moralnych. Zwraca się uwagę na takie cechy kandydata, jak uczciwość, odpowiedzialność i przewidywalność zachowań.

2. Ryzyko ze strony osób, które potencjalnie mogą w łatwiejszy sposób uzyskać dostęp do danych osobowych (np. osoby sprzątające pomieszczenia administratora danych osobowych), jest minimalizowane przez zobowiązywanie ich do zachowania tajemnicy na podstawie odrębnych, pisemnych oświadczeń.

Szkolenia w zakresie ochrony danych osobowych

1. Administrator bezpieczeństwa informacji organizuje następujące typy szkoleń:

1) szkoli się każdą osobę, która ma zostać upoważniona do przetwarzania danych osobowych;

2) szkolenia wewnętrzne wszystkich osób upoważnionych do przetwarzania danych osobowych przeprowadzane są w przypadku każdej zmiany zasad lub procedur ochrony danych osobowych;

3) przeprowadza się szkolenia dla osób innych niż upoważnione do przetwarzania danych, jeśli pełnione przez nich funkcje wiążą się z zabezpieczeniem danych osobowych;

2.Tematyka szkoleń obejmuje między innymi:

1) przepisy i procedury dotyczące ochrony danych osobowych, sporządzania i przechowywania ich kopii, niszczenia wydruków i zapisów na nośnikach;

2) sposoby ochrony danych osobowych przed osobami postronnymi i procedury udostępniania danych osobom, których one dotyczą;

3) obowiązki osób upoważnionych do przetwarzania danych osobowych;

4) odpowiedzialność za naruszenie obowiązków z zakresu ochrony danych osobowych;

5) zasady i procedury określone w polityce bezpieczeństwa i instrukcji.

Strefy bezpieczeństwa.

1. W siedzibie administratora danych osobowych wydzielono **strefę bezpieczeństwa klasy I**, w której dostęp do informacji zabezpieczony jest wewnętrznymi środkami kontroli. W skład tej strefy wchodzą:

1) pomieszczenie z serwerami, w którym może przebywać wyłącznie administrator systemu i administrator bezpieczeństwa informacji; inne osoby upoważnione do przetwarzania danych osobowych tylko w ich towarzystwie, a osoby postronne w ogóle nie mają dostępu;

2) pomieszczenie wydziału finansowego i gospodarki nieruchomościami z kasą pancerną - kasa (I piętro), w którym mogą przebywać wyłącznie upoważnieni do tego pracownicy ww. wydziału, inne osoby upoważnione do przetwarzania danych osobowych tylko w towarzystwie ww. pracowników, a osoby postronne w ogóle nie mają dostępu.

2. W **strefie bezpieczeństwa klasy II** do danych osobowych mają dostęp wszystkie osoby upoważnione do przetwarzania danych osobowych zgodnie z zakresami upoważnień do ich

przetwarzania, a osoby postronne mogą w niej przebywać tylko w obecności pracownika upoważnionego do przetwarzania danych osobowych. Strefa ta obejmuje wszystkie pozostałe pomieszczenia zaliczone do obszaru przetwarzania danych w siedzibie administratora danych osobowych.

Zabezpieczenie sprzętu.

1. Serwery znajdują się w odrębnym pomieszczeniu zamykanym wzmocnionymi drzwiami z dwoma zamkami, okna do pomieszczenia są okratowane oraz zainstalowany jest system alarmowy. W pomieszczeniu może przebywać wyłącznie administrator bezpieczeństwa informacji i administrator systemu, inne osoby upoważnione do przetwarzania danych osobowych tylko w ich towarzystwie, a osoby postronne w ogóle nie mają dostępu.

2. Administrator systemu instruuje użytkowników jak postępować aby zapewnić prawidłową eksploatację systemu informatycznego.

3. Wszystkie urządzenia systemu informatycznego administratora danych są zasilane za pośrednictwem zasilaczy awaryjnych (UPS).

4. Okablowanie sieciowe zostało zaprojektowane w ten sposób, że dostęp do linii teletransmisyjnych jest możliwy tylko z pomieszczeń zamykanych na klucz. Ponadto kable sieciowe nie krzyżują się z okablowaniem zasilającym, co zapobiega interferencjom.

5. Bieżąca konserwacja i drobne naprawy sprzętu wykorzystywanego do przetwarzania danych osobowych prowadzone są tylko przez administratora systemu. Natomiast poważne naprawy wykonywane przez podmioty zewnętrzny realizowane są po zawarciu z tymi podmiotami odpowiednich umów, których celem jest należyte zabezpieczenie i ochrona danych osobowych w trakcie wykonywania ww. napraw.

6. Administrator systemu dopuszcza konserwowanie i naprawę sprzętu poza siedzibą administratora danych osobowych jedynie po trwałym usunięciu danych osobowych. Zużyty sprzęt służący do przetwarzania danych osobowych może być zbywany dopiero po trwałym usunięciu danych, a urządzenia uszkodzone mogą być przekazywane w celu utylizacji (jeśli trwałe usunięcie danych wymagałoby nadmiernych nakładów ze strony administratora) właściwym podmiotom, z którymi zawiera się odpowiednie umowy.

7. Wszystkie awarie, działania konserwacyjne i naprawy systemu informatycznego są opisywane w stosownych protokołach, podpisywanych przez osoby w tych działaniach uczestniczące, a także przez administratora systemu.

Zabezpieczenia we własnym zakresie.

Niezwykle ważne dla bezpieczeństwa danych osobowych jest bezwzględne przestrzeganie przez każdą osobę upoważnioną do przetwarzania danych osobowych i użytkownika następujących zasad:

1) ustawiania ekranów komputerowych tak, by osoby niepowołane nie mogły oglądać ich zawartości, a zwłaszcza nie naprzeciwko wejścia do pomieszczenia;

2) niepozostawiania bez kontroli dokumentów, nośników danych i sprzętu w hotelach i innych miejscach publicznych oraz w samochodach;

3) dbania o prawidłową wentylację komputerów (nie można zasłaniać kratek wentylatorów

meblami, zasłonami lub stawiać komputerów tuż przy ścianie);

4) niepodłączania do listew podtrzymujących napięcie przeznaczonych dla sprzętu komputerowego innych urządzeń, szczególnie tych łatwo powodujących spięcia (np. grzejniki, czajniki, wentylatory);

5) pilnego strzeżenia akt, dyskietek, pamięci przenośnych i komputerów przenośnych;

6) kasowania po wykorzystaniu danych na dyskach przenośnych;

7) nieużywania powtórnie dokumentów zadrukowanych jednostronnie;

8) niezapisywania hasła wymaganego do uwierzytelnienia się w systemie na papierze lub innym nośniku i pozostawianie ich w łatwo dostępnych miejscach;

