WÓJT GMINY SZCZUTOWO
09-227 Szczutowo, ul. Lipowa 5a
woj. mazowieckie
tel. 276 71 67
(1)

Zarządzenie Nr Or. 120. 41 . 2012
Wójta Gminy Szczutowo
z dnia 20 lipca 2012 r.

w sprawie wprowadzenia w życie „Polityki bezpieczeństwa danych osobowych w Urzędzie Gminy Szczutowo" oraz „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Szczutowo".

Na podstawie art. 36 ust. 2 ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.) oraz §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. Nr 100, poz. 1024) zarządzam, co następuje:

§1

Wprowadza się „Politykę bezpieczeństwa danych osobowych w Urzędzie Szczutowo", stanowiącą Załącznik Nr 1 do niniejszego Zarządzenia.

§2

Wprowadza się „Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Szczutowo", stanowiącą Załącznik Nr 2 do niniejszego Zarządzenia.

§3

Wszelkiego rodzaju oświadczenia oraz upoważnienia do przetwarzania danych osobowych sporządzone na podstawie przepisów wewnętrznych dotychczas obowiązujących, o których mowa w § 4 zachowują ważność.

§4

Traci moc Zarządzenie Nr 61 /08 Wójta Gminy Szczutowo z dnia 11 lutego 2008 roku
W sprawie wprowadzenia:

1. „Polityki bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy w Szczutowie"
2. „Instrukcji zarządzania systemem informatycznym w Urzędzie Gminy w Szczutowie

§5

1. Administrator Danych Osobowych dostosuje dokumentację wewnętrzną do zgodności z niniejszym zarządzeniem, w terminie 3 miesięcy od daty wejścia w życie zarządzenia.
2. Zarządzenie wchodzi w życie z dniem podpisania.

Wójt Gminy Szczutowo

Andrzej Twardowski

WÓJT GMINY SZCZUTOWO
09-227 Szczutowo, ul. Lipowa 5a
woj. mazowieckie
tel. 276 71 67
(1)

Załącznik Nr 1
do Zarządzenia Nr Or.120.41 .2012
Wójta Gminy Szczutowo
z dnia 20 lipca 2012 r.

POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH
w Urzędzie Gminy Szczutowo

Rozdział 1. Postanowienia ogólne.

§ 1. Podstawa prawna

Podstawę prawną dla polityki bezpieczeństwa danych osobowych w Urzędzie Gminy Szczutowo stanowią:

1) Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. (tekst jednolity z 2002 roku Dz. U. Nr 101 poz. 926, z późn. zm.);
2) 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).

§ 2. Definicje

Definicje stosowanych pojęć:

1) **Polityka bezpieczeństwa** – „Polityka bezpieczeństwa danych osobowych w Urzędzie Gminy w Szczutowie;
2) **dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby;
3) **osoba możliwa do zidentyfikowania** – każda osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne;
4) **zbiór danych** – każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie;
5) **komputerowy zbiór danych** – zbiór danych osobowych w formie elektronicznej;
6) **tradycyjny zbiór danych** – zbiór danych osobowych w formie papierowej (np. księgi, wykazy, ewidencje);
7) **przetwarzanie danych** – 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;
8) **Urząd** – Urząd Gminy w Szczutowie, z siedzibą: ul. Lipowa 5A; 09 – 227 Szczutowo;
9) **Administrator Danych Osobowych - dale (ADO)**– Wójt Gminy Szczutowo, reprezentujący Urząd, który decyduje o celach i środkach przetwarzania danych osobowych oraz monitoruje wdrożone zabezpieczenia systemu informatycznego;
10) **Administrator Bezpieczeństwa Informacji – dalej (ABI)** osoba nadzorująca przestrzeganie zasad przetwarzania i ochrony danych osobowych;
11) **Administrator Systemów Informatycznych (dalej ASI)** – osoba odpowiedzialna za bezpieczeństwo danych osobowych przetwarzanych w systemach informatycznych w Urzędzie, w tym w szczególności za przeciwdziałanie dostępowi osób trzecich do systemów oraz podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w tych systemach;
12) **GIODO** – Generalny Inspektor Ochrony Danych Osobowych lub osoba przez niego upoważniona zwana dalej osobą uprawnioną;
13) **osoba upoważniona** – osoba posiadająca upoważnienie do przetwarzania danych osobowych w określonym zakresie wydane przez Administratora Danych Osobowych;

14) **osoba uprawniona** – osoba upoważniona lub inna osoba uprawniona do przetwarzania danych osobowych na podstawie szczególnych przepisów prawa (lex specialis)- np. Inspektor GIODO;
15) **osoba trzecia** – każda osoba nieuprawniona do przetwarzania danych osobowych będących w posiadaniu Administratora Danych Osobowych, a także osoba posiadająca upoważnienie wydane przez Administratora Danych Osobowych, ale podejmująca czynności w zakresie przekraczającym zakres jej upoważnienia;
16) **użytkownik** – osoba upoważniona do przetwarzania danych osobowych w określonym zakresie w systemie informatycznym;
17) **stacja robocza** - stacjonarny lub przenośny komputer, umożliwiający użytkownikowi dostęp do danych przetwarzanych w formie elektronicznej;
18) **zewnętrzne nośniki danych** - przedmiot fizyczny służący do zapisywania, przechowywania, przetwarzania i transmisji danych (np. pendrive, CD, DVD);
19) **system informatyczny** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
20) **zakres czynności** – zakres czynności, upoważnień, odpowiedzialności i zastępstwa określony w opisie stanowiska;
21) **zabezpieczenie systemu informatycznego** – wdrożone przez ABI i ASI odpowiednie środki organizacyjne i techniczne w celu zabezpieczenia zasobów oraz ochrony danych przed dostępem, modyfikacją ujawnieniem, pozyskaniem lub zniszczeniem przez użytkownika lub osobę trzecią;
22) **Zapewnienie bezpieczeństwa systemów informatycznych** oznacza, utrzymanie takich atrybutów informacji jak:
    a) **poufność** – rozumie się przez to ograniczony i ściśle zdefiniowany krąg osób mających dostęp do informacji;
    b) **integralność** – rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
    c) **rozliczalność** – rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;
    d) **uwierzytelnianie** – rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu za pomocą:
        - **identyfikatora użytkownika** – przypisanego jednej osobie identyfikatora jednoznacznie określającego użytkownika w systemie informatycznym;
        - **hasła** – ciągu znaków (stanowiącego tajemnicę użytkownika), który w połączeniu z identyfikatorem użytkownika umożliwia uwierzytelnienie go w systemie informatycznym.

Rozdział 2. Cel i zakres polityki bezpieczeństwa danych osobowych

§ 3. Cel polityki bezpieczeństwa

1. Celem niniejszej Polityki jest określenie kierunków działań oraz wsparcia dla zapewnienia wysokiego bezpieczeństwa przetwarzania danych osobowych w Urzędzie Miasta Bielsk Podlaski.
2. Przez bezpieczeństwo danych osobowych rozumie się zapewnienie ich poufności, integralności, dostępności oraz rozliczalności działań podejmowanych zgodnie z niniejszą Polityką.
3. Urząd zarządza bezpieczeństwem danych osobowych w celu:
    1) zapewnienia sprawnego i zgodnego z przepisami prawa wykonywania swoich zadań oraz zadań realizowanych na podstawie umów lub porozumień;
    2) minimalizacji ryzyk w obszarze przetwarzania i ochrony danych osobowych, o których mowa w ust. 4.
4. Wdrożenie niniejszej polityki bezpieczeństwa przez Urząd ma na celu zabezpieczenie danych osobowych przetwarzanych w związku z wykonywaniem zadań Administratora Danych Osobowych oraz podejmowanie wszelkich możliwych działań koniecznych do zapobiegania zdarzeniem naruszającym ochronę danych osobowych, o których mowa w § 5 niniejszej Polityki bezpieczeństwa.

§ 4. Zakres polityki bezpieczeństwa

1. Zakres przedmiotowy niniejszej Polityki obejmuje dane osobowe przetwarzane w Urzędzie, zarówno w formie elektronicznej, jak i tradycyjnej.
2. Procedury i zasady określone w niniejszej Polityce stosuje się do wszystkich pracowników Urzędu, jak i innych osób mających dostęp do danych osobowych przetwarzanych w Urzędzie (np. osób realizujących zadania na podstawie umów zlecenia lub o dzieło, wolontariuszy, stażystów, praktykantów, serwisantów). § 4. 0
3. Niniejsza „Polityka bezpieczeństwa" zawiera w szczególności:
   1) wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe;
   2) wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych;
   3) opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi;
   4) sposób przepływu danych pomiędzy poszczególnymi systemami;
   5) określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

§ 5. Opis zdarzeń naruszających ochronę danych osobowych

1. Zagrożenia naruszające ochronę danych osobowych dziali się na:
   1) **zagrożenia losowe zewnętrzne** (np. klęski żywiołowe, przerwy w zasilaniu), ich występowanie może prowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej systemu, ciągłość systemu zostaje zakłócona, nie dochodzi do naruszenia poufności danych;
   2) **zagrożenia losowe wewnętrzne** (np. niezamierzone pomyłki operatorów, administratora, awarie sprzętowe, błędy oprogramowania), może dojść do zniszczenia danych, może zostać zakłócona ciągłość pracy systemu, może nastąpić naruszenie poufności danych;
   3) **zagrożenia zamierzone**, świadome i celowe - najpoważniejsze zagrożenia, naruszenia poufności danych, (zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy), zagrożenia te możemy podzielić na:
      a) nieuprawniony dostęp do systemu z zewnątrz (włamanie do systemu);
      b) nieuprawniony dostęp do systemu z jego wnętrza;
      c) nieuprawniony przekaz danych;
      d) pogorszenie jakości sprzętu i oprogramowania;
      e) bezpośrednie zagrożenie materialnych składników systemu.
2. Przypadki zakwalifikowane jako naruszenie lub uzasadnione podejrzenie naruszenia zabezpieczenia systemu informatycznego, w którym przetwarzane są dane osobowe to głównie:
   1) sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu jak np.: wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej itp.;
   2) niewłaściwe parametry środowiska, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy lub wibracje pochodzące od urządzeń przemysłowych;
   3) awaria sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych lub wręcz sabotaż, a także niewłaściwe działanie serwisu, a w tym sam fakt pozostawienia serwisantów bez nadzoru;
   4) pojawienie się odpowiedniego komunikatu alarmowego od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu;
   5) jakość danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie;

6) nastąpiło naruszenie lub próba naruszenia integralności systemu lub bazy danych w tym systemie;
7) stwierdzono próbę lub modyfikację danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji);
8) nastąpiła niedopuszczalna manipulacja danymi osobowymi w systemie;
9) ujawniono osobom nieupoważnionym dane osobowe lub objęte tajemnicą procedury ochrony przetwarzania albo inne strzeżone elementy systemu zabezpieczeń;
10) praca w systemie lub jego sieci komputerowej wykazuje nieprzypadkowe odstępstwa od założonego rytmu pracy wskazujące na przełamanie lub zaniechanie ochrony danych osobowych - np. praca przy komputerze lub w sieci osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu, itp.;
11) ujawniono istnienie nieautoryzowanych kont dostępu do danych lub tzw. "bocznej furtki", itp.;
12) podmieniono lub zniszczono nośniki z danymi osobowymi bez odpowiedniego upoważnienia lub w sposób niedozwolony skasowano lub skopiowano dane osobowe;
13) rażąco naruszono dyscyplinę pracy w zakresie przestrzegania procedur bezpieczeństwa informacji (nie wylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych osobowych w drukarce, na ksero, nie zamknięcie pomieszczenia z komputerem, nie wykonanie w określonym terminie kopii bezpieczeństwa, prace na danych osobowych w celach prywatnych, itp.).

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

Rozdział 3
Organizacja przetwarzania danych osobowych

§ 6. Prawa i obowiązki Administratora Danych Osobowych (Wójta)

1. Administrator Danych Osobowych (Wójt) :
   1) Określa zasady postępowania przy przetwarzaniu danych osobowych;
   2) Przetwarza dane osobowe zgodnie z prawem oraz realizuje zadania w zakresie ochrony danych osobowych;
   3) Podejmuje decyzje o celach i środkach przetwarzania danych osobowych uwzględniając zmiany: prawodawstwa, organizacyjne w Urzędzie oraz technik zabezpieczenia danych osobowych;
   4) Wyznacza ABI oraz określa zakres jego zadań w szczegółowym zakresie czynności, uprawnień i odpowiedzialności, o ile sam nie wykonuje czynności związanych z ochroną danych osobowych, na podstawie art. 36 ust. 3 ustawy;
   5) Zgłasza zbiory danych do rejestracji bądź zgłasza zmiany w zbiorach danych osobowych zarejestrowanych w GIODO;
   6) Udostępnia dane osobowe ze zbiorów, na żądanie uprawnionych podmiotów w przypadkach wskazanych prawem bądź odmawia ich udostępnienia;
   7) Na wniosek ABI:
      a) wyznacza bądź zleca wykonywanie obowiązków ASI spośród osób mających przygotowanie informatyczne;
      b) upoważnia poszczególne osoby do przetwarzania danych osobowych w Urzędzie, w stosownym, indywidualnie określonym zakresie. **Wzór upoważnienia do przetwarzania danych osobowych** określa **załącznik nr 1** do niniejszej polityki.
   8) Podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia procedur bezpiecznego przetwarzania danych osobowych;
   9) Zabezpiecza dane osobowe przed ich udostępnianiem lub pozyskaniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy o ochronie danych osobowych, nieautoryzowaną zmianą, utratą, uszkodzeniem lub zniszczeniem danych zawartych w zbiorach.

