Urząd Gminy Gościeradów

ZAŁĄCZNIK NR 1 DO ZARZĄDZENIA WÓJTA GMINY GOŚCIERADÓW
NR 120/2013 Z DNIA 9 kwietnia 1013 r.

POLITYKA BEZPIECZEŃSTWA INFORMACJI

Niniejszy dokument zgodny jest z ustawą z dnia 29 sierpnia 1997r. o ochronie danych osobowych (tekst jednolity Dz. U. 02.101.926 z późn. zm. oraz rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. 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.04.100.1024)

Spis treści

I. Wstęp

Polityka bezpieczeństwa zwana dalej „Polityką” określa środki techniczne i organizacyjne zastosowane przez Administratora Danych dla zapewnienia ochrony danych osobowych zawartych w systemie informatycznym w wewnętrznej sieci intranetowej oraz zbiorach danych zapisanych w postaci dokumentacji papierowej w Urzędzie Gminy Gościeradów.

Administrator Danych, 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, 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:
   - 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 dokumentów zawierających dane osobowe, niezamknięcie na klucz pokoju po jego opuszczeniu),
   - naruszenie bezpieczeństwa danych przez nieautoryzowane ich przetwarzanie,
   - ujawnienie osobom nieupoważnionym procedur ochrony danych stosowanych u Administratora Danych,

- 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,
- niewykonywanie stosownych kopii zabezpieczających,
- przetwarzanie danych osobowych w celach prywatnych,
- wprowadzanie zmian do systemu informatycznego Administratora Danych i instalowanie programów bez zgody Administratora Systemu Informatycznego.

II. Postanowienia ogólne

1. Definicje

Ilekroć w polityce bezpieczeństwa jest mowa o:

1) **Administratorze Bezpieczeństwa Informacji /ABI/** – rozumie się przez to osobę, której Administrator Danych powierzył pełnienie obowiązków Administratora Bezpieczeństwa Informacji, nadzorującą stosowanie środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych, a w szczególności zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz.U.02.101.926 z późn. zm.) oraz zmianą, utratą, uszkodzeniem lub zniszczeniem, a także przeprowadzająca kontrole w zakresie określonym regulacjami wewnętrznymi Administratora Danych,
2) **Administratorze Danych** – rozumie się przez to Wójta Gminy Gościeradów,
3) **Administratorze Systemu Informatycznego /ASI/**– rozumie się przez to osobę zarządzającą systemem informatycznym w którym przetwarzane są dane osobowe,
4) **haśle** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym,
5) **identyfikatorze użytkownika** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym,
6) **integralności danych** – rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
7) **odbiorcy danych** – rozumie się przez to każdego, komu udostępnia się dane osobowe, z wyłączeniem:
   - osoby, której dane dotyczą,
   - osoby upoważnionej do przetwarzania danych,
   - przedstawiciela, o którym mowa w art. 31a ustawy,
   - podmiotu, o którym mowa w art. 31 ustawy,
   - organów państwowych lub organów samorządu terytorialnego, którym dane są

udostępniane w związku z prowadzonym postępowaniem,

8) **osobie upoważnionej do przetwarzania danych osobowych** – rozumie się przez to osobę, która upoważniona została do przetwarzania danych osobowych przez Wójta na piśmie,

9) **pomieszczeniach –** rozumie się przez to budynki, pomieszczenia lub części pomieszczeń określone przez Administratora Danych, tworzące obszar, w którym przetwarzane są dane osobowe z użyciem stacjonarnego sprzętu komputerowego oraz gromadzone w formie dokumentacji papierowej

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

11) **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,

12) **przetwarzającym** – rozumie się przez to podmiot, któremu zostało powierzone przetwarzanie danych osobowych na podstawie umowy zawieranej zgodnie z art. 31 ustawy,

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

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

15) **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),

16) **sieci publicznej** – rozumie się przez to sieć publiczną w rozumieniu art. 2 pkt 22 ustawy z dnia 21 lipca 2000 r. – Prawo telekomunikacyjne (Dz.U. nr 73, poz. 852 ze zm.),

17) **sieci telekomunikacyjnej** – rozumie się przez to sieć telekomunikacyjną w rozumieniu art. 2 pkt 23 ustawy z dnia 21 lipca 2000 r. – Prawo telekomunikacyjne,

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

19) **systemie informatycznym** – rozumie się przez to sprzęt komputerowy, oprogramowanie, dane eksploatowane w zespole współpracujących ze sobą urządzeń, programów procedur przetwarzania informacji i narzędzi programowych; w systemie tym pracuje co najmniej jeden komputer centralny i system ten tworzy sieć teleinformatyczną Administratora Danych,

20) **teletransmisji** – rozumie się przez to przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej,

21) **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.),

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

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

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

2. Cel

Wdrożenie polityki bezpieczeństwa danych osobowych Urzędu Gminy Gościeradów ma na celu zabezpieczenie danych osobowych zarówno tych przetwarzanych w systemie informatycznym jak i poza nim. Realizowane jest to poprzez wykonanie obowiązków wynikających z ustawy i rozporządzenia.

W związku z tym, że system informatyczny przetwarzający dane osobowe jest podpięty do publicznej sieci telekomunikacyjnej (Internet), wymagana jest ochrona na poziomie wysokim zgodnie z § 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. Niniejsza polityka bezpieczeństwa dotyczy zarówno danych osobowych przetwarzanych w sposób tradycyjny jak i w systemie informatycznym.

2. Procedury i zasady określone w niniejszym dokumencie stosuje się do wszystkich osób upoważnionych do przetwarzania danych osobowych, zarówno zatrudnionych, jak i innych, np. wolontariuszy, praktykantów, stażystów.

III. Organizacja przetwarzania danych osobowych

1. Administrator Danych

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

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

2) upoważnia poszczególne osoby do przetwarzania danych osobowych w określonym indywidualnie zakresie, odpowiadającym zakresowi jej obowiązków;

3) odwołuje upoważnienia do przetwarzania danych osobowych;

4) wyznacza Administratora Bezpieczeństwa Informacji oraz określa zakres jego zadań i czynności;

5) wyznacza ASI jako właściwego do prowadzenia ewidencji osób upoważnionych do przetwarzania danych osobowych oraz pozostałej dokumentacji z zakresu ochrony danych;

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

2. Administrator Bezpieczeństwa Informacji /ABI/

Administrator Bezpieczeństwa Informacji realizuje zadania w zakresie nadzoru nad przestrzeganiem zasad ochrony danych osobowych, w tym zwłaszcza:

1) sprawuje nadzór nad wdrożeniem stosownych środków fizycznych, a także organizacyjnych i technicznych – w celu zapewnienia bezpieczeństwa danych,
2) sprawuje nadzór nad funkcjonowaniem systemu zabezpieczeń, w tym także nad prowadzeniem ewidencji z zakresu ochrony danych osobowych,
3) koordynuje wewnętrzne audyty przestrzegania przepisów o ochronie danych osobowych,
4) nadzoruje udostępnianie danych osobowych odbiorcom danych i innym podmiotom,
5) nadzoruje przygotowywanie wniosków zgłoszeń rejestracyjnych i aktualizacyjnych zbiorów danych do GIODO,
6) zatwierdza wzory dokumentów dotyczących ochrony danych osobowych, przygotowywane przez komórki organizacyjne Administratora Danych,
7) nadzoruje prowadzenie ewidencji i innej dokumentacji z zakresu ochrony danych osobowych przez Administratora Systemu Informatycznego,
8) prowadzi oraz aktualizuje dokumentację opisującą sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych,
9) podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia systemu informatycznego,
10) przygotowuje materiały szkoleniowe z zakresu ochrony danych osobowych i prowadzi szkolenia osób upoważnianych do przetwarzania danych osobowych,
11) w porozumieniu z Administratorem Danych na czas nieobecności (urlop, choroba) wyznacza swojego zastępcę.