9) powstrzymywania się przez osoby upoważnione do przetwarzania danych osobowych od samodzielnej ingerencji w oprogramowanie i konfigurację powierzonego sprzętu (szczególnie komputerów przenośnych), nawet gdy z pozoru mogłoby to usprawnić pracę lub podnieść poziom bezpieczeństwa danych;

10) przestrzegania przez osoby upoważnione do przetwarzania danych osobowych swoich uprawnień w systemie, tj. właściwego korzystania z baz danych, używania tylko własnego identyfikatora i hasła oraz stosowania się do zaleceń administratora systemu i administratora bezpieczeństwa informacji;

11) opuszczania stanowiska pracy dopiero po aktywizowaniu wygaszacza ekranu lub po zablokowaniu stacji roboczej w inny sposób;

12) kopiowania tylko jednostkowych danych (pojedynczych plików); obowiązuje zakaz robienia kopii całych zbiorów danych lub takich ich części, które nie są konieczne do wykonywania obowiązków przez pracownika; jednostkowe dane mogą być kopiowane na nośniki magnetyczne, optyczne i inne po ich zaszyfrowaniu i przechowywane w zamkniętych na klucz szafach; po ustaniu przydatności tych kopii dane należy trwale skasować lub fizycznie zniszczyć nośniki, na których są przechowywane;

13) udostępniania danych osobowych pocztą elektroniczną tylko w postaci zaszyfrowanej;

14) niewynoszenia na jakichkolwiek nośnikach całych zbiorów danych oraz szerokich z nich wypisów, nawet w postaci zaszyfrowanej;

15) wykonywania kopii roboczych danych, na których się właśnie pracuje, tak często, aby zapobiec ich utracie;

16) kończenia pracy na stacji roboczej po wprowadzeniu danych przetwarzanych tego dnia w odpowiednie obszary serwera, a następnie prawidłowym wylogowaniu się użytkownika i wyłączeniu komputera oraz odcięciu napięcia w UPS i listwie;

17) niszczenia w niszczarce lub chowania do szaf lub biurek zamykanych na klucz wszelkich wydruków zawierających dane osobowe przed opuszczeniem miejsca pracy, po zakończeniu dnia pracy;

18) niepozostawiania osób postronnych w pomieszczeniu, w którym przetwarzane są dane osobowe, bez obecności osoby upoważnionej do przetwarzania danych osobowych;

19) zachowania w tajemnicy danych osobowych, w tym także wobec najbliższych;

20) chowania do zamykanych na klucz szaf lub biurek wszelkich akt zawierających dane osobowe przed opuszczeniem miejsca pracy, po zakończeniu dnia pracy;

21) należytym zabezpieczaniu kluczy do szaf i biurek;

22) zamykania okien w razie opadów czy innych zjawisk atmosferycznych, które mogą zagrozić bezpieczeństwu danych osobowych;

23) zamykania okien w razie opuszczenia pomieszczenia, w tym zwłaszcza po zakończeniu dnia pracy;

24) zamykania drzwi do biur na klucz po zakończeniu pracy w danym dniu i złożenia klucza w sekretariacie lub przekazanie sprzątaczce;

25) zabronione jest przebywanie w obszarze przetwarzania danych osobowych po godzinach pracy urzędu bez zgody administratora bezpieczeństwa informacji oraz bezpośredniego przełożonego pracownika.

Postępowanie z nośnikami i ich bezpieczeństwo.

Osoby upoważnione do przetwarzania danych osobowych powinny pamiętać, że:

1) dane z nośników przenośnych niebędących kopiami zapasowymi po wprowadzeniu do systemu informatycznego administratora danych powinny być trwale usuwane z tych nośników przez fizyczne zniszczenie (np. płyty CD-ROM) lub usunięcie danych programem trwale usuwającym pliki; jeśli istnieje uzasadniona konieczność, dane pojedynczych osób (a nie całe zbiory czy szerokie wypisy ze zbiorów) mogą być przechowywane na specjalnie oznaczonych nośnikach; nośniki te muszą być przechowywane w zamkniętych na klucz szafach, nieudostępnianych osobom postronnym; po ustaniu przydatności tych danych nośniki powinny być trwale kasowane lub niszczone;

2) uszkodzone nośniki przed ich wyrzuceniem należy zniszczyć fizycznie w niszczarce służącej do niszczenia nośników;

3) zabrania się powtórnego używania do sporządzania brudnopisów pism jednostronnie zadrukowanych, jeśli zawierają one dane chronione; zaleca się natomiast dwustronne drukowanie brudnopisów pism i sporządzanie dwustronnych dokumentów;

4) po wykorzystaniu wydruki zawierające dane osobowe należy codziennie przed zakończeniem pracy zniszczyć w niszczarce. O ile to możliwe, nie należy przechowywać takich wydruków w czasie dnia na biurku ani też wynosić poza siedzibę administratora danych osobowych.

Wymiana danych i ich bezpieczeństwo.

1. Bezpieczeństwo danych, a w szczególności ich integralność i dostępność, w dużym stopniu zależy od zdyscyplinowanego, codziennego umieszczania danych w wyznaczonych zasobach serwera. Pozwala to – przynajmniej w pewnym stopniu – uniknąć wielokrotnego wprowadzania tych samych danych do systemu informatycznego administratora danych osobowych.

2. Sporządzanie kopii zapasowych następuje w trybie opisanym w §7 instrukcji.

3. Inne wymogi bezpieczeństwa systemowego są określane w instrukcjach obsługi

producentów sprzętu i używanych programów, wskazówkach administratora systemu, administratora bezpieczeństwa informacji oraz w instrukcji.

4. Przed atakami z sieci zewnętrznej wszystkie komputery administratora danych osobowych (w tym także przenośne) chronione są środkami dobranymi przez administratora systemu w porozumieniu z administratorem bezpieczeństwa informacji.

5. Ważne jest, by użytkownicy zwracali uwagę na to, czy urządzenie, na którym pracują, domaga się aktualizacji tych zabezpieczeń. O wszystkich takich przypadkach należy informować administratora systemu oraz umożliwić mu monitorowanie oraz aktualizację środków (urządzeń, programów) bezpieczeństwa.

6. Administrator systemu w porozumieniu z administratorem bezpieczeństwa informacji, dobiera elektroniczne środki ochrony przed atakami z sieci stosownie do pojawiania się nowych zagrożeń (nowe wirusy, robaki, trojany, inne możliwości wdarcia się do systemu), a także stosownie do rozbudowy systemu informatycznego administratora danych osobowych i powiększania bazy danych. Jednocześnie należy zwracać uwagę, czy rozwijający się system zabezpieczeń sam nie wywołuje nowych zagrożeń.

Kontrola dostępu do systemu.

1. Poszczególnym osobom upoważnionym do przetwarzania danych osobowych przydziela się konta opatrzone niepowtarzalnym identyfikatorem, umożliwiające dostęp do danych osobowych, zgodnie z zakresem upoważnienia do ich przetwarzania.