§ 7. Zakres zadań i obowiązków Administratora Bezpieczeństwa Informacji (ABI)

1. Administrator Bezpieczeństwa Informacji :
   1) Sprawuje nadzór nad przestrzeganiem zasad przetwarzania i ochrony danych osobowych w imieniu i na rzecz Administratora Danych Osobowych;
   2) Sprawuje nadzór nad wdrożeniem odpowiednich środków organizacyjnych, technicznych i fizycznych w celu zapewnienia bezpieczeństwa danych osobowych przetwarzanych w Urzędzie;
   3) Wnioskuje do Administratora Danych Osobowych o wprowadzanie nowych rozwiązań i zmian organizacyjnych, jeżeli wpłyną na poprawę ochrony danych osobowych w Urzędzie, w tym nadanie, modyfikację lub odwołanie upoważnienia do przetwarzania danych osobowych w Urzędzie;
   4) prowadzi zbiory przepisów, w tym przepisów wewnętrznych dotyczących przetwarzania danych osobowych (polityki, instrukcje) w Urzędzie, oraz utrzymuje te zbiory w stałej aktualności, w szczególności:
      a) „Polityki bezpieczeństwa danych osobowych";
      b) „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych".
   5) Zakłada, prowadzi i aktualizuje dokumentację wynikającą z przepisów prawa powszechnie obowiązującego oraz przepisów wewnętrznych (polityk, instrukcji, itp.), w szczególności prowadzi :
      a) **Wykaz budynków i pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe** – wg wzoru stanowiącego **Załącznik nr 2** do niniejszej Polityki bezpieczeństwa;
      b) **Granice obszarów oraz osoby, które przetwarzają dane osobowe** – wg wzoru stanowiącego **Załącznik nr 3** do niniejszej Polityki bezpieczeństwa;
      c) **Wykaz zbiorów danych osobowych i programów zastosowanych do ich przetwarzania** – wg wzoru stanowiącego **Załącznik nr 4** do niniejszej Polityki bezpieczeństwa ;
      d) **Opis struktury zbiorów danych przetwarzanych w Urzędzie** - wg wzoru stanowiącego **Załącznik nr 5** do niniejszej Polityki bezpieczeństwa ;
      e) **Ewidencję osób upoważnionych do przetwarzania danych osobowych w Urzędzie** – wg wzoru stanowiącego **Załącznik nr 6** do niniejszej Polityki bezpieczeństwa;
      f) **Ewidencję nadanych identyfikatorów dostępu do systemów informatycznych** – wg wzoru stanowiącego **załącznik Nr 7** do niniejszej Polityki bezpieczeństwa.
   6) Prowadzi sprawy dotyczące przetwarzania danych osobowych w Urzędzie, w tym teczki aktowe dotyczące: rejestracji zbiorów do GIODO, szkoleń pracowników w zakresie ochrony danych osobowych, kontroli przestrzegania ochrony danych osobowych, stwierdzenia naruszeń bezpieczeństwa danych itp. ;
   7) Nadzoruje prace wykonywane przez ASI w Urzędzie.

§ 8. Zakres zadań i obowiązków Administratora Systemów Informatycznych (ASI)

1. ASI realizuje zadania w zakresie zarządzania i bieżącego nadzoru nad systemem informatycznym Administratora Danych Osobowych, w szczególności:
   1) Zarządza systemem informatycznym, w którym przetwarzane są dane osobowe, posługując się hasłem dostępu do wszystkich stacji roboczych z poziomu administratora;
   2) Zarządza systemem komunikacji w sieci komputerowej oraz przesyłania danych za pośrednictwem urządzeń teletransmisji;
   3) Nadzoruje funkcjonowanie mechanizmów uwierzytelniania użytkowników w systemie informatycznym służącym do przetwarzania danych osobowych oraz kontroli dostępu do danych osobowych;
   4) Przeciwdziała dostępowi osób nieupoważnionych do systemu informatycznego;

5) Na wniosek ABI:
   a) przydziela każdemu użytkownikowi identyfikator i hasło dostępu do systemu informatycznego bądź dokonuje ewentualnych modyfikacji uprawnień;
   b) zmienia w poszczególnych stacjach roboczych hasła dostępu, ujawniając je wyłącznie danemu użytkownikowi, a w razie potrzeby ADO i ABI;
   c) wyrejestrowuje użytkowników z systemu.
6) W sytuacji stwierdzenia naruszenia zabezpieczeń systemu informatycznego informuje ABI o naruszeniu i współdziała z nim w usuwaniu skutków naruszenia;
7) Nadzoruje wykonanie napraw, konserwację lub likwidację urządzeń komputerowych, na których zapisane są dane osobowe, sprawuje nadzór nad wykonaniem kopii zapasowych, ich przechowywaniem oraz okresowym sprawdzaniem pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu informatycznego;
8) 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.

§ 9. Zakres zadań i obowiązków Kierowników referatów

1. Kierownicy referatów realizując ochronę danych osobowych w Urzędzie są odpowiedzialni za:
   1) Nadzorowanie przestrzegania zasad przetwarzania i ochrony danych osobowych przyjętych w Urzędzie przez podległych pracowników, w szczególności:
      a) przetwarzania danych osobowych w celu i zakresie określonym w imiennym upoważnieniu do przetwarzania danych osobowych;
      b) stosowania przydzielonych im indywidualnych identyfikatorów dostępu do systemu informatycznego przez podległych pracowników;
      c) przeciwdziałania dostępowi osób nieuprawnionych do danych osobowych i systemu informatycznego, w którym są przetwarzane;
      d) prawidłowego zabezpieczania danych osobowych oraz miejsc ich przechowywania w trakcie i po zakończeniu pracy;
   2) Niedopuszczenie do używania zewnętrznych nośników danych do celów innych niż niezbędne do realizacji zadań referatu lub tworzenia kopii bezpieczeństwa, z wyjątkiem sytuacji gdy jest to niezbędne ze względu na specyfikę zadania;
   3) Współdziałanie z ABI w zakresie przestrzegania zasad przetwarzania i ochrony danych osobowych w Urzędzie oraz identyfikacji i analizy ryzyk z tym związanych;
   4) Niezwłoczne informowanie ABI , o każdym stwierdzeniu lub podejrzeniu naruszenia bezpieczeństwa danych osobowych lub systemu informatycznego, w którym są przetwarzane oraz współdziałanie przy usuwaniu skutków takiego naruszenia.

§ 10. Zakres zasad, obowiązków i odpowiedzialności osób przetwarzających dane osobowe w Urzędzie

1. Osoby upoważnione do przetwarzania danych osobowych, zobowiązane są w szczególności do:
   1) Przetwarzania danych osobowych wyłącznie w zakresie ustalonym indywidualnie przez Administratora Danych Osobowych w upoważnieniu i tylko w celu wykonywania nałożonych na nią obowiązków;
   2) Poznania i bezwzględnego przestrzegania obowiązujących u Administratora Danych Osobowych zasad przetwarzania i ochrony danych osobowych oraz bezpieczeństwa systemu informatycznego;
   3) Zachowania w tajemnicy danych, które przetwarza oraz sposobów ich zabezpieczenia przez cały okres zatrudnienia u Administratora Danych Osobowych, a także po ustaniu stosunku pracy lub odwołaniu z pełnionej funkcji;
   4) korzystania z systemu informatycznego Administratora Danych Osobowych w sposób zgodny ze wskazówkami zawartymi w instrukcjach obsługi urządzeń wchodzących w skład systemu informatycznego, oprogramowania i nośników oraz zasadami przyjętymi w Urzędzie;

5) zabezpieczania danych osobowych oraz informacji o zabezpieczeniach systemu informatycznego przed ich udostępnianiem osobom nieuprawnionym, nieuprawnioną modyfikacją, utratą lub zniszczeniem;
6) Kasowania po wykorzystaniu danych na dyskach przenośnych (dyskietka, CD-Rom, Kongston, itp);
7) Nieużywania powtórnego jednostronne drukowanych dokumentów zawierających dane osobowe;
8) Niepodawania w treści korespondencji wychodzącej z Urzędu (pisma, decyzje, itp.) do wiadomości stronom postępowania, danych adresowych stron. Rozdzielniki stron pozostają w aktach Urzędu;
9) Pilnego strzeżenia na stanowiskach służbowych akt i dysków przenośnych;
10) Niepozostawiania bez kontroli, dokumentów, nośników danych i sprzętu komputerowego w miejscach publicznych, pojazdach itp.;
11) Ustawiania ekranów komputerowych tak, aby osoby niepowołane nie mogły oglądać zawartości, a zwłaszcza nie naprzeciwko wejścia do pomieszczenia;
12) Niezapisywania hasła wymaganego do uwierzytelnienia się w systemie na papierze lub innym nośniku;
13) Niepodłączania do listew podtrzymujących napięcie przeznaczonych do systemu komputerowego innych urządzeń (np. czajników elektrycznych, grzejników, wentylatorów, itp.);
14) Dbania o prawidłową wentylację komputerów (unikać zasłaniania kratek wentylatorów meblami, ustawiania bezpośrednio przy ścianie, itp.);
15) Powstrzymywania od samodzielnej ingerencji w oprogramowanie i konfigurację powierzonego sprzętu, nawet gdy mogłoby to usprawnić pracę lub nawet podnieść poziom bezpieczeństwa danych;
16) Przestrzegania zasad korzystania z uprawnień w systemie (używanie wyłącznie własnego identyfikatora i hasła oraz stosowanie się do zaleceń ABI i ASI;
17) Niepozostawiania osób postronnych w pomieszczeniach, w których przetwarzane są dane osobowe, bez obecności osoby upoważnionej do przetwarzania danych osobowych;
18) Opuszczania stanowiska pracy dopiero po aktywowaniu wygaszacza ekranu lub po zablokowaniu stacji roboczej w inny sposób;
19) Kopiowania całych zbiorów danych osobowych na jednym nośniku, za wyjątkiem tworzenia kopii bezpieczeństwa, których procedurę określa „Instrukcja zarządzania systemem informatycznym w Urzędzie Gminy w Szczutowie;
20) Kopiowania na jednym nośniku informatycznym tylko jednostkowych danych (pojedynczych plików), które po wykorzystaniu niezwłocznie się usuwa.
21) Wynoszenia danych osobowych na jakichkolwiek nośnikach (papierowych, elektronicznych) poza obszar przetwarzania, nie związany z wypełnianiem obowiązków służbowych;
22) Wykonywania kopii roboczych danych, na których się właśnie pracuje, tak często, aby zapobiec ich ewentualnej utracie;
23) Dochowania szczególnej staranności przy udostępnianiu danych osobowych, uwzględniając procedury określone w rozdziale III niniejszej polityki;
24) 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;
25) Niszczenia w sposób uniemożliwiający dokonanie odczytu (np. niszczarce) lub chowania do szaf zamykanych na klucz wszelkich wydruków zawierających dane osobowe, przed każdorazowym opuszczeniem stanowiska pracy;
26) Zamykania okien w pomieszczeniach, w których przetwarzane są dane osobowe w czasie intensywnych opadów atmosferycznych, w czasie wyładowań atmosferycznych, w razie opuszczania pomieszczeń oraz po zakończeniu dnia pracy;

27) Każdorazowego zamykania na klucz drzwi wejściowych do pomieszczeń, w których przetwarzane są dane osobowe, jeżeli w tych pomieszczeniach nie przebywają inni współpracownicy. W takich przypadkach klucz zabiera ze sobą pracownik lub zdaje na sekretariacie Urzędu.

2. Każda osoba przetwarzająca dane osobowe posiada odpowiednie upoważnienie do przetwarzania danych osobowych zawierające: imię i nazwisko, datę nadania i okres jego obowiązywania, zakres lub zbiory danych, które osoba upoważniona może przetwarzać. **Wzór upoważnienia do przetwarzania danych osobowych** określa **załącznik Nr 1** do niniejszej polityki bezpieczeństwa.
3. Każdej osobie przetwarzającej dane osobowe w systemach informatycznych na wniosek Administratora Danych Osobowych - Administrator Systemów Informatycznych nadaje niepowtarzalny identyfikator i hasło dostępu do systemu informatycznego bądź dokonuje ewentualnych modyfikacji uprawnień. Wzór **Ewidencji nadanych identyfikatorów dostępu do systemów informatycznych** określa **załącznik Nr 7** do niniejszej polityki bezpieczeństwa.