3. Administrator Systemu Informatycznego /ASI/

Administrator Systemu Informatycznego realizuje zadania w zakresie zarządzania i bieżącego nadzoru nad systemem informatycznym Administratora Danych, 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) przesyła wnioski zgłoszeń rejestracyjnych i aktualizacyjnych zbiorów danych do GIODO,
3) przeciwdziała dostępowi osób niepowołanych do systemu informatycznego, w którym przetwarzane są dane osobowe,
4) 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,

5) nadzoruje działanie mechanizmów uwierzytelniania użytkowników oraz kontroli dostępu do danych osobowych,
6) podejmuje działania w zakresie ustalania i kontroli identyfikatorów dostępu do systemu informatycznego,
7) wyrejestrowuje użytkowników,
8) zmienia w poszczególnych stacjach roboczych hasła dostępu, ujawniając je wyłącznie danemu użytkownikowi oraz, w razie potrzeby, Administratorowi Bezpieczeństwa Informacji lub Administratorowi Danych,
9) w sytuacji stwierdzenia naruszenia zabezpieczeń systemu informatycznego informuje ABI o naruszeniu i współdziała z nim przy usuwaniu skutków naruszenia,
10) prowadzi szczegółową dokumentację naruszeń bezpieczeństwa danych osobowych przetwarzanych w systemie informatycznym,
11) sprawuje nadzór nad wykonywaniem napraw, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są dane osobowe, nad wykonywaniem kopii zabezpieczających, ich przechowywaniem oraz okresowym sprawdzaniem pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu informatycznego,
12) prowadzi rejestr wykonywanych kopii zabezpieczających oraz dziennik systemu informatycznego,
13) 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,
14) prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych.

4. Osoba upoważniona do przetwarzania danych osobowych

Osoba upoważniona do przetwarzania danych osobowych jest zobowiązana przestrzegać następujących zasad:

1) przetwarza dane osobowe wyłącznie w zakresie ustalonym przez Administratora Danych w upoważnieniu i tylko w celu wykonywania nałożonych na nią 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) musi 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) zapoznaje się z przepisami prawa w zakresie ochrony danych osobowych oraz postanowieniami niniejszej polityki i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych;

4) stosuje określone przez Administratora Danych oraz Administratora Bezpieczeństwa Informacji procedury oraz wytyczne mające na celu zgodne z prawem, w tym zwłaszcza adekwatne, przetwarzanie danych;
5) korzysta z systemu informatycznego w sposób zgodny ze wskazówkami zawartymi w instrukcjach obsługi urządzeń wchodzących w skład systemu informatycznego, oprogramowania i nośników;
6) zabezpiecza dane przed ich udostępnianiem osobom nieupoważnionym.

IV. Infrastruktura przetwarzania danych osobowych

1. Obszar przetwarzania danych osobowych

Tabela 1. Wykazu budynków i pomieszczeń wchodzących w skład obszaru przetwarzania danych osobowych

Wykaz budynków i pomieszczeń wchodzących w skład obszaru przetwarzania danych osobowych.	
Adres:	Pomieszczenia:
Urząd Gminy Gościeradów Gościeradów Ukazowy 61 23-275 Gościeradów	Budynek Urzędu: – Archiwum - piwnica – parter, pokoje nr: 1,2,3,5,6,7,8 – I piętro, pokoje nr: 10,11, 12,13,14, 15,18,19,20 – Serwerownia: 14A

2. Zbiory danych

Tabela 2. Wykaz zbiorów danych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych w jednostce

Wykaz zbiorów danych wraz ze wskazaniem programów zastosowanych do przetwarzania danych osobowych w Urzędzie Gminy Gościeradów.				
Lp.	Zbiór danych	Programy zastosowane do przetwarzania / Nazwa zasobu*	Lokalizacja zbioru/zasobu	Miejsce przetwarzania danych
1.	Akcyza	Przetwarzany w sposób papierowy i w systemie informatycznym – POGRUN (Radix Software)	Serwerownia Pokój nr 1	Pokój nr 1
2.	Dodatki mieszkaniowe	Przetwarzany w	Pokój nr 1	Pokój nr 1

		sposób papierowy		
3.	Windykacja i zbyt	Przetwarzany w sposób papierowy i w systemie informatycznym – Media (Etob-res)	Pokój nr 1	Pokój nr 1
4.	Umowy na dostawę wody i zrzut ścieków	Przetwarzany w sposób papierowy	Pokój nr 1	Pokój nr 1
5.	Umowy najmu lokali użytkowych	Przetwarzany w sposób papierowy	Pokój nr 1	Pokój nr 1
6.	Umowy najmu lokali mieszkalnych	Przetwarzany w sposób papierowy	Pokój nr 1	Pokój nr 1
7.	Ewidencja działalności gospodarczej	Przetwarzane w sposób papierowy	Pokój nr 1	Pokój nr 1
8.	Zezwolenia na sprzedaż napojów alkoholowych	Przetwarzane w sposób papierowy	Pokój nr 1	Pokój nr 1
9.	Faktury za dostawę wody i zrzut ścieków	Przetwarzane w sposób papierowy	Pokój nr 1	Pokój nr 1
10.	Decyzje o warunkach zabudowy	Przetwarzane w sposób papierowy	Pokój nr 2	Pokój nr 2
11.	Decyzje zezwalające na wycinkę drzew	Przetwarzane w sposób papierowy	Pokój nr 2	Pokój nr 2
12.	Zaświadczenia z miejscowego planu zagospodarowania przestrzennego	Przetwarzane w sposób papierowy	Pokój nr 2	Pokój nr 2
13.	Wypisy i wyrysy z miejscowego planu zagospodarowania przestrzennego	Przetwarzane w sposób papierowy	Pokój nr 2	Pokój nr 2
14.	Zezwolenia na uprawę maku	Przetwarzane w sposób papierowy	Pokój nr 2	Pokój nr 2
15.	Uzgodnienia i opinie na wydawanie koncesji i rozpoznanie złóż kruszywa naturalnego	Przetwarzane w sposób papierowy	Pokój nr 2	Pokój nr 2
16.	Wydawanie decyzji o ustaleniu lokalizacji celu publicznego	Przetwarzane w sposób papierowy	Pokój nr 2	Pokój nr 2
17.	Wnioski zmian do miejscowego planu zagospodarowania	Przetwarzane w sposób papierowy	Pokój nr 2	Pokój nr 2

	przestrzennego			
18.	Grunty i działki	Przetwarzany w systemie informatycznym – EWOPIS (GEOBID)	Serwerownia	Pokój nr 3
19.	Urząd Stanu Cywilnego	Przetwarzany w sposób papierowy i w systemie informatycznym – System USC (Wojewódzki Ośrodek Informatyki Oddział Terenowy w Lublinie)	Pokój nr 5 Archiwum	Pokój nr 5
20.	Ewidencja ludności i dowodów osobistych	Przetwarzany w sposób papierowy i w systemie informatycznym – Mikropesel (Wojewódzki Ośrodek Informatyki Oddział Terenowy w Lublinie) SOO	Pokój nr 6 Archiwum	Pokój nr 6
21.	Nakazy płatnicze	Przetwarzany w systemie informatycznym – POGRUN (Radix Software)	Serwerownia	Pokój nr 7
22.	Podania i decyzje o udzieleniu ulgi podatkowej i umorzeniu	Przetwarzane w sposób papierowy	Pokój nr 7	Pokój nr 7
23.	Rejestr korespondencji z innymi podmiotami	Przetwarzane w sposób papierowy	Pokój nr 7	Pokój nr 7
24.	Wnioski o wydanie zaświadczeń	Przetwarzane w sposób papierowy	Pokój nr 7	Pokój nr 7
25.	Zaświadczenia o stanie majątkowym lub niezaleganiu	Przetwarzane w sposób papierowy	Pokój nr 7	Pokój nr 7
26.	Dowody wpłat	Przetwarzane w systemie informatycznym – WIP (Radix Software)	Serwerownia	Pokój nr 7
27.	Upomnienia	Przetwarzane w sposób papierowy	Pokój nr 7	Pokój nr 7
28.	Tytuły wykonawcze	Przetwarzane w	Pokój nr 7	Pokój nr 7