2. Administrator systemu po uprzednim przedłożeniu mu upoważnienia do przetwarzania danych osobowych, przydziela pracownikowi upoważnionemu do przetwarzania danych osobowych konto w systemie informatycznym, dostępne po wprowadzeniu prawidłowego identyfikatora i uwierzytelnieniu hasłem. System wymusza zmianę hasła przy pierwszym logowaniu.

3. W razie potrzeby, po uzyskaniu uprzedniej akceptacji administratora bezpieczeństwa informacji, administrator systemu może przydzielić konto opatrzone identyfikatorem osobie upoważnionej do przetwarzania danych osobowych, nieposiadającej statusu pracownika.

4. Pierwsze hasło wymagane do uwierzytelnienia się w systemie informatycznym przydzielane jest przez administratora systemu.

5. Do zagwarantowania poufności i integralności danych osobowych konieczne jest przestrzeganie przez użytkowników swoich uprawnień w systemie, tj. właściwego korzystania z baz danych, używania tylko własnego identyfikatora i hasła oraz stosowania się do zaleceń administratora systemu i administratora bezpieczeństwa informacji .

Kontrola dostępu do sieci.

1. System informatyczny posiada połączenie z Internetem. Dostęp do niego jest jednak ograniczony.

2. Administrator danych wykorzystuje centralną zaporę sieciową w celu separacji lokalnej sieci od sieci publicznej.

3. Operacje za pośrednictwem rachunku bankowego administratora danych osobowych

może wykonywać wyłącznie pracownik upoważniony przez Wójta, po uwierzytelnieniu się zgodnie z procedurami określonymi przez bank obsługujący rachunek.

Komputery przenośne i praca na odległość.

1. Urządzenia przenośne oraz nośniki danych wynoszone z siedziby administratora danych osobowych nie powinny być pozostawiane bez nadzoru w miejscach publicznych. Komputery przenośne należy przewozić w służbowych torbach; stosowanie własnych charakterystycznych toreb na laptopy nie jest dopuszczalne.

2. Nie należy pozostawiać bez kontroli dokumentów, nośników danych i sprzętu w hotelach i innych miejscach publicznych ani też w samochodach.

3. Informacje przechowywane na urządzeniach przenośnych lub komputerowych nośnikach danych należy chronić przed uszkodzeniami fizycznymi; w przypadku działania silnego pola elektromagnetycznego należy przestrzegać zaleceń producentów dotyczących ochrony sprzętu.

4. Wykorzystywanie komputerów przenośnych administratora danych w miejscach publicznych jest dozwolone, o ile otoczenie, w którym znajduje się użytkownik, stwarza warunki minimalizujące ryzyko zapoznania się z danymi przez osoby nieupoważnione. W konsekwencji korzystanie z komputera przenośnego będzie z reguły niedozwolone w restauracjach czy środkach komunikacji publicznej.

5. W domu niedozwolone jest udostępnianie domownikom komputera przenośnego należącego do administratora danych osobowych. Użytkownik powinien zachować w tajemnicy wobec domowników identyfikator i hasło, których podanie jest konieczne do rozpoczęcia pracy na komputerze przenośnym administratora danych osobowych.

Monitorowanie dostępu do systemu i jego użycia.

1. System informatyczny administratora danych osobowych dzięki funkcjonalności polegającej na monitorowaniu użycia stacji roboczych śledzi, kto, kiedy i jakie programy uruchamia na poszczególnych stacjach roboczych.

2. Administrator systemu przeprowadza synchronizację zegarów stacji roboczych z serwerem, ograniczając dopuszczalność zmian w ustawieniach zegarów. Jakiekolwiek zmiany ustawień zegarów mogą być dokonywane jedynie przez administratora systemu z konta o uprawnieniach administracyjnych.

3. Przeglądy okresowe zapobiegające naruszeniom obowiązku szczególnej staranności administratora danych (art. 26 ust. 1 ustawy).

1. Administrator bezpieczeństwa informacji przeprowadza raz w roku przegląd przetwarzanych danych osobowych pod kątem celowości ich dalszego przetwarzania. Osoby upoważnione do przetwarzania danych osobowych, w tym zwłaszcza kierownicy poszczególnych działów, są obowiązani współpracować z administratorem bezpieczeństwa informacji w tym zakresie i wskazywać mu dane osobowe, które powinny zostać usunięte ze względu na zrealizowanie celu przetwarzania danych osobowych lub brak ich adekwatności do realizowanego celu.

2. Administrator bezpieczeństwa informacji może zarządzić przeprowadzenie dodatkowego

przeglądu w wyżej określonym zakresie w razie zmian w obowiązującym prawie, ograniczających dopuszczalny zakres przetwarzanych danych osobowych. Dodatkowy przegląd jest możliwy także w sytuacji zmian organizacyjnych u administratora danych osobowych.

3. Z przebiegu usuwania danych osobowych należy sporządzić protokół, który podpisuje administrator systemu, administrator bezpieczeństwa informacji i kierownik działu, w którym usunięto dane osobowe.

4. Udostępnianie danych osobowych.

1. Udostępnianie danych osobowych odbiorcom danych może nastąpić wyłącznie na zasadach określonych w ustawie lub w innych ustawach szczególnych.

2. Udostępnianie danych osobowych funkcjonariuszom policji, innych służb lub organom wymiaru sprawiedliwości na podstawie ustaw szczególnych może nastąpić tylko po przedłożeniu wniosku o przekazanie lub udostępnienie danych osobowych. Wniosek ten powinien mieć formę pisemną i zawierać:

1) oznaczenie wnioskodawcy;

2) wskazanie przepisów uprawniających do dostępu do danych osobowych;

3) określenie rodzaju i zakresu potrzebnych danych osobowych oraz formy ich przekazania lub udostępnienia;

4) wskazanie imienia, nazwiska i stopnia służbowego funkcjonariusza upoważnionego do pobrania danych osobowych lub zapoznania się z ich treścią.

3. Udostępnianie danych osobowych na podstawie ustnego wniosku zawierającego wszystkie powyższe cztery elementy wniosku pisemnego może nastąpić tylko wtedy, gdy zachodzi konieczność niezwłocznego działania, np. w trakcie pościgu za osobą podejrzaną o popełnienie czynu zabronionego albo podczas wykonywania czynności mających na celu ratowanie życia lub zdrowia ludzkiego lub mienia.

4. Osoba udostępniająca dane osobowe jest obowiązana zażądać od funkcjonariusza pokwitowania pobrania dokumentów zawierających dane osobowe przekazane na podstawie pisemnego wniosku albo potwierdzenia faktu uzyskania wglądu w treść tych danych. Funkcjonariusz jest obowiązany do pokwitowania lub potwierdzenia tego faktu.