§ 11. Uprawnienia osób, których dane dotyczą

1. Każdej osobie, której dotyczą dane osobowe przetwarzane u Administratora Danych Osobowych, przysługuje prawo do:
   1) dostępu do treści przetwarzanych danych osobowych tej osoby;
   2) poprawiania treści przetwarzanych danych osobowych tej osoby (bez zbędnej zwłoki), tj. do uzupełnienia, uaktualnienia, sprostowania danych osobowych, a także żądania czasowego lub trwałego wstrzymania ich przetwarzania bądź usunięcia ze zbioru, jeżeli są one niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy, albo są już zbędne dla realizacji celu, dla którego zostały zebrane;
   3) kontroli przetwarzanych danych osobowych tej osoby, w szczególności uzyskania informacji o:
      a) istnieniu zbioru danych osobowych i jego administratorze (wraz z siedzibą);
      b) celu, zakresie i sposobie przetwarzania danych osobowych;
      c) terminie rozpoczęcia przetwarzania danych osobowych w zbiorze;
      d) treści jej danych osobowych (podanej w powszechnie zrozumiałej formie);
      e) źródle, z jakiego pochodzą te dane (chyba że Administrator Danych Osobowych jest zobowiązany do zachowania w tym zakresie tajemnicy państwowej, służbowej lub zawodowej);
      f) sposobie udostępniania jej danych osobowych (w szczególności o odbiorcach lub kategoriach odbiorców, którym dane są udostępniane);
      g) przesłankach podjęcia rozstrzygnięcia indywidualnej sprawy uwzględniającej wniosek osoby, której dane dotyczą, podjętego podczas zawierania lub wykonywania umowy wyłącznie na podstawie operacji na danych osobowych prowadzonych w systemie informatycznym;
      h) obowiązku lub dobrowolności podania danych, a także jeśli taki obowiązek istnieje – jego podstawie prawnej;
      i) prawie dostępu do treści swoich danych i ich poprawiania, o których mowa w pkt. 1 i 2,
      j) wniesienia sprzeciwu wobec ich wykorzystania w celach marketingowych lub przekazania innemu administratorowi danych (z uwzględnieniem wyjątków ustawowych);
      k) udzielenia informacji o przysługujących prawach osobie, której dane dotyczą, na jej wniosek w terminie 30 dni.
2. W przypadku zbierania danych osobowych bezpośrednio od osoby, której one dotyczą, na jej żądanie udziela się informacji wskazanych w ust. 1 pkt 3 lit. a-f, ale nie częściej niż raz na 6 miesięcy.
3. Informacja, o której mowa w ust. 1 pkt. 3, powinna być udzielana w zrozumiałej formie oraz na piśmie, jeśli osoba o to wnioskuje.
4. W przypadku, gdy w niedużym odstępie czasowym dochodzi do ponownego lub kolejnego zbierania danych tej samej osoby do tych samych celów, można powołać się na fakt wcześniejszego udzielenia informacji, o których mowa w ust. 1 pkt. 3.

5. Obowiązek informacyjny nie występuje w przypadku, gdy:
   1) ze względu na okoliczności przekazania danych osobowych do przetwarzania w zbiorze zachodzi pewność (tj. obiektywna świadomość), że osoba, której dane dotyczą, posiada wszystkie informacje, o których mowa w ust. 1 pkt 3;
   2) dane są przetwarzane dla celów naukowych, dydaktycznych, historycznych, statystycznych lub archiwalnych, a udzielenie informacji pociągałoby za sobą nakłady niewspółmierne z zamierzonym celem;
   3) przekazanie informacji spowodowałoby:
      a) ujawnienie wiadomości zawierających informacje niejawne;
      b) zagrożenie dla obronności lub bezpieczeństwa państwa, życia lub zdrowia ludzi lub bezpieczeństwa publicznego;
      c) zagrożenie dla podstawowego interesu gospodarczego lub finansowego państwa;
      d) istotne naruszenie dóbr osobistych osób, których dane dotyczą lub innych osób.

Rozdział 4
Określenie środków technicznych i organizacyjnych, niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych

§ 12. Zachowanie poufności

1. W przypadku naboru na wolne stanowiska należy zwracać uwagę miedzy innymi na takie cechy kandydata, jak uczciwość, odpowiedzialność, przewidywalność zachowań.
2. Ryzyko utraty bezpieczeństwa danych przetwarzanych przez Administratora Danych Osobowych, pojawiające się ze strony osób trzecich, które mają dostęp do danych osobowych (np. serwisanci, usługodawcy), jest minimalizowane przez wprowadzanie do podpisanych umów zapisów powierzeniu przetwarzania danych osobowych.
3. Ryzyko ze strony osób, które potencjalnie mogą w łatwiejszy sposób uzyskać dostęp do danych osobowych (np. konserwatorzy i osoby sprzątające pomieszczenia Administratora Danych Osobowych), jest minimalizowane przez zobowiązywanie ich do zachowania tajemnicy na podstawie odrębnych, pisemnych oświadczeń. Wzór **Oświadczenia osoby upoważnionej do przetwarzania danych osobowych w Urzędzie Gminy w Szczutowie** określa **Załącznik nr 8** do niniejszej Polityki bezpieczeństwa.

§ 13. Zabezpieczenie danych osobowych

1. Administratorem danych osobowych zawartych i przetwarzanych w systemach tradycyjnych i informatycznych Urzędu jest Wójt.
2. Administrator danych osobowych jest obowiązany do zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych w systemach informatycznych Urzędu, a w szczególności:
   1) zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym;
   2) zapobiegać przed zabraniem danych przez osobę nieuprawnioną;
   3) zapobiegać przetwarzaniu danych z naruszeniem ustawy oraz zmianie, utracie, uszkodzeniu lub zniszczeniu tych danych.
3. Środki techniczne i organizacyjne niezbędne do zapewnienia poufności, integralności i wyćwiczalności danych przetwarzanych w systemie.
   1) **Środki ochrony fizycznej**:
      a) Urządzenia służące do przetwarzania danych osobowych znajdują się w pomieszczeniach zabezpieczonych zamkami patentowymi;
      b) Dostęp do pokoi posiadają wyłącznie pracownicy (po zakończeniu pracy klucze zabierane są przez pracowników). Drugi komplet kluczy znajduje się w szafie metalowej;
      c) Poza godzinami pracy Urzędu włączony jest system alarmowy;
      d) Do przechowywania nośników z kopiami zapasowymi zawierających dane osobowe stosuje się szafy metalowe zamykane na zamki patentowe;

e) Koniecznym jest wydzielenie pomieszczenia serwerowni, do którego dostęp może, tylko Administrator Bezpieczeństwa Informacji(ABI) oraz Administrator Systemu Informatycznego a inni pracownicy wyłącznie w ich obecności.

2) **Środki sprzętowe, informatyczne i telekomunikacyjne**:
   a) Stosuje się niszczarki dokumentów;
   b) Urządzenia wchodzące w skład infrastruktury sieciowej, serwera oraz komputery, na których przetwarzane są dane osobowe powinny być podłączone są do lokalnych awaryjnych zasilaczy UPS, zabezpieczających przed skokami napięcia i zanikiem zasilania;
   c) Sieć lokalna powinna być skonfigurowana w ten sposób, aby nie było możliwości dostępu do plików nie zamieszczonych na odrębnych skrzynkach poszczególnych pracowników;
   d) Nazwy skrzynek w sieci lokalnej powinny odpowiadać nazwom stanowisk (podobnie jak pierwsze człony służbowej poczty elektronicznej);
   e) Sieć lokalna powinna być podłączona do Internetu poprzez router spełniający jednocześnie funkcję sprzętowego, zewnętrznego firewalla filtrującego dane przechodzące pomiędzy siecią lokalną i siecią publiczną;
   f) Kopie zapasowe powinny być wykonywane są raz w miesiącu na nośnikach DVD.

3) **Środki ochrony w ramach oprogramowania urządzeń teletransmisji:**
   a) Na wszystkich komputerach użytkowników systemu powinien działać program antywirusowy aktualizowany automatycznie, oraz monitorujący termin wygaśnięcia licencji;
   b) Na komputerach użytkowników systemu powinien działać programowy firewall;
   c) Dostęp do serwera zawierającego dane osobowe musi być zabezpieczony hasłem.

4) **Środki ochrony w ramach oprogramowania systemu:**
   a) Dostęp do baz danych osobowych musi być bezwzględnie zastrzeżony wyłącznie dla uprawnionych pracowników;
   b) Konfiguracja systemu umożliwia użytkownikom końcowym dostęp do danych osobowych przechowywanych w systemie informatycznym wyłącznie za pośrednictwem odpowiednich aplikacji;
   c) System informatyczny powinien pozwalać zdefiniować odpowiednie prawa dostępu do zasobów informatycznych systemu odrębnie dla każdego pracownika;
   d) Należy dążyć aby każdy ściągany z internetu plik jak też przenoszony z innego komputera za pomocą dysku wymiennego (Płyta CD, DVD, USB, dyskietka, itp.) był wymuszony do przeskanowania przez system antywirusowy - działający w tle program antywirusowy na komputerach użytkowników;
   e) W systemie sieciowym stosuje się mechanizm wymuszający okresową zmianę haseł dostępu.

5) **Środki ochrony w ramach narzędzi baz danych i innych narzędzi programowych**.
   a) Dal zbiorów danych przetwarzanych w systemach informatycznych należy stosować identyfikator i hasło dostępu do danych na poziomie aplikacji;
   b) Dla każdego użytkownika systemu wyznaczony jest odrębny identyfikator;
   c) Użytkownicy mają dostęp do aplikacji umożliwiający dostęp tylko do tych danych osobowych, do których mają uprawnienia.

6) **Środki ochrony w ramach systemu użytkowego**.
   a) Komputer, z którego możliwy jest dostęp do danych osobowych musi być zabezpieczony hasłem uruchomieniowym;
   b) Należy bezwzględnie stosować wygaszenie ekranu w przypadku dłuższej nieaktywności użytkownika. Przyjmuje się, że maksymalny czas nieaktywności nie może przekroczyć 15 minut;
   c) Należy stosować blokadę hasłem podczas dłuższej nieaktywności użytkownika.

7) **Środki organizacyjne**.
   a) Wyznaczono Administratora Bezpieczeństwa Informacji;

b) Tymczasowe wydruki z danymi osobowymi są po ustaleniu ich przydatności niszczone;
c) Do przetwarzania danych osobowych przy użyciu systemu informatycznego dopuszczane są osoby na podstawie indywidualnego pozwolenia na dostęp do przetwarzania danych osobowych wydawanego przez ADO;
d) Osoby zatrudnione przy przetwarzaniu danych osobowych zobowiązane są do zachowania ich w tajemnicy;
e) Kontrolowanie otwierania i zamykania pomieszczeń, w których są przetwarzane dane osobowe, polegające na otwarciu pomieszczenia przez pierwszą osobę, która rozpoczyna pracę oraz zamknięciu pomieszczenia przez ostatnią wychodzącą osobę;
f) Osoby przetwarzające dane osobowe są przed dopuszczeniem ich do tych danych szkolone w zakresie obowiązujących przepisów o ochronie danych osobowych, procedur przetwarzania danych oraz informowane o podstawowych zagrożeniach związanych z przetwarzaniem danych osobowych w systemie informatycznym;
g) Prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych;
h) Ustalono Instrukcję Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych;
i) Zdefiniowano procedury postępowania w sytuacji naruszenia ochrony danych osobowych;
j) Zdefiniowano procedury dotyczące korzystania z internetu za pomocą komputerów służbowych;
k) Zdefiniowano zasady postępowania z komputerami przenośnymi (notebukami, laptopami, tabletami, itp.);
l) Rejestracji podlegają wszystkie przypadki awarii systemu, działania konserwacyjne w systemie oraz naprawy;
m) W przypadku, gdy zachodzi konieczność naprawy sprzętu poza siedzibą urzędu, należy wymontować z niego nośniki informacji zawierające dane osobowe;
n) W przypadku, gdy uszkodzenie sprzętu zawierającego nośnik danych, na którym zapisane są dane osobowe wymusza konieczność przekazania go poza siedzibę urzędu, nośnik ten należy wymontować.

4. Niezależnie od niniejszych zasad opisanych w Polityce bezpieczeństwa, w zakresie bezpieczeństwa mają zastosowanie wszelkie wewnętrzne regulaminy lub instrukcje dotyczące bezpieczeństwa ludzi i zasobów informacyjnych oraz indywidualne zakresy zadań osób zatrudnionych przy przetwarzaniu danych osobowych w określonym systemie.

§ 14. Szkolenia w zakresie ochrony danych osobowych.