		sposób papierowy		
29.	Podatek od środków transportowych	Przetwarzane w sposób papierowy i w systemie informatycznym – POST (Radix Software)	Pokój nr 7	Pokój nr 7
30.	Kwalifikacja wojskowa	Przetwarzane w sposób papierowy	Pokój nr 8	Pokój nr 8
31.	Rejestracja przedpoborowych	Przetwarzane w sposób papierowy	Pokój nr 8	Pokój nr 8
32.	Rejestr osób skierowanych do odbycia prac społecznie - użytecznych	Przetwarzane w sposób papierowy	Pokój nr 8	Pokój nr 8
33.	Ewidencja kierowców i rejestracja pojazdów oraz zezwolenia na transport	Przetwarzane w sposób papierowy	Pokój nr 8	Pokój nr 8
34.	System Komputerowego Obiegu Korespondencji	Przetwarzane w systemie informatycznym – E-obieg	Serwerownia	Pokój nr 10 Cały budynek Urzędu Gminy
35.	Wnioski i skargi	Przetwarzane w sposób papierowy	Pokój nr 10	Pokój nr 10
36.	Akta osobowe	Przetwarzane w sposób papierowy	Pokój nr 13 Archiwum	Pokój nr 13
37.	Ewidencje wynikające z umowy z PUP (Powiatowym Urzędem Pracy)	Przetwarzane w sposób papierowy	Pokój nr 13	Pokój nr 13
38.	Oświadczenia majątkowe kierowników i radnych Rady Gminy Gościeradów	Przetwarzane w sposób papierowy	Pokój nr 13 Archiwum	Pokój nr 13
39.	Umowy związane z obsługą wyborów	Przetwarzane w sposób papierowy	Pokój nr 13	Pokój nr 13
40.	Rp - 7	Przetwarzane w sposób papierowy	Pokój nr 13	Pokój nr 13, 20
41.	Aneksy do umów o pracę	Przetwarzane w sposób papierowy	Pokój nr 13	Pokój nr 13
42.	Deklaracje udziału w konkursach	Przetwarzane w sposób papierowy	Pokój nr 14	Pokój nr 14

	organizowanych przez Urząd Gminy Gościeradów			
43.	System Informacji Oświatowej	Centrum Informatyczne Edukacji MEN	Pokój nr 15	Pokój nr 15
44.	Stypendia szkolne i zasiłki szkolne	Przetwarzane w sposób papierowy i w systemie informatycznym – Świadczenia rodzinne (Signity)	Pokój nr 15	Pokój nr 15
45.	Przygotowanie zawodowe młodocianych	Przetwarzane w sposób papierowy	Pokój nr 15	Pokój nr 15
46.	Podsystem monitorowania EFS 2007 u Beneficjenta POKL	Przetwarzane w sposób papierowy i w systemie informatycznym – PEFS 2007	Pokój nr 15	Pokój nr 15
47.	Obowiązek szkolny i obowiązek nauki	Przetwarzane w sposób papierowy	Pokój nr 15	Pokój nr 15
48.	Awans zawodowy	Przetwarzane w sposób papierowy	Pokój nr 15	Pokój nr 15
49.	Płatnik	Przetwarzane w systemie informatycznym – Płatnik Asseco Poland S.A.	Serwerownia	Pokój nr 18
50.	Płace	Przetwarzane w systemie informatycznym – Płace + (Radix Software)	Serwerownia	Pokój nr 18
51.	Kadry	Przetwarzane w systemie informatycznym – Kadry (Radix Software)	Serwerownia	Pokój nr 18
52.	Karty wynagrodzeń, PIT-11 i angaże	Przetwarzane w sposób papierowy	Pokój nr 18	Pokój nr 18
53.	Listy płac	Przetwarzane w sposób papierowy	Pokój nr 18	Pokój nr 18
54.	Dowóz dzieci niepełnosprawnych do	Przetwarzane w sposób papierowy	Pokój nr 18	Pokój nr 18

	szkoły			
55.	Faktury/rachunki (osoby fizyczne)	Przetwarzane w sposób papierowy	Pokój nr 18	Pokój nr 18
56.	Zwolnienia lekarskie ZUS ZLA	Przetwarzane w sposób papierowy	Pokój nr 18	Pokój nr 18
57.	Pożyczki mieszkaniowe	Przetwarzane w sposób papierowy	Pokój nr 18	Pokój nr 18
58.	Gospodarka odpadami	Przetwarzane w systemie informatycznym – GOK	Pokój nr 17	Pokój nr 17

3. System informatyczny

System informatyczny Administratora Danych obsługiwany jest przez serwer zlokalizowany w Serwerowni Urzędu Gminy.

System ten ma bezpieczne połączenie z Internetem. W systemie informatycznym przetwarzane są dane ze zbiorów danych Administratora Danych, tj.

1. Akcyza
2. Windykacja i zbyt
3. Grunty i działki
4. Urząd Stanu Cywilnego
5. Ewidencja ludności i dowody osobiste
6. Nakazy płatnicze
7. Dowody wpłat
8. Podatek od środków transportowych
9. System Komputerowego Obiegu Korespondencji
10. System Informacji Oświatowej
11. Stypendia szkolne i zasiłki szkolne
12. Podsystem Monitorowania Europejskiego Funduszu Społecznego 2007 u Beneficjenta POKL
13. Płatnik
14. Płace
15. Kadry
16. Księgowość
17. Przelewy
18. Gospodarka odpadami

Lokalizacja stacji roboczych:

- Pomieszczenia Księgowości
- Pomieszczenia USC
- Sekretariat

- Pokój Inspektora ds. edukacji i spraw społecznych
- Pomieszczenie podinspektora ochrony środowiska

4. Ewidencje

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

1) Administrator Systemu Informatycznego prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych,
2) Administrator Bezpieczeństwa Informacji prowadzi ewidencję udostępnień danych odbiorcom danych oraz innym podmiotom,
3) Administrator Systemu Informatycznego prowadzi przechowywaną w szafie metalowej ewidencję sprzętu komputerowego, licencji i oprogramowania oraz haseł dostępu.

V. Struktura zbiorów danych, sposób przepływu danych w systemie i zakres przetwarzania danych

Wykaz zbiorów danych wraz ze wskazaniem ich struktury.

Lp.	Zbiór danych	Struktura zbioru
1.	Akcyza	– Imiona i nazwiska – Adresy zamieszkania lub pobytu – Seria i numer dowodu osobistego – Numer ewidencyjny PESEL – Numer Identyfikacji Podatkowej – Powierzchnia nieruchomości – Numer konta bankowego
2.	Dodatki mieszkaniowe	– Imię i nazwisko – Data urodzenia – Adres zamieszkania – Dochody – Wydatki miesięczne – Miejsce pracy
3.	Windykacja i zbyt	– Imię i nazwisko – Adres zamieszkania
4.	Umowy na dostawę wody i zrzut ścieków	– Imię i nazwisko – Adres zamieszkania
5.	Umowy najmu lokali użytkowych	– Imię i nazwisko – Adres zamieszkania
6.	Umowy najmu lokali mieszkalnych	– Imię i nazwisko – Adres zamieszkania
7.	Ewidencja działalności	– Imię i nazwisko