5. Jeśli dane osobowe są przekazywane na podstawie ustnego wniosku, należy stosownie do okoliczności zwrócić się z prośbą o pokwitowanie albo potwierdzenie tego faktu. Jeśli pokwitowanie albo potwierdzenie ze względu na okoliczności udostępniania nie są możliwe, osoba udostępniająca dane osobowe sporządza na tę okoliczność notatkę służbową.

5. Odpowiedzialność osób upoważnionych do przetwarzania danych osobowych.

1. Niezastosowanie się do prowadzonej przez administratora danych osobowych polityki bezpieczeństwa, której założenia określa niniejszy dokument, i naruszenie procedur ochrony danych osobowych przez pracowników upoważnionych do przetwarzania danych osobowych może być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, skutkujące rozwiązaniem stosunku pracy bez wypowiedzenia na podstawie art. 52 ustawy Kodeks pracy.

2. Niezależnie od rozwiązania stosunku pracy osoby popełniające przestępstwo będą

pociągane do odpowiedzialności karnej na podstawie przepisów ustawy o ochronie danych osobowych lub/i ustawy Kodeks karny.

6. Przeglądy polityki bezpieczeństwa i audyty systemu.

1. Polityka bezpieczeństwa powinna być poddawana przeglądowi przynajmniej raz na rok. W razie istotnych zmian dotyczących przetwarzania danych osobowych administrator danych może zarządzić przegląd polityki bezpieczeństwa stosownie do potrzeb.

2. Administrator bezpieczeństwa informacji analizuje, czy polityka bezpieczeństwa i pozostała dokumentacja z zakresu ochrony danych osobowych jest adekwatna do:

1) zmian w budowie systemu informatycznego;

2) zmian organizacyjnych u administratora danych osobowych, w tym również zmian statusu osób upoważnionych do przetwarzania danych osobowych;

3) zmian w obowiązującym prawie.

3. Administrator bezpieczeństwa informacji po uzgodnieniu z Wójtem może, stosownie do potrzeb, przeprowadzić wewnętrzny audyt zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych.

4. Przeprowadzenie audytu wymaga uzgodnienia jego zakresu z administratorem systemu. Zakres, przebieg i rezultaty audytu dokumentowane są w protokole podpisywanym zarówno przez administratora bezpieczeństwa informacji jak i administratora danych osobowych oraz administratora systemu.

5. Wójt, biorąc pod uwagę wnioski administratora bezpieczeństwa informacji, może zlecić przeprowadzenie audytu zewnętrznego przez wyspecjalizowany podmiot.

7. Postanowienia końcowe.

1. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest zapoznać się przed dopuszczeniem jej do przetwarzania danych osobowych z polityką bezpieczeństwa oraz złożyć oświadczenie potwierdzające znajomość jej treści oraz zobowiązanie do przestrzegania jej postanowień, według wzoru stanowiącego załącznik nr 9 do polityki bezpieczeństwa.

2. Osoby, o których mowa w pkt 1, zobowiązane są zachować w tajemnicy dane osobowe do których miały dostęp oraz sposoby ich zabezpieczenia. W tym celu podpisują oświadczenie, według wzoru stanowiącego załącznik nr 10 do polityki bezpieczeństwa.

3. Kierownicy działów zobowiązani są zapoznać z treścią polityki bezpieczeństwa tych pracowników urzędu, którzy nie mają dostępu do komputerów.

4. Niezastosowanie się do procedur określonych w polityce bezpieczeństwa przez pracowników upoważnionych do przetwarzania danych osobowych oraz przez innych pracowników urzędu może być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, skutkujące rozwiązaniem stosunku pracy bez wypowiedzenia na podstawie art. 52 Kodeksu pracy.

5. Niezależnie od rozwiązania stosunku pracy osoby popełniające przestępstwo będą pociągane do odpowiedzialności karnej na podstawie przepisów ustawy o ochronie danych osobowych lub/i ustawy Kodeks karny.

Załącznik nr 1 do polityki bezpieczeństwa danych osobowych przetwarzanych w Urzędzie Gminy Zbójno, przyjętej zarządzeniem nr 1/2016 Wójta Gminy Zbójno z dnia 5 stycznia 2016 r.

Zbójno, dnia .....

.....

(Znak sprawy)

UPOWAŻNIENIE nr .....

Na podstawie art.37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz.926 z późn.zm.) upoważniam:

Panią/Pana* .....

(Imię i nazwisko oraz stanowisko)

(zatrudnioną/zatrudnionego)/(wykonującą/wykonującego umowę numer ..... z dnia .....)*

.....

(Stanowisko i nazwa działu)*

do przetwarzania danych osobowych zgromadzonych w Urzędzie Gminy Zbójno w zakresie niezbędnym do realizacji zadań i wykonywania obowiązków wynikających z aktualnego zakresu obowiązków, czynności, uprawnień i odpowiedzialności oraz posiadanych upoważnień i pełnomocnictw/umowy numer ..... z dnia ..... zawartej w sprawie .....*

Upoważnienie wydaje się na czas trwania stosunku pracy/umowy/stażu/praktyki/do odwołania/na czas określony do dnia* .....

.....

(Podpis osoby reprezentującej administrator danych osobowych)

.....

(Data i podpis upoważnionego)

Otrzymują:

1. Upoważniony;
2. Akta osobowe;
3. Administrator Bezpieczeństwa Informacji.

W załączeniu wyciąg z polityki bezpieczeństwa danych osobowych przetwarzanych w Urzędzie Gminy Zbójno dotyczący obowiązków osób upoważnionych do przetwarzania danych osobowych.

Pouczenie

Osoba upoważniona do przetwarzania danych osobowych jest obowiązana zgodnie z art. 39 ust. 2 ustawy o ochronie danych osobowych zachować w tajemnicy dane osobowe oraz sposoby ich zabezpieczenia, w tym także po ustaniu zatrudnienia/odwołaniu upoważnienia/upływie jego ważności. Ponadto podlega odpowiedzialności karnej wynikającej z art. 51-52 ustawy o ochronie danych osobowych, a także art. 266 Kodeksu karnego.

Załącznik nr 2 do polityki bezpieczeństwa danych osobowych przetwarzanych w Urzędzie Gminy Zbójno, przyjętej zarządzeniem nr 1/2016 Wójta Gminy Zbójno z dnia 5 stycznia 2016 r.

ZAŚWIADCZENIE nr .....
o ukończeniu szkolenia w zakresie ochrony danych osobowych przetwarzanych w Urzędzie[1]

Pan/i: .....
(Imię i nazwisko)

zatrudniony/a w: .....
(Nazwa działu)

na stanowisku: .....
(Nazwa stanowiska pracy)

ukończył/a w dniu ..... szkolenie w zakresie:

„ OCHRONA DANYCH OSOBOWYCH PRZETWARZANYCH W URZĘDZIE GMINY ZBÓJNO "

Celem szkolenia było zapoznanie ww. osoby z przepisami oraz procedurami, zasadami i sposobami ochrony danych osobowych[2] obowiązującymi w Urzędzie.