1. Wszyscy pracownicy Urzędu mają obowiązek brać udział w szkoleniach w zakresie ochrony danych osobowych.
2. Szkolenie powinno dotyczyć:
   1) obowiązujących przepisów i instrukcji wewnętrznych dotyczących ochrony danych osobowych, sposobu niszczenia wydruków i zapisów na nośnikach informatycznych;
   2) przedstawienie zasad ochrony danych osobowych dotyczących bezpośrednio wykonywanych obowiązków na stanowisku pracy.
3. Administrator Bezpieczeństwa Informacji jest odpowiedzialny za szkolenie:
   1) każdej osoby, która ma zostać dopuszczona do przetwarzania danych osobowych;
   2) wszystkich osób upoważnionych do przetwarzania danych osobowych w przypadku:
      a) zmiany zasad przetwarzania i ochrony danych osobowych;
      b) stwierdzenia istotnych lub powtarzalnych naruszeń zasad przetwarzania i ochrony danych osobowych lub naruszenia bezpieczeństwa systemu informatycznego;
   3) osób dopuszczonych do przebywania w obszarze przetwarzania danych osobowych;

4) osób innych niż upoważnione do przetwarzania danych osobowych, jeśli pełnione przez nie funkcje wiążą się z przetwarzaniem i ochroną danych osobowych.

4. Tematyka szkoleń jest dostosowana do stanowiska/funkcji danej osoby i obejmuje:
   1) zasady przetwarzania i ochrony danych osobowych, sporządzania i przechowywania ich kopii;
   2) niszczenia wydruków i/lub zapisów na zewnętrznych nośnikach danych;
   3) sposoby ochrony danych osobowych przed osobami nieuprawnionymi i procedury udostępniania danych osobom, których one dotyczą;
   4) obowiązki osób upoważnionych do przetwarzania danych osobowych;
   5) odpowiedzialność za naruszenie zasad przetwarzania i ochrony danych osobowych,
   6) zasady powiadamiania i reakcji na stwierdzenie lub podejrzenie naruszenia zasad przetwarzania i ochrony danych osobowych;
   7) zasady i procedury określone w „Polityce bezpieczeństwa danych osobowych" i „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych".

§ 15. Odpowiedzialność osób upoważnionych do przetwarzania danych osobowych

1. Niezastosowanie się do obowiązujących u Administratora Danych zasad bezpieczeństwa danych osobowych, w szczególności świadome 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.
2. 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.
3. Przykładowo przestępstwo można popełnić wskutek:
   1) stworzenia możliwości dostępu do danych osobowych osobom nieupoważnionym albo osobie nieupoważnionej;
   2) niezabezpieczenia nośnika lub komputera przenośnego;
   3) zapoznania się z hasłem innego pracownika wskutek wykonania nieuprawnionych operacji w systemie informatycznym Administratora Danych Osobowych.

§ 16. Przeglądy i aktualizacje „Polityki bezpieczeństwa danych osobowych"

1. Niniejsza Polityka podlega przeglądowi pod kątem aktualności i stosowalności nie rzadziej niż raz do roku. Przeglądu dokonuje ABI.
2. Niniejsza Polityka podlega aktualizacji każdorazowo w przypadku:
   1) likwidacji, utworzenia lub zmiany zawartości informacyjnej zbioru;
   2) zmiany lokalizacji zbioru;
   3) zmiany administratora zbioru lub administratora informacji;
   4) zmiany przepisów prawa dotyczącego ochrony danych osobowych, wymagającej aktualizacji niniejszej Polityki;
   5) innych znaczących zmian w funkcjonowaniu Urzędu dotyczących danych osobowych.
3. Aktualizacji niniejszej Polityki dokonuje ABI. Zatwierdzenia zaktualizowanej Polityki dokonuje Administrator Danych Osobowych.
4. ABI po uzgodnieniu z Administrator Danych Osobowych może, stosownie do potrzeb, przeprowadzić wewnętrzną kontrolę zgodności przetwarzania danych z przepisami o ochronie danych osobowych. Zakres, przebieg i rezultaty kontroli są dokumentowane na piśmie w protokole podpisywanym przez ABI i Administratora Danych Osobowych.

§ 17. Monitorowanie zabezpieczeń

1. Prawo do monitorowania systemu zabezpieczeń posiadają ,
   1) Administrator Danych Osobowych;
   2) Administrator Bezpieczeństwa Informacji.
2. W ramach kontroli należy zwracać szczególna uwagę na:

1) okresowe sprawdzanie kopii bezpieczeństwa pod względem przydatności do możliwości odtwarzania danych;
2) kontrola ewidencji nośników magnetycznych;
3) kontrola właściwej częstotliwości zmiany haseł .

§ 18. Niszczenie wydruków i zapisów na nośnikach magnetycznych

1. Nośniki magnetyczne przekazywane na zewnątrz powinny być pozbawione zapisów zawierających dane osobowe.
2. Niszczenie poprzednich zapisów powinno odbywać się poprzez wymazywanie informacji oraz formatowanie nośnika.
3. Uszkodzone nośniki magnetyczne przed ich wyrzuceniem należy fizycznie zniszczyć poprzez przecięcie, przełamanie itp.
4. Wydruki po wykorzystaniu należy zniszczyć w mechanicznej niszczarce do papieru.

Rozdział 5
Zasady postępowania w przypadku stwierdzenia naruszenia ochrony danych osobowych w Urzędzie

§ 19. Przypadki naruszenia ochrony danych osobowych w Urzędzie.

1. Naruszenie systemu ochrony danych osobowych w Urzędzie Gminy w Szczutowie ma miejsce w każdym przypadku gdy:
   1) Stwierdzono naruszenie zabezpieczenia systemu informatycznego;
   2) Stan urządzenia, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej mogą wskazywać na naruszenie zabezpieczeń tych danych;
   3) Stwierdzono niekompletną zawartość zbioru danych osobowych;
   4) Ujawniono niezgodne z polityką bezpieczeństwa metody pracy, obieg dokumentów w urzędzie, itp.;
   5) Stan pomieszczeń i szaf bądź innych mebli biurowych, w których przechowuje się dokumentacje Urzędu Gminy lub nośniki informacji oraz zawartości tej dokumentacji lub nośników informacji wzbudzają podejrzenie że dostęp do nich mogły mieć osoby trzecie
2. Naruszenie ochrony danych osobowych może przejawiać się w szczególności w postaci:
   1) Widocznych uszkodzeń bądź naruszeń powierzchni drzwi, szaf lub innych mebli biurowych lub ich zamknięć;
   2) Uszkodzenia opakowania dokumentacji Urzędu Gminy lub nośnika informacji, budzące podejrzenie iż do ich treści mogły mieć dostęp osoby trzecie;
   3) Nieprawidłowego dostępu lub próby dostępu do systemu lub pomieszczeń,
   4) Naruszenia lub próbie naruszenia integralności systemu;
   5) Zmiany lub utraty danych zapisanych na kopiach zapasowych lub archiwalnych dokonanej w sposób nieautoryzowany;
   6) Zniszczenia oraz próby zniszczenia w sposób nieautoryzowany danych zgromadzonych
   7) w systemie;
   8) Innego stanu systemu lub pomieszczeń niż pozostawiony przez użytkownika po zakończeniu lub po przerwie w pracy z systemem.

§ 20. Rodzaje przedsięwzięć zabezpieczających przed naruszeniem ochrony danych osobowych w zbiorach ewidencyjnych i zbiorach informatycznych.

1. W celu uniemożliwienia osobom nieuprawnionym dostępu do zbiorów danych osobowych, których Administratorem jest Urząd Gminy w Szczutowie dokonano identyfikacji możliwych zagrożeń, podjęto stosowne przedsięwzięcia, których celem jest zapewnienie odpowiednich standardów zabezpieczeń systemu ochrony danych osobowych przed jego naruszeniem.
2. Do przedsięwzięć o których mowa w ust. 1 należą:

1) Całodobowa ochrona budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe w Urzędzie Gminy w Szczutowie systemem alarmowym podłączonym do firmy ochroniarskiej;
2) Wydzielenie pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe;
3) Wyposażenie pomieszczeń tworzących obszar przetwarzania danych osobowych w szafy zamykane na klucz i niezbędne urządzenia (np. niszczarki);
4) Określono standardy dostępu do pomieszczeń, w których przetwarzane są dane osobowe, w szczególności:
   a) Stały dostęp do pomieszczeń mają tylko przetwarzający dane osobowe;
   b) Klucze do pomieszczeń przechowywane są u pracowników;
   c) Klucze zapasowe do wyżej wymienionych pomieszczeń, w zapieczętowanej kopercie przechowywane są w specjalnej szafie u ABI i mogą być wydawane w sytuacjach awaryjnych;
   d) Klucze do szaf, w których przechowywana jest dokumentacja zawierająca dane osobowe znajdują się u pracowników merytorycznych. Zapasowy komplet kluczy winien znajdować się w specjalnie wyznaczonym przez Kierownika Referatu miejscu;
   e) Pomieszczenia, w których przetwarzane są dane osobowe po zakończeniu pracy zamyka ostatni wychodzący pracownik, po czym upoważniony przez ADO pracownik dokonuje za pomocą indywidualnego hasła włączenia sygnalizacji alarmowej w budynku i zamyka drzwi wejściowe do budynku;
   f) Upoważniony pracownik przed rozpoczęciem pracy Urzędu otwiera drzwi wejściowe do budynku, za pomocą indywidualnego hasła wyłącza sygnalizację alarmową;
   g) Pomieszczenia, w których przetwarzane są dane osobowe otwiera osoba, która rozpoczyna pracę jako pierwsza;
   h) Wszyscy pracownicy, którzy jako pierwsi wchodzą do budynku i ww. pomieszczeń zostali pouczeni o obowiązkach w sytuacji naruszenia zabezpieczeń budynku.

§ 21. Obowiązek zgłoszenia naruszenia danych osobowych:

W przypadku stwierdzenia naruszenia ochrony danych osobowych należy bezzwłocznie:
1) W przypadku włamania do budynku, każda osoba która ten fakt ujawniła zobowiązana jest:
   a) zabezpieczyć miejsce włamania przed dostępem pracowników i osób trzecich - do czasu przybycia odpowiednich organów ścigania lub ADO bądź ABI - a po ich przybyciu podejmować czynności przez nich określone;
   b) zawiadomić ADO i ABI o włamaniu;
   c) zawiadomić odpowiednie organy ścigania;
2) W przypadku innych zagrożeń:
   a) Zablokować dostęp do systemu dla użytkowników oraz osób nieupoważnionych;
   b) Powiadomić bezpośredniego przełożonego i ABI lub ADO;
   c) Podjąć działania mające na celu zminimalizowanie lub całkowite wyeliminowanie powstałego zagrożenia - o ile czynności te nie spowodują przekroczenia uprawnień pracownika;
   d) Zabezpieczyć dowody umożliwiające ustalenie przyczyn oraz skutków naruszenia bezpieczeństwa systemu.
3) Użytkownik systemu informatycznego zobowiązany jest zawiadomić niezwłocznie Administratora Bezpieczeństwa Informacji lub ASI o każdym naruszeniu lub podejrzeniu naruszenia bezpieczeństwa systemu informatycznego, a w szczególności o:
   a) użyciu hasła dostępu i identyfikatora przez inne osoby niż dany użytkownik, naruszeniu hasła dostępu i identyfikatora (system nie reaguje na hasło lub je ignoruje bądź można przetwarzać dane bez wprowadzenia hasła);
   b) nieuprawnionej modyfikacji danych, uszkodzeniu lub zniszczeniu, częściowym lub całkowitym braku danych albo dostępie do danych w zakresie szerszym niż wynikający z przyznanych uprawnień;

c) braku dostępu do właściwej aplikacji lub zmianie zakresu wyznaczonego dostępu do zasobów;
d) wykryciu wirusa komputerowego przez program antywirusowy;
e) próbie włamania do systemu informatycznego;
f) znacznym spowolnieniu działania systemu informatycznego lub innym nieprawidłowym;
g) funkcjonowaniu, podejrzeniu kradzieży sprzętu komputerowego lub dokumentów zawierających dane osobowe;
h) zmianie położenia sprzętu komputerowego;
i) zauważeniu śladów usiłowania lub dokonania włamania do pomieszczeń lub zamykanych szaf.

4) ASI jest zobowiązany do natychmiastowego informowania ABI o wszelkich 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 w sposób niezgodny z procedurami ochrony danych osobowych.