	gospodarczej	– Adres zamieszkania – Data urodzenia – Obywatelstwo – Imiona rodziców – Numer ewidencyjny PESEL – Numer Identyfikacji Podatkowej – Telefon – Adres poczty elektronicznej – Numer rachunku bankowego
8.	Zezwolenia na sprzedaż napojów alkoholowych	– Imię i nazwisko – Adres zamieszkania
9.	Faktury za dostawę wody i zrzut ścieków	– Imię i nazwisko / nazwa firmy – Adres – Numer Identyfikacji Podatkowej
10.	Decyzje o warunkach zabudowy	– Imię i nazwisko – Adres – Numer działki
11.	Decyzje zezwalające na wycinkę drzew	– Imię i nazwisko – Adres – Numer działki
12.	Zaświadczenia z miejscowego planu zagospodarowania przestrzennego	– Imię i nazwisko – Adres – Numer działki
13.	Wypisy i wyrysy z miejscowego planu zagospodarowania przestrzennego	– Imię i nazwisko – Adres – Numer działki
14.	Zezwolenia na uprawę maku	– Imię i nazwisko – Adres – Numer działki
15.	Uzgodnienia i opinie na wydawanie koncesji i rozpoznanie złóż kruszywa naturalnego	– Imię i nazwisko / nazwa firmy – Adres – Numer działki – REGON – NIP
16.	Wydawanie decyzji o ustaleniu lokalizacji celu publicznego	– Imię i nazwisko / nazwa firmy – Adres – Numer działki
17.	Wnioski zmian do miejscowego planu zagospodarowania	– Imię i nazwisko / nazwa firmy – Adres zamieszkania

	przestrzennego	
18.	Grunty i działki	– Imię i nazwisko – Adres zamieszkania lub pobytu – PESEL – NIP – Imiona rodziców
19.	Urząd Stanu Cywilnego	– Nazwiska i imiona – Imiona rodziców – Data urodzenia – Adres zamieszkania lub pobytu – PESEL – Miejsce pracy – Zawód – Wykształcenie – Seria i numer dowodu osobistego – Źródło utrzymania – Płeć – Stan cywilny – Nazwisko z poprzedniego małżeństwa i rodowe – Nazwisko i imię: ojca, matki, współmałżonka – Nazwisko po zawarciu małżeństwa – Miejsce i godzina urodzenia – Data i numer aktu: urodzenia, małżeństwa, zgonu – Data i miejsce zawarcia małżeństwa – Miejsce wystawienia i numer aktu urodzenia współmałżonka – Data, godzina, miejsce odnalezienia zwłok – Nazwisko, imię i adres osoby zgłaszającej zgon – Adnotacje o rozwodzie i separacji – Miejsce wydania dowodu osobistego – Data unieważnienia aktu: urodzenia, małżeństwa, zgonu – Imię nadane z urzędu – Data i numer orzeczenia sądu ustalającego ojcostwo, zaprzeczającego ojcostwo, przysposabiającego dziecko – Imię i nazwisko osoby przysposabiającej dziecko – Zmiana nazwiska dziecka – Numer aktu zgonu współmałżonka – Nazwisko, nazwisko rodowe i imię współmałżonka – Nazwisko rodowe matki i ojca – Data rozwiązania poprzedniego małżeństwa
20.	Ewidencja ludności i dowody osobiste	– Nazwiska i imiona – Imiona rodziców – Data urodzenia

		– Adres zamieszkania lub pobytu – PESEL – Seria i numer dowodu osobistego – Obywatelstwo – Płeć – Stan cywilny – Miejsce urodzenia – Wystawca dokumentu tożsamości – Rysopis /wzrost, kolor oczu/ – Poprzednie adresy – Nazwisko rodowe – Nazwisko rodowe matki – Dane współmałżonka – Właściwy USC i numer aktu urodzenia – Stosunek do powszechnego obowiązku obrony – Dane o poprzednich stanach cywilnych
21.	Nakazy płatnicze	– Imię i nazwisko – Adres zamieszkania – Powierzchnia gospodarstwa – Numer ewidencyjny PESEL – NIP
22.	Podania i decyzje o udzieleniu ulgi podatkowej i umorzeniu	– Imię i nazwisko – Adres zamieszkania – Dane dot. stanu majątkowego – Zaświadczenia lekarskie
23.	Rejestr korespondencji z innymi podmiotami	– Imiona i nazwiska – Adres zamieszkania – Dane dot. stanu majątkowego
24.	Wnioski o wydanie zaświadczeń	– Imię i nazwisko – Adres zamieszkania – Data urodzenia – PESEL – NIP – Numer telefonu
25.	Zaświadczenia o stanie majątkowym lub niezaleganiu	– Imię i nazwisko – Adres zamieszkania – Dane dot. stanu majątkowego – Dochody – Zaległości w płatnościach
26.	Dowody wpłat	– Imię i nazwisko – Adres zamieszkania
27.	Upomnienia	– Imię i nazwisko – Adres zamieszkania

		– Zaległości w płatnościach
28.	Tytuły wykonawcze	– Imię i nazwisko – Adres zamieszkania – Imię ojca i matki – PESEL – NIP
29.	Podatek od środków transportowych	– Imię i nazwisko – Adres zamieszkania – Dane dotyczące posiadanych pojazdów
30.	Kwalifikacja wojskowa	– Imię i nazwisko – Adres – Seria i numer dowodu osobistego – PESEL – Kategoria zdrowia – Książeczka wojskowa
31.	Rejestracja przedpoborowych	– Imię i nazwisko – Adres – PESEL
32.	Rejestr osób skierowanych do odbycia prac społecznie - użytecznych	– Imię i nazwisko – Adres – PESEL – Wyrok / orzeczenie sądu
33.	Ewidencja kierowców i rejestracja pojazdów oraz zezwolenia na transport	– Imię i nazwisko / nazwa firmy – Adres zamieszkania / firmy – NIP – REGON – Imiona rodziców – Data i miejsce urodzenia – Miejsce pracy / zawód – Wykształcenie – Seria i numer dowodu osobistego – Informacje o stanie zdrowia – Orzeczenia o ukaraniu i inne wydane w postępowaniu administracyjnym lub sądowym
34.	System Komputerowego Obiegu Korespondencji	– Imię i nazwisko/ nazwa firmy lub instytucji – Adres zamieszkania/ siedziba
35.	Wnioski i skargi	– Imię i nazwisko – Adres zamieszkania
36.	Akta osobowe	Zbiór ten obejmuje dane byłych i obecnych pracowników oraz osób świadczących usługi na rzecz Administratora Danych na innej podstawie niż stosunek pracy. Zakres pierwszy danych tego zbioru, tzn. imię i nazwisko osoby, dostępny jest wszystkim pracownikom

		Administratora Danych, a także niektórym osobom świadczącym usługi na rzecz Administratora Danych na innej podstawie niż stosunek pracy. Zakres drugi danych tego zbioru, tzn. imię i nazwisko osoby, jej adres, numer telefonu, wysokość wynagrodzenia, podstawowe, niezbędne do ustalenia wysokości wynagrodzenia, dane dotyczące stażu pracy, wykształcenia, urlopów i zwolnień, numer dowodu osobistego, numer NIP i PESEL, imiona rodziców, datę i miejsce urodzenia, dostępny jest: 4) Inspektorom ds. księgowości 5) Skarbnikowi Gminy. Dane tego zakresu są udostępniane przez upoważnionych pracowników księgowości ZUS-owi i urzędom skarbowym. Zakres trzeci danych tego zbioru obejmuje dane kadrowe (w tym wiele danych wrażliwych), tj. informacje o odbytych szkoleniach, urlopach, dokładne dane dotyczące wykształcenia, ewentualnie zainteresowań i hobby, informacje o posiadanych dzieciach, zawartych związkach małżeńskich, a także dane o stanie zdrowia, wynikające z zaświadczeń lekarskich, wydawanych zwłaszcza w wyniku badań profilaktycznych (wstępnych, okresowych i kontrolnych). Dostęp do tych danych posiadają wyłącznie: 6) Wójtowi Gminy 7) Sekretarzowi Gminy 8) Inspektorowi ds. kadrowych Dane z zakresu trzeciego mogą być udostępniane organom prowadzącym kontrolę, w tym zwłaszcza Państwowej Inspekcji Pracy i sądom powszechnym w związku z prowadzonym postępowaniem.
37.	Ewidencje wynikające z umowy z PUP (Powiatowym Urzędem Pracy)	– Imiona i nazwiska – Adres zamieszkania lub pobytu – Numer ewidencyjny PESEL – Numer rejestracyjny pojazdu lub dane osoby na którą jest zarejestrowany – Data urodzenia
38.	Oświadczenia majątkowe kierowników i radnych Rady Gminy Gościeradów	– Imię i nazwisko, także rodowe – Data i miejsce urodzenia – Adres zamieszkania – Miejsce zatrudnienia i zawód – Adresy nieruchomości będących w posiadaniu – Informacje o stanie majątkowym i dochodach – Informacje nt. prowadzonej działalności gospodarczej – Informacje nt. członkostwa w zarządach – Informacje nt. zobowiązań