Szkolenie zorganizował/a i przeprowadził/a .....
(Imię i nazwisko Administratora Bezpieczeństwa Informacji)

Zbójno, dnia .....
(Data wystawienia zaświadczenia)

.....
(Podpis Administratora Bezpieczeństwa Informacji)

Otrzymują:

1. Uczestnik szkolenia.
2. Akta osobowe.
3. Administrator Bezpieczeństwa Informacji.

---

[1] Urzędzie – należy przez to rozumieć Urząd Gminy Zbójno.

[2] Przepisy oraz procedury, zasady i sposoby ochrony danych osobowych wynikające z ustawy o ochronie danych osobowych, polityki bezpieczeństwa danych osobowych przetwarzanych w Urzędzie Gminy Zbójno oraz instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Zbójno.

Załącznik nr 3 do polityki bezpieczeństwa danych osobowych przetwarzanych w Urzędzie Gminy Zbójno, przyjętej zarządzeniem nr 1/2016 Wójta Gminy Zbójno z dnia 5 stycznia 2016 r.

Wykaz budynków i pomieszczeń wchodzących w skład obszaru przetwarzania danych osobowych

Adres	Pomieszczenia
Urząd Gminy Zbójno Zbójno 35 A 87-645 Zbójno	Parter, pomieszczenia nr: 22, 23, 25, 26, 27, 28, 29 I piętro, pomieszczenia nr: 32, 33, 34, 37, 38, 39, 40, 41

Załącznik nr 5 do polityki bezpieczeństwa danych osobowych przetwarzanych w Urzędzie Gminy Zbójno, przyjętej zarządzeniem nr 1/2016 Wójta Gminy Zbójno z dnia 5 stycznia 2016 r.

Ewidencja osób upoważnionych do przetwarzania danych osobowych

Lp.	Imię i nazwisko osoby upoważnionej	Data nadania upoważnienia	Data ustania upoważnienia	Zakres upoważnienia	Identyfikator

Załącznik nr 6 do polityki bezpieczeństwa danych osobowych przetwarzanych w Urzędzie Gminy Zbójno, przyjętej zarządzeniem nr 1/2016 Wójta Gminy Zbójno z dnia 5 stycznia 2016 r.

Ewidencja wniosków o udostępnienie danych osobowych oraz udzielonych na nie odpowiedzi

Lp.	Data wpływu	Nazwa wnioskodawcy	Treść żądania wnioskodawcy	Pracownik odbierający wniosek	Pracownik udzielający odpowiedzi	Data udzielenia odpowiedzi	Znak sprawy

Załącznik nr 7 do polityki bezpieczeństwa danych osobowych przetwarzanych w Urzędzie Gminy Zbójno, przyjętej zarządzeniem nr 1/2016 Wójta Gminy Zbójno z dnia 5 stycznia 2016 r.

Ewidencja oprogramowania komputerowego

Lp.	Nazwa oprogramowania i jego ilość	Dostawca oprogramowania	Przeznaczenie oprogramowania	Okres obowiązywania licencji

Ewidencja serwerów, komputerów, nośników przenośnych i kluczy kryptograficznych

Lp.	Nazwa urządzenia	Numer fabryczny/seria urządzenia	Przeznaczenie urządzenia	Użytkownik

Załącznik nr 9 do polityki bezpieczeństwa danych osobowych przetwarzanych w Urzędzie Gminy Zbójno, przyjętej zarządzeniem nr 1/2016 Wójta Gminy Zbójno z dnia 5 stycznia 2016 r.

Zbójno, dnia .....

OŚWIADCZENIE

Ja niżej podpisany/a* ..... oświadczam, że zapoznałem/am* się z treścią obowiązujących w Urzędzie Gminy Zbójno, w chwili podpisania niniejszego oświadczenia, przepisów oraz procedur, zasad i sposobów ochrony danych osobowych, tj.:

1) polityką bezpieczeństwa danych osobowych przetwarzanych w Urzędzie Gminy Zbójno;
2) instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Zbójno;
3) ustawą o ochronie danych osobowych,

oraz **zobowiązuje się** do przestrzegania ich postanowień.

Ponadto zobowiązuje się do aktualizowania swojej wiedzy w ww. zakresie, w przypadku zmiany postanowień ww. przepisów oraz procedur, zasad i sposobów ochrony danych osobowych.

.....

(Podpis składającego oświadczenie)

Otrzymują:

1. Składający oświadczenie.
2. Akta osobowe.
3. Administrator Bezpieczeństwa Informacji.

* Niepotrzebne skreślić.

Załącznik nr 10 do polityki bezpieczeństwa danych osobowych przetwarzanych w Urzędzie Gminy Zbójno, przyjętej zarządzeniem nr 1/2016 Wójta Gminy Zbójno z dnia 5 stycznia 2016 r.

Zbójno, dnia .....

OŚWIADCZENIE

Ja niżej podpisany/a* ..... zobowiązuję się do zachowania w tajemnicy danych osobowych do których mam/będę miał/a dostęp w związku z wykonywaniem przeze mnie zadań służbowych i obowiązków pracowniczych/stażysty/zobowiązań umownych w Urzędzie Gminy Zbójno, oraz sposobów ich zabezpieczenia, zarówno w trakcie obecnie wiążącego mnie stosunku pracy/umowy/stażu/praktyki[1], jak i po ich ustaniu.

Przyjmuję do wiadomości, że postępowanie sprzeczne z powyższym zobowiązaniami może być potraktowane jako ciężkie naruszenie obowiązków pracowniczych/postanowień umowy[2], skutkujące rozwiązaniem stosunku pracy/umowy[2] bez wypowiedzenia, oraz/lub pociągnięciem do odpowiedzialności karnej na podstawie przepisów ustawy o ochronie danych osobowych lub/i ustawy Kodeks karny.

.....

(Podpis składającego oświadczenie)

Otrzymują:

1. Uczestnik szkolenia.
2. Akta osobowe.
3. Administrator Bezpieczeństwa Informacji.

Załącznik nr 2 do zarządzenia nr 1/2016 Wójta Gminy Zbójno z dnia 5 stycznia 2016 r. w sprawie przyjęcia polityki bezpieczeństwa danych osobowych przetwarzanych w Urzędzie Gminy Zbójno oraz instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Zbójno.