§ 22. Zasady postępowania w przypadku naruszenia danych osobowych:

1. Do czasu przybycia na miejsce ABI należy:
   1) niezwłocznie, o ile to możliwe, podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego zdarzenia, a następnie uwzględnić w działaniu również ustalenie jego przyczyn lub sprawców;
   2) 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 obsługi, regulaminów lub dokumentacji aplikacji, jeśli odnoszą się one do zaistniałego przypadku;
   5) nie opuszczać bez uzasadnionej przyczyny miejsca zdarzenia do czasu przybycia ABI lub osoby przez niego wskazanej.
2. ABI jest obowiązany niezwłocznie:
   1) poinformować Administratora Danych Osobowych o naruszeniu lub podejrzeniu naruszenia bezpieczeństwa systemu;
   2) przeprowadzić postępowanie wyjaśniające w celu ustalenia okoliczności naruszenia ochrony danych osobowych i przygotować opis incydentu;
   3) podjąć działania chroniące system przed ponownym naruszeniem w porozumieniu z Administratorem Danych Osobowych, w szczególności w razie potrzeby, może zarządzić odłączenie części systemu informatycznego dotkniętej incydentem od pozostałej jego części.
3. W przypadku naruszenia bądź podejrzenia naruszenia danych osobowych, czynności związane z wyjaśnieniem okoliczności naruszenia prowadzi zespół w składzie:
   1) ABI, a w przypadku jego nieobecności, wyznaczony praz ADO pracownik – jako osoba kierująca pracami zespołu;
   2) Kierownik referatu, w którym nastąpiło naruszenie danych osobowych bądź nasuwają się podejrzenia o ich naruszeniu;
   3) ASI – jeżeli naruszenie nastąpiło w systemach informatycznych Urzędu;
   4) pracownik, który wykrył naruszenie bądź wobec którego nasuwają się podejrzenia ich naruszeniu – celem złożenia wyjaśnień w sprawie.
4. Prace zespołu, o którym mowa w ust. 3, mają na celu ustalenie:
   1) przyczyn i okoliczności naruszenia bezpieczeństwa danych osobowych;
   2) osób winnych naruszenia bezpieczeństwa danych osobowych;
   3) skutków naruszenia.
5. Zespół, o którym mowa w ust. 3 i 4 podejmuje prace niezwłocznie, po ujawnieniu naruszenia.

6. Kierujący pracami zespołu obowiązany jest na bieżąco informować ADO o ustalonych przez zespół faktach,
7. Z czynności podejmowanych przez zespół sporządza się protokół , wg wzoru stanowiącego **Załącznik Nr 9 do** niniejszej Polityki bezpieczeństwa., zawierający co najmniej:
   1) datę i miejsce wystąpienia naruszenia;
   2) zakres ujawnionych danych;
   3) przyczynę ujawnienia, osoby odpowiedzialne oraz stwierdzone nieprawidłowości;
   4) sposób rozwiązania problemu;
   5) przyjęte rozwiązania mające na celu wyeliminowanie podobnych zdarzeń w przyszłości;
   6) Jeżeli okoliczności zdarzenia tego wymagają, dopuszcza się sporządzanie z miejsca naruszenia szkiców sytuacyjnych, fotografii itp.. stanowiących załącznik do protokołu.
8. Decyzję o przywróceniu normalnego toku pracy podejmuje ADO.
9. Protokół o którym mowa w ust.7, kierujący pracami zespołu przekazuje ADO.
10. Dokumentację dotyczącą naruszenia danych osobowych prowadzi ABI.

§ 23. Sankcje z tytułu naruszenia procedur oraz zasady ochrony danych osobowych

1. Za naruszanie ochrony danych osobowych, sprawca naruszenia podlega sankcjom karnym określonym w przepisach prawa powszechnie obowiązującego, w szczególności:
   1) ustawie o ochronie danych osobowych;
   2) ustawie z dnia 6 czerwca 1997 r. Kodeks karny.
2. Za naruszenie zasad ochrony danych osobowych pracownik podlega sankcjom: finansowym, dyscyplinarny, i porządkowym w przypadkach oraz na zasadach określonych w Kodeksie Pracy i regulaminie pracy Urzędu Gminy w Szczutowie.
3. Administrator Danych Osobowych po zapoznaniu się z protokołem, o którym mowa w § 22 ust. 7, podejmuje decyzję o dalszym trybie postępowania, powiadomieniu właściwych organów oraz podjęciu innych szczególnych czynności zapewniających bezpieczeństwo systemu informatycznego Administratora Danych Osobowych bądź zastosowaniu środków ochrony fizycznej.

Rozdział 5
Postanowienia końcowe

§ 24.

1. Niniejsza Polityka zostaje wprowadzona zarządzeniem Wójta Gminy Szczutowo.
2. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest zapoznać się z niniejszym dokumentem przed dopuszczeniem do przetwarzania danych oraz złożyć stosowne oświadczenie, potwierdzające znajomość jego treści.
3. ABI prowadzi dokumentację osób, które zostały zapoznane z przepisami ochrony danych osobowych i zobowiązały się je przestrzegać.
4. Wobec osoby, która zaniechała działań do których została zobowiązana a w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, pracodawca może wszcząć postępowanie dyscyplinarne.

WÓJT
Andrzej Twardowski

Załącznik nr 1
do Polityki bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy w Szczutowie

WZÓR

Upoważnienie do przetwarzania danych osobowych

..... Szczutowo, dnia .....
(pieczęć Administratora Danych Osobowych)

Znak sprawy .....

Upoważnienie
do przetwarzania danych osobowych

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (tekst jednolity z 2002 roku Dz. U. Nr 101 poz. 926 – z późn. zmianami) **upoważniam:** .....
(imię i nazwisko – stanowisko służbowe)

1. Do przetwarzania danych osobowych :
.....
(określić rodzaje zbiorów danych osobowych (np. ewidencyjne, informatyczne)
w związku z realizacją zadań służbowych na zajmowanym stanowisku, określonych w szczegółowym zakresie czynności, w następującym zakresie:
.....
(określić zakres upoważnienia – np. : zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, usuwanie i udostępnianie).
2. Do przetwarzania danych osobowych :
.....
(określić rodzaje zbiorów danych osobowych (np. ewidencyjne, informatyczne)
związku z zastępstwem w czasie nieobecności w pracy pracownika zatrudnionego na stanowisku: .....
(nazwa stanowiska)
określonych w szczegółowym zakresie czynności w następującym zakresie:
.....
(określić zakres upoważnienia – np. : zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, usuwanie i udostępnianie).
3. Do przetwarzania danych osobowych :
.....
(określić rodzaje zbiorów danych osobowych (np. ewidencyjne, informatyczne)
związku z wykonywaniem obowiązków: .....
.....
(określić zakres obowiązków lub stanowisk np. Kierownika Referatu (nazwa), Sekretarza Gminy, Skarbnika Gminy, czynności kontrolnych w sprawach b.h.p., p.poż, Pełnomocnika Ochrony Informacji Niejawnych, Administratora Bezpieczeństwa Informacji , - Administratora Biuletynu Informacji Publicznej (BIP), itp.
określonych w szczegółowym zakresie czynności w następującym zakresie:
.....
(określić zakres upoważnienia – np. : zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, usuwanie i udostępnianie).

Upoważnienie udzielone jest na czas trwania stosunku pracy w Urzędzie Gminy w Szczutowie. Wszelkie zmiany niniejszego zakresu upoważnienia dokonywane będą w drodze aneksów.

.....
(podpis i pieczęć Administratora Danych Osobowych)

P o u c z e n i e

Osoba upoważniona do przetwarzania danych osobowych zobowiązana jest (zgodnie z art. 39 ust. 2 ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych - tekst jednolity z 2002 roku Dz. U. Nr 101 poz. 926 – z późn. zmianami) **zachować w tajemnicy te dane osobowe przetwarzane u wyżej wymienionego Administratora Danych Osobowych oraz sposoby ich zabezpieczania zarówno w czasie jak i po ustaniu zatrudnienia** (odwołania lub upływu ważności upoważnienia do przetwarzania danych osobowych).

Za naruszenie ochrony danych osobowych osoba upoważniona podlega odpowiedzialności karnej wynikającej z art. 51 i 52 ustawy o ochronie danych osobowych jak również art. 266 ustawy z dnia 06 czerwca 1997 roku Kodeks karny (Dz. U. Nr 88 poz. 553 – z późn. zmianami).

Otrzymują:
1. Upoważniony pracownik (Imię i nazwisko oraz stanowisko służbowe)
2. Akta osobowe w/m
3. Administrator Bezpieczeństwa Informacji
   Urzędu Gminy Szczutowo - aa

Załącznik nr 2
do Polityki bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy w Szczutowie

WZÓR

Wykaz budynków i pomieszczeń tworzących obszar*, w którym przetwarzane są dane osobowe

Budynek .....z lokalizowany przy ul. .....
(nazwa budynku – np. administracyjny, magazyn, itp.)

Lp.	Numer pokoju lub nazwa pomieszczenia , kondygnacja	Sposób przetwarzania danych osobowych (wykonywania operacji – np. wpisywanie, modyfikowanie, kopiowanie, usuwanie, tylko przechowywanie – archiwum, itp.)	Uwagi dotyczące zabezpieczeń (np. krata, alarm, drzwi obite blachą, inne)
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			
17			
18			

/* Obszarem, o którym mowa w § 4 pkt. 1 rozporządzenia 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. Nr 100, poz. 1024), są wszystkie miejsca w Urzędzie, w których dokonuje się przetwarzania danych osobowych, w szczególności:

1. Gdzie wykonuje się operacje na danych osobowych (wpisuje, modyfikuje, kopiuje, usuwa),
2. Miejsca gdzie przechowuje się dane osobowe, np. archiwum, szafy z dokumentacją papierową, szafy zawierające nośniki informacji z kopiami zapasowymi, skład zużytego sprzętu komputerowego zawierającego dyski z zapisanymi danymi osobowymi, itp.).

.....
(czytelny podpis ABI)

Załącznik nr 3
do Polityki bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy w Szczutowie

WZÓR

Granice obszarów oraz osoby, które przetwarzają dane osobowe.

Pokój Nr ....
(Numer lub nazwa pomieszczenia w których przetwarzane są dane osobowe, kondygnacja)

1	..... (Nazwa zbioru danych, którego dane osobowe przetwarzane są w tym pomieszczeniu)			
	Osoby przetwarzające dane osobowe (edytujące bądź mające wgląd do danych osobowych)	Imię i nazwisko	Stanowisko służbowe	Uwagi
2	..... (Nazwa zbioru danych, którego dane osobowe przetwarzane są w tym pomieszczeniu)			
	Osoby przetwarzające dane osobowe (edytujące bądź mające wgląd do danych osobowych)	Imię i nazwisko	Stanowisko służbowe	Uwagi
3	..... (Nazwa zbioru danych, którego dane osobowe przetwarzane są w tym pomieszczeniu)			
	Osoby przetwarzające dane osobowe (edytujące bądź mające wgląd do danych osobowych)	Imię i nazwisko	Stanowisko służbowe	Uwagi

.....
(czytelny podpis ABI)

Załącznik nr 4
do Polityki bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy w Szczutowie

WZÓR

Wykaz zbiorów danych osobowych i programów zastosowanych do ich przetwarzania

Lp.	Nazwa zbioru danych osobowych	Numer pokoju lub nazwa pomieszczenia, kondygnacja	Nazwa programu zainstalowanego na stacjach komputerowych stosowany do przetwarzania danych osobowych	uwagi
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				

.....
(czytelny podpis ABI)

Załącznik nr 5
do Polityki bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy w Szczutowie

WZÓR

Opis struktury zbiorów danych przetwarzanych w Urzędzie

Przykładowy **zbiór danych EWIDENCJA LUDNOŚCI zawiera następujące pola:**

Dane osobowe
- nazwiska i imiona
- nazwisko rodowe i z poprzedniego małżeństwa,
- imiona rodziców,
- data urodzenia,
- miejsce urodzenia,
- akta urodzenia, data i nr USC
Dane osobowe archiwalne
- nazwiska i imiona,
- nazwisko rodowe i z poprzedniego małżeństwa.
Adres zamieszkania lub pobytu stałego oraz data zameldowania
Archiwalne adresy zamieszkania lub pobytu stałego oraz data zameldowania
Adres czasowy oraz czas pobytu czasowego
Archiwalne adresy czasowe oraz okresy pobytów czasowych
Dokument tożsamości
- rodzaj dokumentu,
- seria i numer dowodu,
- wystawca dokumentu,
- rysopis :wzrost, kolor oczu, znaki szczególne;
Data wydania i wydający dokument tożsamości
Archiwalne dokumenty tożsamości
Numer ewidencyjny PESEL
USC i nr aktu urodzenia
Stan cywilny:
- imię i nazwisko współmałżonka,
- nazwisko rodowe i nazwisko z poprzedniego małżeństwa,
- data zawarcia małżeństwa,
- USC i numer aktu małżeństwa,
- data wydania i wydający dokument tożsamości,
Stan cywilny archiwalny
- imię i nazwisko małżonka,
- nazwisko rodowe i nazwisko z poprzedniego małżeństwa,
- data zawarcia małżeństwa,
- USC i numer aktu małżeństwa,
Obowiązek wojskowy
- czy podlega obowiązkowi,
- nazwa i nr wojskowego dokumentu tożsamości,
- stopień wojskowy,
Data zgonu, USC i numer aktu zgonu
Imiona i nazwiska rodowe
Narodowość
Obywatelstwo (data zmiany, podstawa prawna)
Adnotacje o rozwodzie

Opis struktury zbioru danych przygotował	
Imię i nazwisko	Stanowisko służbowe

.....
(czytelny podpis ABI)

Załącznik nr 6
do Polityki bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy w Szczutowie

WZÓR
Ewidencja osób upoważnionych do przetwarzania danych osobowych w Urzędzie

Lp.	Nazwisko i imię	stanowisko	Data nadania upoważnienia	Data ustania upoważnienia	Zakres upoważnienia/*	Uwagi
1						
2						
3						
4						

Zakres upoważnienia:

Wgląd (przeglądanie)	**P**
Wprowadzanie (edycja)	**W**
Modyfikacja (zmienianie)	**M**
Usuwanie (kasowanie)	**U**

.....
(czytelny podpis ABI)

Załącznik nr 7
do Polityki bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy w Szczutowie

WZÓR
Ewidencji nadanych identyfikatorów dostępu do systemów informatycznych

Lp.	Nazwisko i imię	stanowisko	Data nadania / modyfikacji/ zmiany upoważnienia	Nazwa zbioru danych	Nadany Identyfikator	Uwagi
1						
2						
3						
4						

.....
(czytelny podpis ABI)

Załącznik nr 8
do Polityki bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy w Szczutowie

WZÓR

Oświadczenie
osoby upoważnionej do przetwarzania danych osobowych w Urzędzie Gminy w Szczutowie

Ja niżej podpisana*/podpisany/*.....- .....
(imię i nazwisko) (stanowisko służbowe)

Oświadczam że:

1. Zapoznałam/*zapoznałem/* się z przepisami prawnymi w zakresie ochrony danych osobowych w szczególności z:
   1) przepisami ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (tekst jednolity z 2002 roku Dz. U. Nr 101 poz. 926 – z późn. zmianami);
   2) 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. Nr 100, poz. 1024);
   3) Polityką bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy w Szczutowie;
   4) Instrukcją zarządzania systemem informatycznym w Urzędzie Gminy w Szczutowie,
2. **Zobowiązuję się do** zachowania w tajemnicy:
   1) wszelkich danych osobowych z którymi się zapoznałam/* zapoznałem/* przez cały okres pracy u Administratora Danych Osobowych (dalej ADO), a także do ich zachowania w tajemnicy po ustaniu stosunku pracy/* odwołaniu z pełnionej funkcji/*.
   2) procedur ochrony danych osobowych w Urzędzie, określonych w dokumentach wewnętrznych wprowadzonych przez ADO, przez cały okres pracy u ADO, a także po ustaniu stosunku pracy/* odwołaniu z pełnionej funkcji/*.
3. **Zobowiązuję się do** przestrzegania procedur bezpiecznego przetwarzania danych osobowych określonych w przepisach prawa powszechnie obowiązującego oraz politykach, instrukcjach i wytycznych określonych przez Administratora Danych Osobowych o których mowa w pkt. 1 niniejszego oświadczenia.
4. **Oświadczam,** że jestem świadoma/* świadomy/* odpowiedzialności karnej, wynikającej z art. 51 i art. 52 ustawy o ochronie danych osobowych, które wobec osób zobowiązanych do ochrony danych osobowych:
   1) za udostępnianie danych osobowych lub umożliwianie dostępu do nich osobom nieupoważnionym, przewidują karę grzywny, karę ograniczenia wolności albo pozbawienia wolności do lat 2;
   2) za naruszenie, choćby nieumyślne, obowiązku zabezpieczenia ich przed zabraniem przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.
5. **Oświadczam**, że jestem świadoma/* świadomy/* odpowiedzialności karnej, wynikającej z art. 266 ustawy z dnia 06 czerwca 1997 roku Kodeks Karny – Dz. U. Nr 88 poz. 533 – z późn. zmianami), które:
   1) Za ujawnianie lub wykorzystywanie informacji, z którą zapoznał się w związku z pełnioną funkcją, wykonywaną pracą, działalnością publiczną, społeczną, gospodarczą lub naukową, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.
   2) Za ujawnienie przez funkcjonariusza publicznego osobie nieuprawnionej informacji stanowiącej tajemnicę służbową lub informację, którą uzyskał w związku z wykonywaniem czynności służbowych, a której ujawnienie może narazić na szkodę prawnie chroniony interes, podlega karze pozbawienia wolności do lat 3.

Szczutowo, dnia ....
(data złożenia oświadczenia) (czytelny podpis składającego oświadczenie)

/* - niepotrzebne skreślić

Załącznik nr 9
do Polityki bezpieczeństwa przetwarzania danych
osobowych w Urzędzie Gminy w Szczutowie

WZÓR

Protokół
z podjętych działań w sprawie naruszenia ochrony danych osobowych

1. Data wystąpienia naruszenia ..... Godzina .....

2. Osoba powiadamiająca o zaistniałym naruszeniu :

.....- .....
(imię i nazwisko) (stanowisko służbowe)

3. Zespół powołany do ustalenia przyczyn naruszenia:

.....- .....
(imię i nazwisko) (stanowisko służbowe)
.....- .....
.....- .....

4. Osoba składająca wyjaśnienia w sprawie naruszenia:

.....- .....
(imię i nazwisko) (stanowisko służbowe)

5. Lokalizacja

.....
(Numer lub nazwa pomieszczenia w którym wystąpiło naruszenie danych osobowych)

6. Rodzaj naruszenia, okoliczności towarzyszące temu naruszeni, prawdopodobne przyczyny wystąpienia naruszenia ochrony danych osobowych, osoby odpowiedzialne oraz stwierdzone nieprawidłowości:

.....
.....
.....

7. Proponowane rozwiązania mające na celu wyeliminowanie podobnych zdarzeń w przyszłości:

.....
.....
.....

8. Uwagi :

.....
.....
.....
.....

2. Załączniki : Szkice, pisemne wyjaśnienia, itp.: (ew. załączyć do protokołu)

.....
.....
.....

Protokół sporządzono dnia ..... godz. .....

Podpisy członków zespołu :

1. ..... - .....
(imię i nazwisko, stanowisko służbowe) (podpis)
2. ..... - .....

3. ..... - .....

Podpis osoby składającej wyjaśnienia :

1. ..... - .....
(imię i nazwisko, stanowisko służbowe) (podpis)

WÓJT GMINY SZCZUTOWO
09-227 Szczutowo, ul. Lipowa 5a
woj. mazowieckie
tel. 276 71 67
(1)

Załącznik Nr 2
do Zarządzenia Nr Or.120.11.2012
Wójta Gminy Szczutowo
z dnia 20.07. 2012 r.

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH w Urzędzie GMINY W Szczutowie

Rozdział 1
Postanowienia ogólne

§ 1. Cel instrukcji

1. Instrukcja określa sposób zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy w Szczutowie w celu zabezpieczenia danych osobowych przed zagrożeniami, w szczególności przed ich udostępnieniem osobom nieupoważnionym, nieautoryzowaną zmianą, utratą, uszkodzeniem lub zniszczeniem.
2. Instrukcja nie dotyczy przypadków, w których Urząd Gminy w Szczutowie posiada podpisane i obowiązujące umowy o powierzeniu przetwarzania danych lub jeśli administrowanie systemem informatycznym odbywa się na podstawie przepisów lub/i umów zawierających odpowiednie klauzule.
3. Procedury określone w niniejszej Instrukcji stosuje się do wszystkich osób upoważnionych do przetwarzania danych osobowych w systemach informatycznych, zatrudnionych w Urzędzie Gminy, na podstawie stosunku pracy jak i poza stosunkiem pracy, np. wolontariuszy, praktykantów, stażystów, itp.
4. Instrukcja, o której mowa w § 3 ust. 1, zawiera w szczególności:
   1) procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności;
   2) stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem;
   3) procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu;
   4) zasady zarządzania sprzętem i oprogramowaniem komputerowym
   5) procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania;
   6) sposób, miejsce i okres przechowywania:
      a) elektronicznych nośników informacji zawierających dane osobowe,
      b) kopii zapasowych, o których mowa w ust. 3 pkt 4,
      c) sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego;
      d) sposób realizacji wymogów, o których mowa w § 7 ust. 1 pkt 4 rozporządzenia;
      e) procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.

§ 2. Definicje stosowanych pojęć

Definicje stosowanych pojęć:

1) **dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby,

2) **osoba możliwa do zidentyfikowania** – każda osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne,
3) **zbiór danych** – każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie,
4) **komputerowy zbiór danych** – zbiór danych osobowych w formie elektronicznej,
5) **tradycyjny zbiór danych** – zbiór danych osobowych w formie papierowej (np. księgi, wykazy, ewidencje),
6) **przetwarzanie danych** – 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,
7) **Urząd** – Urząd Gminy w Szczutowie z siedzibą: ul. Lipowa 5A, 09-227 Szczutowo.
8) **Administrator Danych Osobowych** – Wójt Gminy Szczutowo reprezentujący Urząd, który decyduje o celach i środkach przetwarzania danych osobowych oraz monitoruje wdrożone zabezpieczenia systemu informatycznego,
9) **Administrator Bezpieczeństwa Informacji (dalej ABI)** – osoba nadzorująca przestrzeganie zasad przetwarzania i ochrony danych osobowych,
10) **Administrator Systemu Informatycznego – Informatyk (dalej ASI)** – osoba odpowiedzialna za bezpieczeństwo danych osobowych przetwarzanych systemach informatycznych, w tym w szczególności za przeciwdziałanie dostępowi osób trzecich do systemów oraz podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w tych systemach,
11) **osoba upoważniona** – osoba posiadająca upoważnienie do przetwarzania danych osobowych w określonym zakresie wydane przez Administratora Danych Osobowych,
12) **osoba uprawniona** – osoba upoważniona lub inna osoba uprawniona do przetwarzania danych osobowych na podstawie szczególnych przepisów prawa (lex specialis),
13) **osoba trzecia** – każda osoba nieuprawniona do przetwarzania danych osobowych będących w posiadaniu Administratora Danych Osobowych, a także osoba posiadająca upoważnienie wydane przez Administratora Danych Osobowych, ale podejmująca czynności w zakresie przekraczającym zakres jej upoważnienia,
14) **użytkownik systemu informatycznego** – osoba upoważniona do przetwarzania danych osobowych w określonym zakresie w systemie informatycznym służącym do przetwarzania danych osobowych,
15) **stacja robocza** - stacjonarny lub przenośny komputer, umożliwiający użytkownikowi dostęp do danych przetwarzanych w formie elektronicznej,
16) **zewnętrzne nośniki danych** - przedmiot fizyczny służący do zapisywania, przechowywania, przetwarzania i transmisji danych (np. pendrive, CD, DVD),
17) **zabezpieczenie systemu informatycznego** – wdrożone przez Administratora bezpieczeństwa informacji oraz Informatyka odpowiednie środki organizacyjne i techniczne w celu zabezpieczenia zasobów oraz ochrony danych przed dostępem, modyfikacją ujawnieniem, pozyskaniem lub zniszczeniem przez użytkownika lub osobę trzecią.
18) **Zapewnienie bezpieczeństwa systemów informatycznych oznacza**, utrzymanie takich atrybutów informacji jak:
    a) **poufność** – rozumie się przez to ograniczony i ściśle zdefiniowany krąg osób mających dostęp do informacji,
    b) **integralność** – rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
    c) **rozliczalność** – rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi,
    d) **uwierzytelnianie** – rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu za pomocą,
        - **identyfikatora użytkownika** – przypisanego jednej osobie identyfikatora jednoznacznie określającego użytkownika w systemie informatycznym,
        - **hasła** – ciągu znaków (stanowiącego tajemnicę użytkownika), który w połączeniu z identyfikatorem użytkownika umożliwia uwierzytelnienie go

w systemie informatycznym.

19) **raport** – przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzanych danych,

20) **odbiorca danych** – każdy, komu udostępniane są 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,

21) **przetwarzający** – podmiot, któremu zostało powierzone przetwarzanie danych osobowych na podstawie umowy zawieranej zgodnie z art. 31 ustawy,

22) **sieć publiczna** – sieć publiczna w rozumieniu art. 2 pkt. 22 ustawy z dnia 21 lipca 2000 r. Prawo telekomunikacyjne,

23) **sieć telekomunikacyjna** – sieć telekomunikacyjna w rozumieniu art. 2 pkt. 23 ustawy z dnia 21 lipca 2000 r. – Prawo telekomunikacyjne (DzU nr 73, poz. 852 ze zm.),

24) **teletransmisja** – przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej,

25) **serwisant** – firma lub pracownik firmy zajmującej się sprzedażą, instalacją, naprawą lub konserwacją sprzętu komputerowego,

26) **ustawa** – ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jedn. Dz. U z 2002 r. nr 101, poz. 926 ze zm.),

27) **rozporządzenie MSWiA** – 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),

28) **Polityka** – Polityka Bezpieczeństwa danych osobowych,

29) **Instrukcja** – niniejsza Instrukcja zarządzania systemem informatycznych służącym do przetwarzania danych osobowych,

30) **zakres czynności** – zakres czynności, upoważnień, odpowiedzialności i zastępstwa wynikającego ze stanowiska służbowego i pełnionego stanowiska.