39.	Umowy związane z obsługą wyborów	– Imię i nazwisko – Adres – NIP – PESEL – Imię ojca i matki – Miejsce i data urodzenia – Wynagrodzenie
40.	Rp - 7	– Imię i nazwisko – Adres – Data urodzenia – PESEL – Dane dotyczące zatrudnienia – Wynagrodzenia
41.	Aneksy do umów o pracę	– Imię i nazwisko – Adres zamieszkania – Numer ewidencyjny PESEL
42.	Deklaracje udziału w konkursach organizowanych przez Urząd Gminy Gościeradów	– Imię i nazwisko – Adres zamieszkania – Numer telefonu
43.	System Informacji Oświatowej	– Numer ewidencyjny PESEL – Data urodzenia – Kwalifikacje zawodowe – Wynagrodzenie
44.	Stypendia szkolne i zasiłki szkolne	– Imię i nazwisko – Numer ewidencyjny PESEL – Data i miejsce urodzenia – Adres zamieszkania – Informacja o dochodach – Dane dotyczące stanu cywilnego
45.	Przygotowanie zawodowe młodocianych	– Imię i nazwisko – Adres zamieszkania – Data urodzenia – Numer ewidencyjny PESEL – Dokumenty potwierdzające kwalifikacje zawodowe
46.	Podsystem monitorowania EFS 2007 u Beneficjenta POKL	– Imię i nazwisko – Płeć – Wiek – PESEL – Wykształcenie – Adres zamieszkania – Telefon stacjonarny i komórkowy

		– Adres poczty elektronicznej – Miejsce zatrudnienia / status na rynku pracy – Informacje n.t przyznanego wsparcia
47.	Obowiązek szkolny i obowiązek nauki	– Imię i nazwisko – Adres zamieszkania – Data urodzenia
48.	Awans zawodowy	– Imię i nazwisko – Adres zamieszkania – Data urodzenia
49.	Płatnik	– NIP płatnika, ubezpieczonego i członków rodziny ubezpieczonego – REGON płatnika, ubezpieczonego i członków rodziny ubezpieczonego – PESEL płatnika, ubezpieczonego i członków rodziny ubezpieczonego – Seria i numer dokumentu tożsamości płatnika, ubezpieczonego i członków rodziny ubezpieczonego – Nazwa firmy płatnika – Imię i nazwisko płatnika, ubezpieczonego i członków rodziny ubezpieczonego – Data urodzenia płatnika, ubezpieczonego i członków rodziny ubezpieczonego – Telefon płatnika, ubezpieczonego i członków rodziny ubezpieczonego – Numer rachunku bankowego płatnika, ubezpieczonego i członków rodziny ubezpieczonego – Informacje nt. niepełnosprawności ubezpieczonego i członków rodziny ubezpieczonego – Wykształcenie ubezpieczonego i członków rodziny ubezpieczonego – Zawód i miejsce pracy ubezpieczonego
50.	Płace	– Imiona i nazwiska – Adres zamieszkania – PESEL – NIP – Imię ojca i matki – Data urodzenia – Kwota wynagrodzenia – Numer konta bankowego
51.	Kadry	– Imię i nazwisko – Adres zamieszkania – Imiona rodziców – Nazwisko rodowe matki – Płeć

		– Data urodzenia – Numer konta bankowego – Wykształcenie – Angaże zawodowe – Wymiar czasu pracy
52.	Karty wynagrodzeń, PIT-11 i angaże	– Imiona i nazwiska – Adres zamieszkania – Data urodzenia – PESEL – NIP – Wynagrodzenie – Imiona rodziców
53.	Listy płac	– Imiona i nazwiska – Wynagrodzenie
54.	Dowóz dzieci niepełnosprawnych do szkoły	– Imiona i nazwiska – Adres zamieszkania – PESEL – Orzeczenia o niepełnosprawności
55.	Faktury/rachunki (osoby fizyczne)	– Imię i nazwisko – Adres – PESEL – NIP – Imiona rodziców – Numer konta bankowego
56.	Zwolnienia lekarskie ZUS ZLA	– Imię i nazwisko – Adres zamieszkania – PESEL – NIP – Seria i numer dowodu osobistego – Data urodzenia
57.	Pożyczki mieszkaniowe	– Imiona i nazwiska – Adres zamieszkania – Seria i numer dowodu osobistego
58.	Płace	– Imię i nazwisko – Adres zamieszkania – PESEL – NIP – Seria i numer dowodu osobistego – Nazwisko rodowe – Wynagrodzenie – Telefon – Adres poczty elektronicznej – Angaże

		– Imiona rodziców – Data i miejsce urodzenia
59.	Księgowość	– Imię i nazwisko – Adres zamieszkania – PESEL – Numer konta bankowego
60.	Płatnik	– NIP płatnika, ubezpieczonego i członków rodziny ubezpieczonego – REGON płatnika, ubezpieczonego i członków rodziny ubezpieczonego – PESEL płatnika, ubezpieczonego i członków rodziny ubezpieczonego – Seria i numer dokumentu tożsamości płatnika, ubezpieczonego i członków rodziny ubezpieczonego – Nazwa firmy płatnika – Imię i nazwisko płatnika, ubezpieczonego i członków rodziny ubezpieczonego – Data urodzenia płatnika, ubezpieczonego i członków rodziny ubezpieczonego – Telefon płatnika, ubezpieczonego i członków rodziny ubezpieczonego – Numer rachunku bankowego płatnika, ubezpieczonego i członków rodziny ubezpieczonego – Informacje nt. niepełnosprawności ubezpieczonego i członków rodziny ubezpieczonego – Wykształcenie ubezpieczonego i członków rodziny ubezpieczonego – Zawód i miejsce pracy ubezpieczonego
61.	Przelewy	– Imię i nazwisko – Adres zamieszkania – Numer konta bankowego
62.	Stypendia naukowe	– Imię i nazwisko dziecka
63.	Oświadczenia do celów podatkowych	– Imię i nazwisko – Adres zamieszkania – Numer konta bankowego – Informacje o zatrudnieniu
64.	Decyzje pożyczek mieszkaniowych	– Imię i nazwisko – Adres zamieszkania – Seria i numer dowodu osobistego – PESEL
65	Kopie świadectw pracy angaży i umów o pracę	– Imię i nazwisko – Adres zamieszkania – PESEL – Składniki wynagrodzenia
66	Kartoteka deklaracji o wys. opłaty za gosp. odpadami komunalnymi	– Imię i nazwisko – Adres zamieszkania – PESEL, NIP

Poziom bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym

Ze względu na fakt, że system informatyczny Administratora Danych połączony jest z siecią publiczną, zgodnie z § 6 ust. 4 rozporządzenia należy zapewnić wysoki poziom bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym. Wynikające z tego konsekwencje trzeba uwzględnić w instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

VI. Strategia zabezpieczenia danych osobowych (działania niezbędne do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych)

1. Bezpieczeństwo osobowe

Zachowanie poufności

1. Kandydaci na pracowników są dobierani z uwzględnieniem ich kompetencji merytorycznych, a także kwalifikacji moralnych. Zwraca się uwagę na takie cechy kandydata, jak uczciwość, odpowiedzialność, przewidywalność zachowań.