Instrukcja
zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Zbójno

ROZDZIAŁ I
Postanowienia ogólne

§1. Ilekroć w instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Zbójno mowa jest o:

1) **polityce bezpieczeństwa** – rozumie się przez to politykę bezpieczeństwa danych osobowych przetwarzanych w Urzędzie Gminy Zbójno;

2) **instrukcji** – rozumie się przez to instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Zbójno;

3) **administratorze danych osobowych** – rozumie się przez to Gminę Zbójno reprezentowaną przez Wójta Gminy Zbójno;

4) **urzędzie** – rozumie się przez to Urząd Gminy Zbójno;

5) **administratorze bezpieczeństwa informacji** – rozumie się przez to osobę, którą administrator danych osobowych wyznaczył na administratora bezpieczeństwa informacji w Urzędzie Gminy Zbójno;

6) **administratorze systemu** – rozumie się przez to osobę, którą administrator danych osobowych wyznaczył na administratora systemu informatycznego w Urzędzie Gminy Zbójno;

7) **haśle** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znanych jedynie osobie uprawnionej do pracy w systemie informatycznym;

8) **identyfikatorze użytkownika** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;

9) **integralności danych** – rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;

10) **osobie upoważnionej do przetwarzania danych osobowych** – rozumie się przez to osobę zarówno zatrudnioną na podstawie umowy o pracę, powołania, wyboru, umów cywilno-prawnych, jak i innych, np. praktykantów, stażystów, pracowników interwencyjnych, którzy upoważnieni zostali pisemnie przez administratora danych osobowych do przetwarzania danych osobowych;

11) **kierownikach działów** – rozumie się przez to kierowników wydziałów lub innych wewnętrznych komórek organizacyjnych oraz pracowników zatrudnionych na samodzielnych stanowiskach pracy w Urzędzie Gminy Zbójno;

12) **osoby sprzątające po godzinach pracy urząd** – rozumie się przez to sprzątaczki, pracowników gospodarczych i stażystów zajmujących się utrzymaniem czystości i porządku w Urzędzie Gminy Zbójno;

trona | 2

13) **poufności danych** – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom;

14) **raporcie** – rozumie się przez to przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzanych danych;

15) **rozliczalności** – rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;

16) **rozporządzeniu** – rozumie się przez to rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U nr 100, poz. 1024);

17) **sieci publicznej** – rozumie się przez to sieć publiczną w rozumieniu ustawy Prawo telekomunikacyjne;

18) **sieci telekomunikacyjnej** – rozumie się przez to sieć telekomunikacyjną w rozumieniu ustawy Prawo telekomunikacyjne;

19) **serwisancie** – rozumie się przez to firmę lub pracownika firmy zajmującej się sprzedażą, instalacją, naprawą i konserwacją sprzętu komputerowego;

20) **systemie informatycznym administratora danych osobowych** – rozumie się przez to sprzęt komputerowy, oprogramowanie, dane eksploatowane w zespole współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych;

21) **teletransmisji** – rozumie się przez to przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej;

22) **ustawie** – rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jedn. Dz. U z 2002 r. nr 101, poz. 926 ze zm.);

23) **uwierzytelnianiu** – rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;

24) **użytkowniku** – rozumie się przez to osobę upoważnioną do przetwarzania danych osobowych, której nadano identyfikator i przyznano hasło;

25) **przetwarzaniu danych** – rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych;

26) **zabezpieczeniu danych w systemie informatycznym** – rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;

27) **zbiorze danych** – rozumie się przez to każdy posiadający strukturę zestaw danych o

charakterze osobowym, dostępny według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie;

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

a) osoby, której dane dotyczą,

b) osoby upoważnionej do przetwarzania danych,

c) przedstawiciela, o którym mowa w art. 31a ustawy,

d) podmiotu, o którym mowa w art. 31 ustawy,

e) organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem;

29) **zasadach ochrony danych osobowych** – rozumie się przez to zasady i przepisy w zakresie ochrony danych osobowych wynikające z ustawy, rozporządzenia, polityki bezpieczeństwa oraz instrukcji.

§2.1. Instrukcja obowiązuje w Urzędzie Gminy Zbójno.

2. Procedury i zasady określone w instrukcji stosuje się do wszystkich osób upoważnionych do przetwarzania danych osobowych, zarówno zatrudnionych na podstawie umowy o pracę, powołania, wyboru, umów cywilno-prawnych, jak i innych, np. praktykantów, stażystów, pracowników interwencyjnych.

ROZDZIAŁ II

Zabezpieczenie obszaru przetwarzania danych osobowych

§3. Obszar w którym przetwarzane są dane osobowe – określony w polityce bezpieczeństwa, zabezpiecza się przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych, w sposób i na zasadach określonych w polityce bezpieczeństwa.

ROZDZIAŁ III

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

§4.1. Upoważnienia do przetwarzania danych osobowych nadawane są przez administratora danych osobowych na wniosek administratora bezpieczeństwa informacji. Upoważnienia dotyczą zarówno danych osobowych gromadzonych w systemie informatycznym jak również w tradycyjnych rejestrach/ewidencjach/zbiorach papierowych.

2. Zgoda na pracę w systemie informatycznym wymagana jest także dla użytkowników, którzy nie przetwarzają danych osobowych.

3. Wprowadza się ewidencję osób upoważnionych do przetwarzania danych osobowych.

4. Ewidencja, o której mowa w ust.3, prowadzona jest przez administratora bezpieczeństwa informacji.

5. Upoważnienia, o których mowa w ust.1, odbierane są w przypadku ustania stosunku pracy, zakończenia odbywania stażu, praktyki oraz na wniosek administratora bezpieczeństwa informacji.

trona | 4

6. Użytkowników systemu informatycznego tworzy oraz usuwa administrator systemu.

Stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem

§5.1. Każdy użytkownik systemu informatycznego dopuszczony do pracy przy przetwarzaniu danych osobowych powinien posiadać odrębny identyfikator, którego nazwa składa się z pierwszej litery imienia oraz całego nazwiska pisanych jednym ciągiem z małej litery.

2. Wprowadza się obowiązek uwierzytelnienia własnego identyfikatora poprzez podanie hasła.

3. Zmiany hasła należy dokonywać nie rzadziej niż co 30 dni.

4. Hasło składa się z co najmniej 8 znaków, zawiera małe i wielkie litery oraz cyfry lub znaki specjalne.

5. Początkowe hasło dostępu ustala się z administratorem systemu, a następnie samodzielnie zmienia przy użyciu odpowiednich narzędzi informatycznych.

6. Dane osobowe gromadzone są wyłącznie na serwerze. Zabrania się gromadzenia danych osobowych na innych nośnikach danych.

7. W uzasadnionych przypadkach, za zgodą administratora bezpieczeństwa informacji, dane osobowe można przetwarzać poza serwerem.

8. Tworzy się ewidencje serwerów, komputerów, nośników przenośnych i kluczy kryptograficznych, według wzoru określonego w załączniku nr 7 do polityki bezpieczeństwa.