§ 3. Poziom bezpieczeństwa

1. Uwzględniając kategorie danych osobowych oraz konieczność zachowania bezpieczeństwa ich przetwarzania w systemie informatycznym połączonym z siecią publiczną, w Urzędzie obowiązuje wysoki poziom bezpieczeństwa w rozumieniu § 6 rozporządzenia MSWiA.
2. Ze względu na wysoki poziom bezpieczeństwa w Urzędzie wyodrębnia się:
   1) I (pierwszą) strefę bezpieczeństwa, która obejmuje: kasę, docelowo do tej strefy planuje się włączyć serwerownię.
   2) II (drugą) strefę bezpieczeństwa zwaną strefą administracyjną, która obejmuje wszystkie pozostałe pomieszczenia zaliczone do obszaru przetwarzania danych w siedzibie Administratora Danych Osobowych.
3. W I strefie bezpieczeństwa:
   1) dostęp do pomieszczeń mają osoby upoważnione do przetwarzania danych osobowych (niedopuszczalne jest przebywanie w pomieszczeniu np. klientów urzędu),
   2) osoby z obsługi porządkowo-technicznej oraz osoby trzecie tylko w obecności osoby posiadającej stałe miejsce pracy w tym pomieszczeniu,
   3) pomieszczenia są chronione systemem antywłamaniowym,
   4) okna są chronione za pomocą krat.
4. W II strefie bezpieczeństwa dostęp do pomieszczeń mają wszystkie osoby upoważnione do przetwarzania danych osobowych zgodnie z zakresami tych upoważnień lub osoby z obsługi porządkowo-technicznej upoważnione do przebywania w tych pomieszczeniach, a osoby nieuprawnione mogą przebywać wyłącznie w obecności upoważnionego pracownika.

5. Podstawowe klucze do pomieszczeń są wydawane pracownikom, a zwracane wraz z ustaniem zatrudnienia, natomiast zapasowe klucze są przechowywane w Referacie Organizacyjnym.

Rozdział 2
Procedury nadawania, edytowania oraz cofania uprawnień

§ 4. Procedury nadawania i zmiany uprawnień – identyfikatorów.

1. Dostęp do systemu informatycznego służącego do przetwarzania danych osobowych może uzyskać wyłącznie osoba upoważniona przez Administratora Danych Osobowych, zgodnie z Polityką bezpieczeństwa.
2. Dostęp do zbiorów danych na poszczególnych stanowiskach komputerowych musi być zapewniony z pozycji użytkownika, a w sytuacjach awaryjnych określonych niniejszą instrukcją również z pozycji administratora.
3. Przyznanie uprawnień w zakresie dostępu do systemu informatycznego polega na wprowadzeniu do systemu dla każdego użytkownika unikalnego identyfikatora, hasła oraz zakresu dostępnych danych i operacji (o ile działanie aplikacji na to pozwala).
4. Pracownik ponosi odpowiedzialność za wszystkie operacje wykonane przy użyciu jego identyfikatora i hasła dostępu.
5. Wszelkie przekroczenia lub próby przekroczenia przyznanych uprawnień traktowane będą jako naruszenie podstawowych obowiązków pracowniczych.
6. Obok nadawanych przez ABI identyfikatorów w Urzędzie funkcjonują uprawnienia dostępu do programów obsługiwanych przez pracowników na platformach informatycznych. np. Ewidencja ludności i dowodów osobistych, ewidencja działalności gospodarczej, sprawozdawczość elektroniczna, ZUS, itp.
7. W przypadkach obsługi programów na platformach, o których mowa w ust. 6, obowiązują zasady ustalone dla tych systemów, w tym zasady logowania się do systemu, uwierzytelniania danych, stosowania kart mikroprocesorowych oraz kwalifikowanych podpisów elektronicznych.
8. Na podstawie przyznanego identyfikatora lub karty mikroprocesorowej użytkownik ma dostęp do ściśle określonych zasobów systemu informatycznego zgodnie z zakresem czynności oraz zakresem upoważnienia do przetwarzania danych osobowych.
9. W przypadku zmian w zakresie czynności lub zakresie upoważnienia do przetwarzania danych osobowych zakres uprawnień dostępu do zasobów systemu informatycznego podlega natychmiastowej modyfikacji przez ASI w porozumieniu z ABI a w przypadku programów o których mowa w ust. 6 w porozumieniu z administratorem tych programów.
10. Zasady blokowania identyfikatora użytkownika systemu informatycznego:
    1) zablokowanie identyfikatora użytkownika skutkuje brakiem dostępu do systemu informatycznego,
    2) zablokowanie identyfikatora oraz hasła użytkownika może być czasowe, to jest do momentu ustania przyczyny uzasadniającej blokadę, lub trwałe,
    3) przyczyną czasowego zablokowania identyfikatora użytkownika może być:
        a) wypowiedzenie umowy o pracę (do czasu rozwiązania stosunku pracy),
        b) wszczęcie postępowania dyscyplinarnego względem osoby upoważnionej do przetwarzania danych osobowych,
        c) długotrwała nieobecność w pracy (np. urlop, zwolnienie lekarskie),
        d) inne istotne okoliczności.
    4) przyczyną trwałego zablokowania identyfikatora użytkownika jest rozwiązanie lub wygaśnięcie stosunku pracy, w ramach którego zatrudniony był użytkownik
    5) zablokowania identyfikatora użytkownika dokonuje ASI w porozumieniu z ABI
    6) identyfikator użytkownika, który na stałe stracił uprawnienia do przetwarzania danych osobowych, nie może być przydzielony innej osobie.
11. W systemie informatycznym stosuje się uwierzytelnianie dwustopniowe: na poziomie dostępu do stanowiska komputerowego oraz dostępu do aplikacji (sieci wewnętrznej, poczty elektronicznej, programu dedykowanego, itp.) .

12. Identyfikator użytkownika nie powinien być zmieniany bez wyraźnej przyczyny, a po wyrejestrowaniu użytkownika z systemu informatycznego nie powinien być przydzielany innej osobie.
13. Identyfikatory nadaje ASI.
14. Ewidencję identyfikatorów prowadzi ABI. Dokumentację dotyczącą nadanych identyfikatorów przechowuje w zalakowanej kopercie ABI.
15. Identyfikator użytkownika systemu informatycznego składa się z co najmniej sześciu unikalnych znaków. W identyfikatorze nie stosuje się polskich znaków diakrytycznych.
16. Odebranie uprawnień pracownikowi regulują postanowienia Polityki bezpieczeństwa.
17. Identyfikator osoby, która utraciła uprawnienia do dostępu do danych osobowych należy niezwłocznie wyrejestrować z systemu informatycznego, w którym są one przetwarzane oraz unieważnić jej hasło.
18. Informatycy korzystają ze wspólnego identyfikatora i hasła uprawniających do zarządzania systemem informatycznym na poziomie administratora. Do hasła stosuje się zasady, o których mowa w ust. 8.

§ 5. Zasady posługiwania się hasłami.

1. Bezpośredni dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po podaniu identyfikatora i właściwego hasła.
2. Hasło użytkownika powinno być zmieniane co najmniej raz na kwartał, z zastrzeżeniem ust.8. Po tym okresie hasło powinno stracić ważność, w tym rozumieniu, że użytkownik dalej nie może się nim posługiwać,
3. Jeżeli system komputerowy umożliwia, należy stosować wymuszenie zmiany hasła.
4. Po upływie okresu określonego w ust. 2, hasło może zmienić sam użytkownik lub też, jeśli system nie pozwala na zmianę hasła przez użytkownika, hasło zmienia ASI w porozumieniu z użytkownikiem,
5. Na wypadek sytuacji awaryjnych z przyczyn pracownika (zapomnienie hasła, dłuższa absencja w pracy, itp.) hasło deponuje się w zaklejonej i ostemplowanej kopercie u ABI i może być wykorzystane tylko przez ABI lub ASI. Z otwarcia koperty z hasłem i próby jego wykorzystania sporządza się protokół ze szczegółowym opisaniem przyczyny otwarcia koperty i wykonanych czynności.
6. Na wypadek sytuacji awaryjnych innych nuż określone w ust. 5 tworzy się dostęp do systemu informatycznego na poziomie administratora. Z każdego wejścia do systemu informatycznego pracowników z tego poziomu sporządza się protokół ze szczegółowym opisaniem przyczyny wejścia do systemu i wykonanych czynności.
7. Hasła użytkowników przechowywane w systemie informatycznym mogą być przechowywane wyłącznie w postaci zaszyfrowanej.
8. Każde awaryjne użycie hasła do systemu informatycznego, w przypadkach o których mowa w ust. 5 i 6 wymaga bezzwłocznej jego zmiany oraz odnotowania tego faktu w protokole i dołączenia do dokumentacji systemu ochrony danych osobowych w Urzędzie.
9. Hasła dostępu zmienia się w zawsze gdy:
   1) Pracownik korzysta z platform informatycznych, które określają inny tryb zmiany haseł dostępu. .
   2) W sytuacji, kiedy zachodzi podejrzenie, że ktoś poznał hasło w sposób nieuprawniony, pracownik zobowiązany jest do natychmiastowej zmiany hasła.
10. Pracownicy są odpowiedzialni za zachowanie poufności swoich haseł. Hasła użytkownika utrzymuje się w tajemnicy również po upływie ich ważności.
11. Hasło należy wprowadzać w sposób, który uniemożliwia innym osobom jego poznanie
12. Przy wyborze hasła obowiązują następujące zasady:
    1) minimalna długość hasła - 8 znaków,
    2) <u>zakazuje się stosować</u>:
       a) haseł, które użytkownik stosował uprzednio w okresie minionego roku,
       b) identycznych z identyfikatorem użytkownika ani jego imieniem , przezwiska, pseudonimem lub nazwiskiem, w jakiejkolwiek formie (pisanej dużymi literami, w odwrotnym porządku, dublując każdą literę, itp.),
       c) imion (w szczególności imion osób z najbliższej rodziny),

d) ogólnie dostępnych informacji o użytkowniku takich jak: numer telefonu, numer rejestracyjny samochodu, jego marka, numer dowodu osobistego, nazwa ulicy na której mieszka lub pracuje, itp.
e) przewidywalnych sekwencji znaków z klawiatury np.: QWERTY","12345678",itp.

3) należy stosować:
a) hasła zawierające kombinacje liter i cyfr,
b) hasła zawierające znaki specjalne: znaki interpunkcyjne, nawiasy, symbole @, #, &, itp. o ile system informatyczny na to pozwala
c) hasła, które można zapamiętać bez zapisywania,
d) hasła łatwe i szybkie do wprowadzenia, po to by trudniej było podejrzeć je osobom trzecim,

13. Zmiany hasła nie wolno zlecać innym osobom.
14. W systemach, które umożliwiają opcję zapamiętania nazw użytkownika lub jego hasła nie należy korzystać z tego ułatwienia.

Rozdział 3
Procedury związane z realizacją zadań w systemach informatycznych

§ 6. Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu informatycznego.

1. Rozpoczęcie pracy w systemie informatycznym na stacji roboczej wymaga wprowadzenia indywidualnego identyfikatora i hasła użytkownika.
2. W przypadku pracy kilku użytkowników na jednej stacji roboczej wymagane jest wprowadzanie odrębnych identyfikatorów i haseł przez poszczególnych użytkowników (tzw. przelogowanie).
3. W przypadku braku możliwości wprowadzenia indywidualnego identyfikatora i/lub hasła, bądź braku dostępu do określonych zasobów systemu, wymagany jest niezwłoczny kontakt z ASI.
4. Zakończenie pracy na stacji roboczej następuje po prawidłowym wylogowaniu się użytkownika i wyłączeniu komputera oraz wyłączeniu zasilacza awaryjnego lub listwy zasilającej.
5. Stacje robocze wyposażone są w wygaszacze ekranu, włączające się najpóźniej po 5 minutach od przerwania pracy. Wznowienie pracy w systemie przy aktywnym wygaszaczu wymaga wpisania odpowiedniego hasła użytkownika.
6. W przypadku konieczności opuszczenia stanowiska pracy użytkownik obowiązany jest niezwłocznie zablokować ekran ręcznie (opcja „Zablokuj" z menu „Start" lub kombinacja klawiszy "klawisz z logo Windows i klawisz L") lub wylogować się z systemu. Wznowienie pracy wymaga wprowadzenia odpowiedniego hasła użytkownika i tym samym odblokowania ekranu monitora lub ponownego uruchomienia systemu.
7. Należy uniemożliwiać podgląd danych osobowych przez osoby nieuprawnione na:
   1) ekranach komputerów, w szczególności przez stosowanie wygaszaczy ekranów i odpowiednie ustawienie ekranów,
   2) wydrukach i nośnikach informacji, leżących na biurkach oraz w pobliżu stanowiska pracy w zasięgu osób nieuprawnionych.
8. Przed opuszczeniem miejsca pracy należy:
   1) zakończyć pracę na stacji roboczej zgodnie z ust. 4,
   2) wszelkie akta, dokumenty i/lub wydruki zawierające dane osobowe schować do zamykanych na klucz szaf, a niepotrzebne zniszczyć w sposób uniemożliwiający ich odtworzenie (np. w niszczarce),
   3) schować w ustalonym miejscu klucze od szaf lub zabrać je ze sobą.
   4) zamknąć otwarte wcześniej okna,
   5) opuszczając pokój, należy zamknąć za sobą drzwi na klucz, a klucz zabrać ze sobą, nie pozostawiając klucza w drzwiach.