2. Ryzyko utraty bezpieczeństwa danych przetwarzanych przez Administratora Danych pojawiające się ze strony osób trzecich, które mają dostęp do danych osobowych (np. serwisanci), jest minimalizowane przez podpisanie umów powierzenia przetwarzania danych osobowych.

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

Szkolenia w zakresie ochrony danych osobowych

1. Administrator Bezpieczeństwa Informacji realizuje następujące szkolenia:
   a. szkoli się każdą osobę, która ma zostać upoważniona do przetwarzania danych osobowych,
   b. szkolenia wewnętrzne wszystkich osób upoważnionych do przetwarzania danych osobowych przeprowadzane są w przypadku zmian zasad lub procedur ochrony danych osobowych,
   c. przeprowadza się szkolenia dla osób innych niż upoważnione do przetwarzania danych, jeśli pełnione przez nie funkcje wiążą się z zabezpieczeniem danych osobowych.
2. Tematyka szkoleń obejmuje:
   a. przepisy i procedury dotyczące ochrony danych osobowych, sporządzania i przechowywania ich kopii, niszczenia wydruków i zapisów na nośnikach,
   b. sposoby ochrony danych przed osobami postronnymi i procedury udostępniania danych osobom, których one dotyczą,

c. sposoby ochrony danych w systemach teleinformatycznych,

d. obowiązki osób upoważnionych do przetwarzania danych osobowych i innych,

e. odpowiedzialność za naruszenie obowiązków z zakresu ochrony danych osobowych,

f. zasady i procedury określone w polityce bezpieczeństwa.

3. Poprzez szkolenia należy także rozumieć umieszczanie na folderze sieciowym dostępnym dla wszystkich pracowników obowiązujących przepisów prawa, opracowanych dokumentów, procedur oraz stosownych wyjaśnień i informacji.

2. Zabezpieczenie sprzętu

1. Serwer jest zlokalizowany w serwerowni w budynku Urzędu Gminy.

Serwerownia zabezpieczona jest poprzez:

- systemy sygnalizacji włamania i napadu (SSWiN) oraz kontrola dostępu (KD),
  System sygnalizacji włamania i napadu oraz kontroli dostępu wykonany jest aby zabezpieczyć serwerownię przed takimi zagrożeniami jak: włamanie, kradzież, nieuprawniony dostęp do pomieszczenia oraz pożar. System kontroli dostępu przystosowany jest do obsługi jednego przejścia. Zbudowany jest on z kontrolera przejścia oraz czytnika kart zamontowanego przed wejściem do serwerowni. Zapewnia pełną kontrolę i pamięć zdarzeń (rejestracja wejść wraz z identyfikacją karty). Karty zbliżeniowe są w standardzie UNIQUE.
- klimatyzator,
  Ze względu na potrzebę utrzymania optymalnych warunków dla pracy urządzeń w pomieszczeniu serwerowni zastosowano system klimatyzacji.
- drzwi antywłamaniowych
  - drzwi stalowe antywłamaniowe
  - dwa zamki atestowane,

2. Administrator Systemu Informatycznego wskazuje użytkownikom, jak postępować, aby zapewnić prawidłową eksploatację systemu informatycznego, a zwłaszcza:

- ochronę nośników przenośnych – w tym także nośników danych, na których przechowywane są kopie zabezpieczające,

- prawidłową lokalizację komputerów.

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. Bezprzewodowy punkt dostępowy do sieci lokalnej Administratora Danych przeznaczony dla komputerów przenośnych Administratora Danych chroniony jest za pomocą silnych metod kryptograficznych, uwierzytelniania i szyfrowania komunikacji. Dodatkowo funkcjonalność tego segmentu sieci jest okrojona za pomocą urządzenia UTM.

6. Bezprzewodowa sieć Internetowa dla mieszkańców Gminy jest rozdzielona z

siecią lokalną Urzędu za pomocą urządzenia UTM.

7. Bieżąca konserwacja sprzętu wykorzystywanego przez Administratora Danych do przetwarzania danych prowadzona jest tylko przez Administratora Systemu Informatycznego. Natomiast poważne naprawy wykonywane przez personel zewnętrzny realizowane są w siedzibie Administratora Danych po zawarciu z podmiotem wykonującym naprawę umowy o powierzenie przetwarzania danych osobowych, określającej kary umowne za naruszenie bezpieczeństwa danych.

8. Administrator Systemu Informatycznego dopuszcza konserwowanie i naprawę sprzętu poza siedzibą Administratora Danych 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 także zawiera się umowy powierzenia przetwarzania danych.

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

3. Zabezpieczenia we własnym zakresie

Niezwykle ważne dla bezpieczeństwa danych jest wyrobienie przez każdą osobę upoważnioną do przetwarzania danych lub użytkownika nawyku:

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 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;

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 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 zabezpieczone obszary, a następnie prawidłowym wylogowaniu się użytkownika i wyłączeniu komputera oraz odcięciu napięcia w UPS i listwie;

17) niszczenia w niszczarce lub chowania do szaf 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 tajemnicy danych, w tym także wobec najbliższych;

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

21) umieszczania kluczy do szaf w ustalonym, przeznaczonym do tego odpowiednio zabezpieczonym miejscu po zakończeniu dnia pracy;

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

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

24) zamykania drzwi na klucz po zakończeniu pracy w danym dniu. Jeśli niemożliwe jest umieszczenie wszystkich dokumentów zawierających dane osobowe w zamykanych szafach, należy powiadomić o tym ABI.

4. Postępowanie z nośnikami przenośnymi i ich bezpieczeństwo

Osoby upoważnione do przetwarzania danych osobowych powinny pamiętać zwłaszcza, że:

1) dane z nośników przenośnych niebędących kopiami zabezpieczającymi 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 kart, 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.

5. 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 jednostek. Pozwala to – przynajmniej w pewnym stopniu – uniknąć wielokrotnego wprowadzania tych samych danych do systemu informatycznego Administratora Danych.

2. Sporządzanie kopii zabezpieczających następuje w trybie opisanym w pkt VIII „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych”.

3. Inne wymogi bezpieczeństwa systemowego są określane w instrukcjach obsługi producentów sprzętu i używanych programów, wskazówkach Administratora Bezpieczeństwa Informacji oraz „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych”.

4. Pocztą elektroniczną można przesyłać tylko jednostkowe dane, a nie całe bazy lub szerokie z nich wypisy i tylko w postaci zaszyfrowanej. Chroni to przesyłane dane przed „przesłuchami” na liniach teletransmisyjnych oraz przed przypadkowym rozproszeniem ich w Internecie.

5. Przed atakami z sieci zewnętrznej wszystkie komputery Administratora Danych (w tym także przenośne) chronione są środkami dobranymi przez Administratora Systemu Informatycznego w porozumieniu z Administratorem Bezpieczeństwa Informacji. 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 Bezpieczeństwa Informacji lub pracowników działu informatyki oraz umożliwić im monitorowanie oraz aktualizację środków (urządzeń, programów) bezpieczeństwa.

6. Administrator Systemu Informatycznego 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 i powiększania bazy danych. Jednocześnie należy zwracać uwagę, czy rozwijający się system zabezpieczeń sam nie wywołuje nowych zagrożeń.

7. Należy stosować następujące sposoby kryptograficznej ochrony danych:
   - przy przesyłaniu danych za pomocą poczty elektronicznej stosuje się POP – tunelowanie, szyfrowanie połączenia,
   - przy przesyłaniu danych pracowników, niezbędnych do wykonania przelewów wynagrodzeń, używa się bezpiecznych stron szyfrowanych protokołem SSL oznaczonych jako https://.