9. Ewidencje, o której mowa w ust. 8 prowadzi administrator systemu.

ROZDZIAŁ IV

Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu

§6.1. Przed przystąpieniem do pracy w systemie informatycznym użytkownik zobowiązany jest sprawdzić urządzenie komputerowe i stanowisko pracy ze szczególnym zwróceniem uwagi czy nie zaszły okoliczności wskazujące na naruszenie zasad ochrony danych osobowych. W przypadku ich naruszenia użytkownik niezwłocznie powiadamia administratora bezpieczeństwa informacji.

2. Użytkownik rozpoczyna pracę w systemie informatycznym od następujących czynności:

1) włączenia komputera;

2) uwierzytelnienia się („zalogowania" w systemie) za pomocą identyfikatora i hasła.

3. Niedopuszczalne jest uwierzytelnianie się na hasło i identyfikator innego użytkownika lub praca w systemie informatycznym na koncie innego użytkownika.

4. Użytkownik systemu informatycznego jest odpowiedzialny za zabezpieczenie danych wyświetlanych przez system informatyczny przed osobami nie mającymi uprawnień.

5. Zakończenie pracy użytkownika w systemie następuje po „wylogowaniu się" z systemu. Po zakończeniu pracy użytkownik zabezpiecza swoje stanowisko pracy, w szczególności dyskietki, dokumenty i wydruki zawierające dane osobowe przed dostępem osób nieupoważnionych, poprzez między innymi umieszczenie ich w zamykanych na klucz szafach lub biurkach. Zbędne pisma, dokumenty i inne materiały zawierające dane osobowe należy zniszczyć w niszczarce.

6. W przypadku dłużej trwającego opuszczenia stanowiska pracy, użytkownik zobowiązany jest „wylogować się" lub zaktywizować wygaszacz ekranu z opcją ponownego „logowania" się do systemu. W przypadku wystąpienia nieprawidłowości w mechanizmie uwierzytelniania („logowaniu się" w systemie), użytkownik niezwłocznie powiadamia o nich administratora systemu.

7. Administrator systemu, monitoruje logowanie oraz wylogowanie się użytkowników oraz nadzoruje zakres przetwarzanych przez nich zbiorów danych.

ROZDZIAŁ V

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

§7.1. Tworzenie kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania znajdujących się na serwerach wykonywane jest co najmniej raz w tygodniu.

2. Kopie zapasowe zbiorów danych, o których mowa w ust. 1, zapisywane są na oddzielnym, wyodrębnionym w tym celu serwerze.

3. Administrator systemu nadzoruje i monitoruje tworzenie kopii zapasowych zbiorów danych, o których mowa w ust. 1.

ROZDZIAŁ VI

Sposób, miejsce i okres przechowywania kopii zapasowych zbiorów danych

§8.1. Serwer, o którym mowa w §7 ust.2 znajduje się w odrębnym pomieszczeniu zamykanym wzmocnionymi drzwiami z dwoma zamkami. Okna do pomieszczenia są okratowane oraz zainstalowany jest system alarmowy. W pomieszczeniu może przebywać wyłącznie administrator systemu i administrator bezpieczeństwa informacji, inne osoby upoważnione do przetwarzania danych osobowych tylko w ich towarzystwie, a osoby postronne w ogóle nie mają dostępu.

2. Nadzór nad prawidłowym przechowywaniem i zabezpieczaniem kopii zapasowych, o których mowa w §7, sprawuje administrator systemu.

3. Kopie zapasowe, o których mowa w §7, usuwa się w sposób trwały po ustaniu ich użyteczności.

4. Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:

1) likwidacji — pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie;

2) przekazania podmiotowi nieuprawnionemu do przetwarzania danych — pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie;

3) naprawy — pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem AS lub osoby przez niego upoważnionej.

5. Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przekazywane poza obszar przetwarzania danych zabezpiecza się w sposób zapewniający poufność i integralność tych danych.

ROZDZIAŁ VII

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

§9.1. System obejmuje się ochroną antywirusową polegającą na skanowaniu serwerów oraz stacji roboczych programem antywirusowym.

2. Skanowanie serwerów i stacji roboczych wykonywane jest automatycznie i na bieżąco.

3. Pocztę elektroniczną przychodzącą na serwer pocztowy skanuje się bezpośrednio w trakcie jej odbierania.

4. Administrator systemu monitoruje skanowanie, o którym mowa w ust. 2 i 3.

5. Przed utratą danych spowodowanych awarią zasilania lub zakłóceniami w sieci zasilającej, system jest chroniony zasilaczami awaryjnymi UPS.

6. Administrator systemu monitoruje stan systemu informatycznego, ruch użytkowników w sieci oraz próby ingerencji z zewnątrz w system informatyczny.

ROZDZIAŁ VIII

Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych

§10.1. Przeglądy i konserwacje systemu informatycznego oraz nośników informacji służących do przetwarzania danych mogą być wykonywane jedynie przez osoby posiadające upoważnienie wydane przez administratora danych osobowych.

2. Prace określone w ust.1 wykonywane są pod nadzorem administratora systemu.

3. Tworzy się ewidencję przeglądów i konserwacji, o której mowa w ust. 1, według wzoru stanowiącego załącznik nr 1 do instrukcji.

4. Ewidencje o której mowa w ust. 3 prowadzi administrator systemu.

ROZDZIAŁ IX

Komunikacja w systemie informatycznym

§11. Wprowadza się następujące zasady korzystania z systemu informatycznego:

1) zabrania się instalowania na komputerach oprogramowania niebędącego własnością urzędu;

kk

2) oprogramowanie na komputerach może być instalowane wyłącznie przez administratora systemu lub za jego zgodą;

3) wszelkie programy i dane zainstalowane na komputerach urzędu stanowią własność urzędu;

4) pracownicy mogą używać połączenia z siecią Internet jedynie w celach służbowych;

5) pracownicy urzędu nie mogą ściągać za pośrednictwem sieci komputerowej żadnego oprogramowania bez zgody i wiedzy administratora systemu.

ROZDZIAŁ X

Postępowanie w przypadku stwierdzenia naruszenia bezpieczeństwa systemu informatycznego

§12.1. Użytkownik zobowiązany jest zawiadomić administratora bezpieczeństwa informacji lub administratora systemu o każdym naruszeniu lub podejrzeniu naruszenia bezpieczeństwa systemu informatycznego oraz/lub innych zabezpieczeń służących ochronie danych osobowych, a w szczególności o:

1) naruszeniu hasła dostępu i identyfikatora (system nie reaguje na hasło lub je ignoruje bądź można przetwarzać dane bez wprowadzenia hasła);

2) częściowym lub całkowitym braku danych albo dostępie do danych w zakresie szerszym niż wynikający z przyznanych uprawnień;

3) braku dostępu do właściwej aplikacji lub zmianie zakresu wyznaczonego dostępu do zasobów serwera;

4) wykryciu wirusa komputerowego;

5) zauważeniu elektronicznych śladów próby włamania do systemu informatycznego;

6) znacznym spowolnieniu działania systemu informatycznego;

7) podejrzeniu kradzieży sprzętu komputerowego lub dokumentów zawierających dane osobowe;

8) zmianie położenia sprzętu komputerowego;

9) zauważeniu śladów usiłowania lub dokonania włamania do pomieszczeń lub zamykanych szaf i biurek.