6. Kontrola dostępu do systemu

Poszczególnym osobom upoważnionym do przetwarzania danych osobowych przydziela się konta opatrzone niepowtarzalnym identyfikatorem, umożliwiające dostęp do danych, zgodnie z zakresem upoważnienia do ich przetwarzania. Administrator Systemu Informatycznego po uprzednim przedłożeniu upoważnienia do przetwarzania danych osobowych, zawierającego odpowiedni wniosek, przydziela pracownikowi upoważnionemu do przetwarzania danych konto w systemie informatycznym, dostępne po wprowadzeniu prawidłowego identyfikatora i uwierzytelnieniu hasłem.
W razie potrzeby, po uzyskaniu uprzedniej akceptacji Administratora Bezpieczeństwa Informacji, Administrator Systemu Informatycznego może przydzielić konto opatrzone identyfikatorem osobie upoważnionej do przetwarzania danych osobowych, nieposiadającej statusu pracownika.
Pierwsze hasło wymagane do uwierzytelnienia się w systemie przydzielane jest przez Administratora Bezpieczeństwa Informacji po odebraniu od osoby upoważnionej do przetwarzania danych. Przekazanie tego hasła jest potwierdzone „Protokołem przekazania użytkownikowi systemu informatycznego identyfikatora i hasła”.
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 Bezpieczeństwa Informacji i Administratora Systemu Informatycznego.

7. Kontrola dostępu do sieci

1. System informatyczny posiada połączenie z publiczną siecią telekomunikacyjną (Internetem). Dostęp do niego jest jednak ograniczony na poziomie protokołów komunikacyjnych na routerze brzegowym.

2. Administrator Danych blokuje dostęp inicjowany od strony sieci Internet do sieci Administratora Danych na routerze brzegowym poprzez translację adresów NAT. Uniemożliwia to dostęp do systemu przetwarzającego dane osobowe przez użytkowników sieci Internet.

3. Na jednostkach przetwarzających dane osobowe uruchomiona jest lokalna zapora sieciowa ang. firewall.

4. Korzystanie z zasobów sieci wewnętrznej (intranet) jest możliwe tylko w zakresie uprawnień przypisanych do danego konta osoby upoważnionej do przetwarzania danych osobowych.

5. Operacje za pośrednictwem rachunku bankowego Administratora Danych może

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

8. Komputery przenośne i praca na odległość

1. Urządzenia przenośne oraz nośniki danych wynoszone z siedziby Administratora Danych 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 miejscach publicznych, ani też w samochodach.

3. Informacje przechowywane na urządzeniach przenośnych lub komputerowych nośnikach danych należy chronić przed uszkodzeniami fizycznymi, a ze względu na działanie 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 osoba upoważniona do przetwarzania danych osobowych, 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. Użytkownik powinien zachować w tajemnicy wobec domowników identyfikator i hasło, których podanie jest konieczne do rozpoczęcia pracy na komputerze przenośnym Administratora Danych.

6. Administrator Systemu Informatycznego w razie potrzeby wskazuje w dokumencie powierzenia komputera przenośnego osobie upoważnionej do przetwarzania danych osobowych konieczność i częstotliwość sporządzania kopii zabezpieczających danych przetwarzanych na komputerze przenośnym oraz określa zasady:

- postępowania w razie nieobecności w pracy dłuższej niż 5 dni. Jeśli komputer przenośny nie może być zwrócony przed okresem nieobecności, to użytkownik tego komputera powinien niezwłocznie powiadomić o tym Administratora Bezpieczeństwa Informacji i uzgodnić z nim zwrot komputera przenośnego Administratorowi Danych;
- zwrotu sprzętu w razie zakończenia pracy u Administratora Danych.

7. W zakresie nieuregulowanym w polityce bezpieczeństwa stosuje się do pracy z wykorzystaniem komputerów przenośnych postanowienia instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

9. Monitorowanie dostępu do systemu i jego użycia

System informatyczny Administratora Danych odnotowuje następujące zdarzenia:

1) daty pierwszego wprowadzenia danych do systemu,
2) identyfikatora użytkownika wprowadzającego dane osobowe do systemu,

Odnotowanie informacji, o których mowa w pkt 1 i 2, następuje automatycznie po

zatwierdzeniu przez użytkownika operacji wprowadzenia danych.
Administrator Systemu Informatycznego przeprowadza synchronizację zegarów stacji roboczych z serwerem ntp, ograniczając dopuszczalność zmian w ustawieniach zegarów. Jakiekolwiek zmiany ustawień zegarów mogą być dokonywane jedynie przez pracowników działu informatyki z konta o uprawnieniach administracyjnych.
System informatyczny Administratora Danych umożliwia zapisywanie zdarzeń wyjątkowych na potrzeby audytu i przechowywanie informacji o nich przez określony czas. Zapisy takie obejmują:

1) identyfikator użytkownika,
2) datę i czas zalogowania i wylogowania się z systemu,
3) zapisy udanych i nieudanych prób dostępu do systemu,
4) zapisy udanych i nieudanych prób dostępu do danych osobowych i innych zasobów systemowych.

10. Przeglądy okresowe zapobiegające naruszeniom obowiązku szczególnej staranności Administratora Danych (art. 26 ust. 1 ustawy)

1. Administrator Bezpieczeństwa Informacji przeprowadza co dwa lata przegląd przetwarzanych danych osobowych pod kątem celowości ich dalszego przetwarzania. Osoby upoważnione do przetwarzania danych osobowych, są obowiązane 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 Administratora Danych.

3. Z przebiegu usuwania danych osobowych należy sporządzić protokół podpisywany przez Administratora Bezpieczeństwa Informacji i Wójta Gminy.

4. Wzory dokumentów przewidujących powiadomienie, o którym mowa w art. 24 lub 25 ustawy, mogą być stosowane po zaakceptowaniu przez Administratora Bezpieczeństwa Informacji.

5. Administrator Bezpieczeństwa Informacji przygotuje wykaz zbiorów danych (ewidencyjnych), w którym poszczególnym kategoriom danych osobowych przypisane zostaną okresy ich przechowywania. Wykaz ten zostanie sporządzony po przeanalizowaniu przepisów wyznaczających m.in. obowiązek przechowywania dokumentacji czy też okresy przedawnienia roszczeń udokumentowanych z wykorzystaniem danych osobowych. Przed sporządzeniem takiego wykazu przygotowany zostanie wykaz przepisów, na mocy których przetwarzane są dane osobowe, na podstawie wykazów cząstkowych, sporządzonych przez poszczególne komórki organizacyjne.

11. Odpowiedzialność osób upoważnionych do przetwarzania danych osobowych

Niezastosowanie się do prowadzonej przez Administratora Danych polityki bezpieczeństwa

przetwarzania danych osobowych, której założenia określa niniejszy dokument, i naruszenie procedur ochrony danych 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.
Niezależnie od rozwiązania stosunku pracy osoby popełniające przestępstwo będą pociągane do odpowiedzialności karnej zwłaszcza na podstawie art. 51-52 ustawy oraz art. 266 Kodeksu karnego. Przykładowo przestępstwo można popełnić wskutek:

1) stworzenia możliwości dostępu do danych osobowych osobie nieupoważnionej,
2) niezabezpieczenia nośnika lub komputera przenośnego,
3) zapoznania się z hasłem innego pracownika wskutek wykonania nieuprawnionych operacji w systemie informatycznym Administratora Danych.

Wszyscy pracownicy oraz osoby, które otrzymały pozytywną opinię Administratora Danych w Urzędzie Gminy Gościeradów (zabezpieczoną umową zapewniającą przestrzeganie przepisów dotyczących ochrony danych osobowych), pod groźbą sankcji dyscyplinarnych, mają obowiązek zachowania tajemnicy o przetwarzanych w Urzędzie Gminy Gościeradów danych osobowych oraz stosownych sposobach zabezpieczeń tych danych. Obowiązek zachowania tajemnicy istnieje również po ustaniu zatrudnienia lub współpracy.

VII. Przeglądy polityki bezpieczeństwa i audyty systemu

W razie zmian dotyczących przetwarzania danych osobowych Administrator Bezpieczeństwa Informacji może zarządzić przegląd polityki bezpieczeństwa stosownie do potrzeb.
Administrator Bezpieczeństwa Informacji analizuje, czy polityka bezpieczeństwa informacji i pozostała dokumentacja z zakresu ochrony danych osobowych jest adekwatna do:

1) zmian w budowie systemu informatycznego,
2) zmian organizacyjnych Administratora Danych, w tym również zmian statusu osób upoważnionych do przetwarzania danych osobowych,
3) zmian w obowiązującym prawie.

Administrator Bezpieczeństwa Informacji po uzgodnieniu z Wójtem może, stosownie do potrzeb, przeprowadzić wewnętrzny audyt zgodności przetwarzania danych z przepisami o ochronie danych osobowych. Przeprowadzenie audytu wymaga uzgodnienia jego zakresu z Administratorem Systemu Informatycznego. Zakres, przebieg i rezultaty audytu dokumentowane są na piśmie w protokole podpisywanym zarówno przez Administratora Bezpieczeństwa Informacji, jak i Administratora Systemu Informatycznego.
Wójt, biorąc pod uwagę wnioski Administratora Bezpieczeństwa Informacji, może zlecić przeprowadzenie audytu zewnętrznego przez wyspecjalizowany podmiot.

VIII. Postępowanie w przypadku naruszenia ochrony danych osobowych

1. Każdy pracownik Administratora Danych, w przypadku stwierdzenia lub podejrzenia naruszenia ochrony danych osobowych, jest obowiązany do niezwłocznego poinformowania o tym bezpośredniego przełożonego oraz Administratora Bezpieczeństwa Informacji.
2. Administrator Bezpieczeństwa Informacji, który stwierdził lub uzyskał informację wskazującą na naruszenie ochrony danych osobowych jest obowiązany niezwłocznie:
   - Poinformować Administratora Danych i stosować się do jego zaleceń,
   - Zapisać wszelkie informacje i okoliczności związane z danym zdarzeniem, a w szczególności dokładny czas uzyskania informacji oraz jej treść o naruszeniu ochrony danych osobowych lub samodzielnego wykrycia tego faktu,
3. Administrator Systemu Informatycznego, który stwierdził fakt lub uzyskał informację o naruszeniu bezpieczeństwa danych osobowych w systemie informatycznym jest obowiązany niezwłocznie:
   - Wygenerować i wydrukować wszystkie dokumenty i raporty, które mogą pomóc w ustaleniu wszelkich okoliczności zdarzenia, opatrzyć je datą i godziną oraz podpisać;
   - Przystąpić do zidentyfikowania rodzaju zaistniałego zdarzenia, w tym określić skalę zniszczeń, metody dostępu osoby nieuprawnionej do danych osobowych w systemie informatycznym służącym do przetwarzania danych osobowych;
   - Podjąć odpowiednie kroki w celu powstrzymania lub ograniczenia dostępu osoby nieuprawnionej do danych osobowych, zminimalizować szkody i zabezpieczyć przed usunięciem ślady naruszenia ochrony, w szczególności poprzez:
     a. Fizyczne odłączenie urządzeń i segmentów sieci, które mogły umożliwić dostęp do danych osobowych osobie nieuprawnionej,
     b. Wylogowanie użytkownika podejrzanego o naruszenie bezpieczeństwa danych osobowych,
     c. Zmianę hasła użytkownika, przez konto którego uzyskano nielegalny dostęp do danych osobowych w celu uniknięcia ponownej próby uzyskania takiego dostępu,
   - Dokonać szczegółowej analizy stanu systemu informatycznego w celu potwierdzenia lub wykluczenia faktu naruszenia bezpieczeństwa danych osobowych;
   - Przywrócić prawidłowe działanie systemu informatycznego służącego przetwarzaniu danych osobowych.
4. Po przywróceniu prawidłowego stanu, należy przeprowadzić szczegółową analizę, w celu określenia przyczyn naruszenia ochrony danych osobowych lub podejrzenia takiego naruszenia, oraz podjąć kroki, mające na celu wyeliminowanie podobnych zdarzeń w przyszłości.
5. Jeżeli przyczyną zdarzenia był błąd użytkownika, należy przeprowadzić szkolenie wszystkich osób biorących udział w procesie przetwarzania danych osobowych

w Urzędzie Gminy Gościeradów.

6. Jeżeli przyczyną zdarzenia była infekcja wirusem lub innym szkodliwym oprogramowaniem, należy ustalić źródło jego pochodzenia i utworzyć zabezpieczenia antywirusowe oraz organizacyjne, wykluczające podobne zdarzenia w przyszłości.
7. Jeżeli przyczyną zdarzenia było zaniedbanie ze strony użytkownika należy wyciągnąć wobec niego konsekwencje dyscyplinarne wynikające z przepisów prawa pracy oraz wewnętrznych uregulowań Urzędu Gminy Gościeradów. W przypadku, kiedy użytkownik nie jest pracownikiem Administratora Danych, konsekwencje wynikające z umowy, na podstawie której osoba ta posiada uprawnienia do przetwarzania danych osobowych w Urzędzie Gminy Gościeradów.
8. Administrator Bezpieczeństwa Informacji przygotowuje szczegółowy raport o przyczynach, przebiegu i wnioskach ze zdarzenia naruszenia bezpieczeństwa danych osobowych i przekazuje go Administratorowi Danych. Jeżeli zdarzenie dotyczyło naruszenia zabezpieczeń systemu informatycznego służącego przetwarzaniu danych osobowych to Administrator Bezpieczeństwa Informacji w przygotowaniu raportu współpracuje z Administratorem Systemu Informatycznego.

IX. Postępowanie w wypadku klęski żywiołowej

Klęska żywiołowa jest katastrofą, spowodowaną działaniem sił przyrody takich jak ogień, huragan, woda lub ich przejawami.
W przypadku wystąpienia zagrożenia powodującego konieczność przeprowadzenia ewakuacji osób lub mienia z pomieszczeń, w których przetwarzane są dane osobowe, mają zastosowanie przepisy niniejszego rozdziału oraz innych przepisów szczegółowych.

1. O zagrożeniu, jego skali i podjętych krokach zaradczych osoba kierująca ewakuacją zobowiązana jest powiadomić Administratora Bezpieczeństwa Informacji. W razie niemożności skontaktowania się z nim zawiadamia Wójta Gminy. Numery telefonów Administratora Bezpieczeństwa Informacji i Wójta powinny być znane pracownikom.
2. Osoby biorące udział w akcji ratunkowej moją prawo wejść do pomieszczeń, w których przetwarzane są dane osobowe bez dopełnienia obowiązku o którym mowa w rozdziale polityki bezpieczeństwa informacji.
3. W przypadku ogłoszenia alarmu ewakuacyjnego użytkownicy przebywający w pomieszczeniach, w których są dane osobowe, obowiązani są do przerwania pracy – w miarę możliwości przed opuszczeniem tych pomieszczeń do:
   - zamknięcia systemu informatycznego,
   - zabezpieczenia danych osobowych gromadzonych w kartotekach.
4. W czasie trwania akcji ratunkowej i po jej zakończeniu Administrator Bezpieczeństwa Informacji oraz obecni użytkownicy powinni, w miarę możliwości, zabezpieczyć dane osobowe przed nieuprawnionym do nich dostępem.

5. Obowiązek ten ciąży w równym stopniu na innych pracownikach Administratora Danych, obecnych przy akcji ratunkowej.

X. Postanowienia końcowe

Polityka bezpieczeństwa informacji jest dokumentem wewnętrznym Urzędu Gminy Gościeradów i jest objęta obowiązkiem zachowania w poufności przez wszystkie osoby, którym zostanie ujawniona.

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

Polityka bezpieczeństwa informacji wchodzi w życie od dnia 9 kwietnia 2013 r.