2. Do czasu przybycia na miejsce administratora bezpieczeństwa informacji lub administratora systemu należy:

1) o ile istnieje taka możliwość, niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego zdarzenia, a następnie uwzględnić w działaniu również ustalenie jego 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 udokumentowanie i analizę;

4) zastosować się do instrukcji i regulaminów lub dokumentacji aplikacji, jeśli odnoszą się one do zaistniałego przypadku;

5) przygotować opis incydentu;

6) nie opuszczać bez uzasadnionej przyczyny miejsca zdarzenia do czasu przybycia administratora bezpieczeństwa informacji lub administratora systemu.

3. Administrator systemu przyjmujący zawiadomienie jest obowiązany niezwłocznie poinformować administratora bezpieczeństwa informacji o naruszeniu lub podejrzeniu naruszenia bezpieczeństwa systemu informatycznego oraz/lub innych zabezpieczeń służących ochronie danych osobowych

4. Administrator bezpieczeństwa informacji po otrzymaniu zawiadomienia, o którym mowa w ust.1 lub ust. 3, powinien niezwłocznie:

1) przeprowadzić postępowanie wyjaśniające w celu ustalenia okoliczności naruszenia zasad ochrony danych osobowych,

2) podjąć działania chroniące system przed ponownym naruszeniem,

3) w przypadku stwierdzenia faktycznego naruszenia bezpieczeństwa systemu informatycznego oraz/lub innych zabezpieczeń służących ochronie danych osobowych, sporządzić raport z naruszenia bezpieczeństwa systemu informatycznego oraz innych zabezpieczeń służących ochronie danych osobowych, a następnie niezwłocznie przekazać jego kopię administratorowi danych osobowych.. Wzór raportu określony jest w załączniku nr 2 do instrukcji.

5. Administrator bezpieczeństwa informacji w uzgodnieniu z administratorem sytemu może zarządzić, w razie potrzeby, odłączenie części systemu informatycznego dotkniętej incydentem od pozostałej jego części.

6. W razie odtwarzania danych z kopii danych administrator systemu obowiązany jest upewnić się, że odtwarzane dane zapisane zostały przed wystąpieniem incydentu (dotyczy to zwłaszcza przypadków infekcji wirusowej).

7. Administrator danych osobowych po zapoznaniu się z raportem, o którym mowa w ust. 4 pkt 3, podejmuje decyzję o dalszym trybie postępowania, powiadomieniu właściwych organów oraz podjęciu innych szczególnych czynności zapewniających bezpieczeństwo systemu informatycznego bądź zastosowaniu środków ochrony fizycznej.

8. Administrator bezpieczeństwa informacji i administrator systemu zobowiązani są do informowania administratora danych osobowych o awariach systemu informatycznego, zauważonych przypadkach naruszenia niniejszej instrukcji przez użytkowników, a zwłaszcza o przypadkach posługiwania się przez użytkowników nieautoryzowanymi programami, nieprzestrzegania zasad używania oprogramowania antywirusowego, niewłaściwego wykorzystania sprzętu komputerowego lub przetwarzania danych osobowych w sposób niezgodny z procedurami ochrony danych osobowych.

9. Administrator systemu prowadzi ewidencję zdarzeń zagrażających bezpieczeństwu systemu informatycznego oraz/lub innym zabezpieczeniom służącym ochronie danych osobowych, według wzoru stanowiącego załącznik nr 3 do instrukcji.

ROZDZIAŁ XI

Postanowienia końcowe

§13.1. W sprawach nieokreślonych w instrukcji należy stosować instrukcje obsługi i zalecenia producentów aktualnie wykorzystywanych urządzeń i programów.

2. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest zapoznać się przed dopuszczeniem jej do przetwarzania danych osobowych z instrukcją, oraz złożyć oświadczenie potwierdzające znajomość jej treści, oraz zobowiązanie do przestrzegania jej postanowień, według wzoru stanowiącego załącznik nr 9 do polityki bezpieczeństwa.

3. Niezastosowanie się do procedur określonych w niniejszej instrukcji przez pracowników upoważnionych do przetwarzania danych osobowych może być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, skutkujące rozwiązaniem stosunku pracy bez wypowiedzenia na podstawie art. 52 kodeksu pracy.

4. Niezależnie od rozwiązania stosunku pracy osoby popełniające przestępstwo będą pociągane do odpowiedzialności karnej na podstawie przepisów ustawy o ochronie danych osobowych lub/i ustawy Kodeks karny.

kle

Załącznik nr 1 do instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Zbójno, przyjętej zarządzeniem nr 1/2016 Wójta Gminy Zbójno z dnia 5 stycznia 2016 r.

Ewidencja przeglądów i konserwacji systemu informatycznego oraz nośników informacji

Lp.	Data przeglądu/ konserwacji	Nazwa urządzenia	Rodzaj przeglądu/ konserwacji	Osoba/podmiot dokonujący przeglądu/konserwacji	Pracownik nadzorujący/uczestniczący w przeglądzie/konserwacji

Załącznik nr 2 do instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Zbójno, przyjętej zarządzeniem nr 1/2016 Wójta Gminy Zbójno z dnia 5 stycznia 2016 r.

Raport
z naruszenia bezpieczeństwa systemu informatycznego oraz/lub innych zabezpieczeń służących ochronie danych osobowych

1. Data: ..... Godzina: .....
2. Osoba powiadamiająca o zaistniałym naruszeniu: .....
3. Lokalizacja naruszenia: .....
4. Opis naruszenia oraz okoliczności towarzyszące: .....
.....
.....
.....
.....
5. Przyczyny naruszenia: .....
.....
.....
.....
.....
6. Postępowanie wyjaśniające: .....
.....
.....
.....
.....
7. Podjęte działania: .....
.....
.....
.....
.....

.....
(data i podpis administratora bezpieczeństwa informacji)

Załącznik nr 3 do instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Zbójno, przyjętej zarządzeniem nr 1/2016 Wójta Gminy Zbójno z dnia 5 stycznia 2016 r.

Ewidencja zdarzeń zagrażających bezpieczeństwu systemu informatycznego oraz/lub innym zabezpieczeniom służącym ochronie danych osobowych

Lp.	Data zdarzenia	Osoba powiadamiająca o zaistniałym zdarzeniu	Lokalizacja zdarzenia	Opis zdarzenia	Przyczyny zdarzenia	Podjęte działania	Osoba odpowiedzialna za podjęte działania