9. Komputery wyposażone są w odpowiednie programy ochrony antywirusowej, których aktualizacja następuje automatycznie, kiedy komputer jest podłączony do sieci Internet, a w przypadku komputerów niepodłączonych do sieci Internet – ręcznie przez Informatyka.
10. Obowiązuje zakaz robienia kopii całych zbiorów danych lub ich fragmentów na potrzeby niezwiązane z realizowanymi zadaniami. W innych przypadkach zbiory danych mogą być kopiowane tylko przez ASI, ABI lub automatycznie przez system informatyczny, z zachowaniem procedur ochrony danych osobowych.
11. Obowiązuje bezwzględny zakaz używania i wynoszenia poza teren Urzędu jakichkolwiek zewnętrznych nośników informacji lub dokumentów zawierających dane osobowe bez uprzedniej zgody Administratora Danych Osobowych, z wyjątkiem sytuacji, w których jest to niezbędne ze względu na specyfikę realizowanego zadania.
12. Obowiązuje bezwzględny zakaz samodzielnej modernizacji oprogramowania i sprzętu przez użytkowników na stacjach roboczych. Wszelkie zmiany mogą być dokonywane tylko przez Informatyka lub pod jego nadzorem, stosownie do wymagań niniejszej Instrukcji i/lub instrukcji użytkowania systemu, programu, urządzenia, itp.
13. W razie wystąpienia usterek w pracy komputerów lub błędów wygenerowanych przez system informatyczny, a także w razie konieczności ręcznej aktualizacji oprogramowania należy zgłosić ten fakt ASI.
14. Przy przetwarzaniu danych osobowych na komputerach przenośnych obowiązują procedury jak podczas pracy na komputerach stacjonarnych. Dodatkowo:
    1) obowiązuje bezwzględny zakaz używania komputerów przenośnych przez osoby inne niż użytkownicy, którym zostały one powierzone,
    2) użytkownicy, którym zostały powierzone komputery przenośne, powinni chronić je przed uszkodzeniem, kradzieżą i dostępem osób postronnych, a także zachować szczególną ostrożność podczas ich transportu,
    3) Informatyk prowadzi ewidencję powierzenia i zwrotu komputerów przenośnych.

§ 7. Procedury tworzenia, przechowywania i niszczenia kopii zapasowych

1. Zbiory danych osobowych przetwarzane w systemie informatycznym są przechowywane na serwerze obsługującym system informatyczny Administratora Danych Osobowych, przy czym dane przetwarzane w systemie informatycznym na stacjach roboczych są niezwłocznie umieszczane w odpowiednich miejscach na serwerze,
2. Kopie bezpieczeństwa komputerowych zbiorów danych osobowych oraz kopie systemów informatycznych są wykonywane całościowo po stronie serwera, na którym się znajdują, na taśmach magnetycznych i/lub zewnętrznych dyskach twardych. Kopiowanie następuje automatycznie w każdym dniu roboczym o określonej stałej porze. Taśmy magnetyczne i dyski zewnętrzne są wymieniane przed każdym zapisem z zachowaniem tygodniowego cyklu rotacji. Całkowity czas użytkowania nośników jest zgodny z zaleceniami producenta.
3. Nad poprawnym wykonywaniem kopii bezpieczeństwa nadzór sprawuje Informatyk.
4. W celu zapewnienia poprawności wykonywanych kopii bezpieczeństwa Informatyk, co najmniej raz w miesiącu, poddaje testowi cyklicznie wybraną kopię. Próba polega na odtworzeniu danych w warunkach testowych i sprawdzeniu, czy jest możliwość ich odczytania.
5. Kopie bezpieczeństwa przechowuje się przez okres co najmniej 7 dni, ale nie dłużej niż konieczność ich używania, w szafie ogniotrwałej w pomieszczeniu innym niż Serwerownia, wyposażonym w system wykrywania pożaru. Dostęp do kopii bezpieczeństwa posiada wyłącznie Informatyk, Kierownik Referatu Organizacyjno-Gospodarczego oraz inny upoważniony pracownik Urzędu.
6. Po zakończeniu eksploatacji lub uszkodzeniu zewnętrznych nośników danych służących do sporządzania kopii zapasowych dokonuje się fizycznego ich zniszczenia w sposób
uniemożliwiających ich odczytanie.

§ 8. Procedura używania, przechowywania i niszczenia elektronicznych nośników informacji zawierających dane osobowe

1. Elektroniczne zewnętrzne nośniki informacji mogą być używane w wyjątkowych sytuacjach związanych z realizacją określonych zadań, a w innych przypadkach wyłącznie za zgodą ABI.
2. W przypadku posługiwania się elektronicznymi nośnikami informacji pochodzącymi od podmiotu zewnętrznego, użytkownik jest zobowiązany do uprzedniego sprawdzenia go programem antywirusowym w celu wyeliminowania ewentualnych zagrożeń.
3. Elektroniczne zewnętrzne nośniki informacji zawierające dane osobowe są przechowywane w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem zgodnie z wymogami przewidzianymi dla danych osobowych w formie tradycyjnej (papierowej) w Polityce bezpieczeństwa.
4. Nośniki informacji jednorazowego użytku takie jak płyty CD-R, DVD-R, zawierające nieaktualne lub zbędne kopie danych likwiduje się poprzez fizyczne zniszczenie w taki sposób, by nie można było odczytać ich zawartości.
5. Nośniki informacji wielorazowego użytku, takie jak dyski twarde, pendrive, płyty CD-RW, DVD-RW, dyskietki, itp., zawierające nieaktualne lub zbędne kopie danych, można wykorzystać ponownie po uprzednim usunięciu ich zawartości w sposób uniemożliwiający ich odzyskanie.
6. Nośniki informacji wielorazowego użytku nienadające się do ponownego użycia, a mogące zawierać dane osobowe, niszczy się fizycznie w taki sposób, by nie można było odczytać ich zawartości.

Rozdział 4
Zasady zabezpieczania i kontroli systemów informatycznych, w których przetwarzane są dane osobowe.

§ 9. Sposób zabezpieczenia systemu informatycznego przed działalnością programowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego

1. W Urzędzie nie wyodrębnia się stacji roboczych dedykowanych do przetwarzania danych osobowych, a wszystkie stanowiska komputerowe są połączone z siecią wewnętrzną i pośrednio z siecią publiczną.
2. Z uwagi na wysokie ryzyko ingerencji wirusów komputerowych oraz wszelkiego rodzaju innego szkodliwego oprogramowania pochodzącego z sieci publicznej oraz użycia zewnętrznych elektronicznych nośników informacji, w Urzędzie na wszystkich serwerach i stacjach roboczych, stosuje się oprogramowanie antywirusowe. Dodatkowo dostęp do sieci publicznej z poszczególnych stacji roboczych jest chroniony centralnie specjalnym urządzeniem sprzętowym typu Firewall, który stanowi jedyne połączenie z siecią zewnętrzną.
3. Sprawdzanie obecności wirusów komputerowych w systemie informatycznym oraz ich usuwanie odbywa się przy wykorzystaniu oprogramowania, sprawującego ciągły nadzór (ciągła praca w tle) nad pracą systemu informatycznego i jego zasobami oraz serwerami i stacjami roboczymi.
4. Każdy e-mail wpływający do Urzędu musi być sprawdzony pod kątem występowania wirusów przez bramę antywirusową.
5. Zabrania się używania nośników niewiadomego pochodzenia bez wcześniejszego sprawdzenia ich programem antywirusowym. Sprawdzenia dokonuje użytkownik, który nośnik zamierza użyć.
6. Zabrania się pobierania z Internetu plików niewiadomego pochodzenia. Każdy plik pobrany z Internetu musi być sprawdzony programem antywirusowym. Sprawdzenia dokonuje użytkownik, który pobrał plik.
7. Zabrania się odczytywania załączników poczty elektronicznej bez wcześniejszego sprawdzenia ich programem antywirusowym. Sprawdzenia dokonuje pracownik, który pocztę otrzymał.
8. Administrator Systemu Informatycznego przeprowadza cykliczne kontrole antywirusowe na wszystkich komputerach - minimum raz na kwartał.

9. Kontrola antywirusowa przeprowadzana jest również na wybranym komputerze w przypadku zgłoszenia nieprawidłowości w funkcjonowaniu sprzętu komputerowego lub oprogramowania.
10. W przypadku wykrycia wirusów komputerowych sprawdzane jest stanowisko komputerowe, na którym wirusa wykryto oraz wszystkie posiadane przez użytkownika dyskietki.
11. Niezależnie od ciągłego nadzoru, o którym mowa w ust. 3, ASI:
    1) nie rzadziej niż raz na miesiąc przeprowadza pełną kontrolę obecności wirusów komputerowych w systemie oraz jego zasobach, jak również w serwerach i stacjach roboczych,
    2) nie rzadziej niż raz na 90 dni przeprowadza wyrywkową kontrolę aktualności programu antywirusowego oraz obecności wirusów komputerowych w komputerach przenośnych będących własnością Urzędu.
12. Do obowiązków ASI należy nadzór nad zakupem i przechowywaniem odpowiednich licencji oprogramowania antywirusowego.
13. Użytkownik jest obowiązany niezwłocznie zawiadomić Informatyka o pojawiających się komunikatach, wskazujących na wystąpienie zagrożenia wywołanego szkodliwym oprogramowaniem.

§ 10. Kontrola nad wprowadzaniem, dalszym przetwarzaniem i udostępnianiem danych osobowych

1. Należy dążyć, aby każdy system informatyczny Administratora Danych Osobowych zapewniał w sposób automatyczny, po zatwierdzeniu przez użytkownika operacji wprowadzenia danych odnotowanie:
    1) daty pierwszego wprowadzenia danych do systemu,
    2) przypisanie wprowadzanych danych użytkownikowi (identyfikatorowi użytkownika), który te dane wprowadza do systemu,
    3) źródła danych, w przypadku zbierania danych nie od osoby, której one dotyczą,
    4) informacji o odbiorcach danych w rozumieniu art. 7 pkt. 6 ustawy, którym dane zostały udostępnione oraz dacie i zakresie tego udostępnienia (chyba, że system informatyczny jest używany do przetwarzania danych w zbiorach jawnych),
2. Dla każdej osoby, której dane są przetwarzane w danym systemie informatycznym, system zapewnia sporządzenie i wydrukowanie raportu zawierającego w powszechniej zrozumiałe formie informacji, o której mowa w ust. 1.

Rozdział 5
Konserwacje, przeglądy i naprawy systemów informatycznych zawierających zbiory danych osobowych.

§ 11. Procedury wykonywania przeglądów, konserwacji i naprawy systemów oraz elektronicznych nośników informacji służących do przetwarzania danych

1. Doraźne przeglądy i konserwacje oraz drobne naprawy lub zmiany systemu informatycznego oraz Sewerów i stacji roboczych Administratora Danych Osobowych są dokonywane przez ASI. Pozostałe przeglądy, konserwacje, naprawy lub zmiany są przeprowadzane przez serwisanta lub inny podmiot zewnętrzny pod nadzorem ASI w siedzibie Administratora Danych Osobowych z zachowaniem zasad ochrony danych osobowych.
2. Jeśli jest to konieczne naprawy i zmiany mogą być dokonywane przez serwisanta danego systemu poza siedzibą Administratora Danych Osobowych wyłącznie na podstawie odpowiednich umów zawierających zapisy o powierzeniu przetwarzania danych osobowych lub po uprzednim usunięciu danych w nich przetwarzanych w sposób uniemożliwiający ich odczytanie.

Rozdział 6
Zasady zarządzania sprzętem i oprogramowaniem komputerowym

§ 12. Stosowanie oprogramowania.

1. Do każdego komputera przypisana jest licencja oprogramowania zgodnie z zasadą: 1 komputer = 1 licencja"
2. Stacje robocze korzystające z serwera muszą mieć zakupione licencje dostępowe zgodnie z zasadą: „1 komputer = 1 licencja dostępowa"
3. Wszelkie oprogramowanie na stacjach roboczych instaluje ASI. Zabrania się instalowania jakiegokolwiek oprogramowania bez zgody ASI.
4. Zabrania się instalowania tej samej licencji na wielu komputerach, chyba że warunki licencji na to zezwalają.
5. Każda zainstalowana licencja oprogramowania musi posiadać określoną liczbę atrybutów legalności.
6. Zabrania się stosowania programów komputerowych w wersji edukacyjnej, które podlegają graniczonemu rozpowszechnianiu, jak również wersji oprogramowania, których licencja nie zezwala na użytkowanie w celach komercyjnych.
7. Zabrania się używania w Urzędzie oprogramowania prywatnego, z wyjątkiem łącznego spełnienia następujących wymagań:
   1) Właściciel oprogramowania złoży oświadczenie, że:
      a) jego użycie jest niezbędne dla terminowego wykonania zadania publicznego, a nabycie tegoż oprogramowania na własność Urzędu w danej chwili jest niemożliwe z przyczyn zewnętrznych
      b) jest właścicielem licencji oprogramowania, na którego używanie w siedzibie Urzędu otrzymał zgodę,
      c) ASI zainstaluje oprogramowania a po zakończeniu pracy z programem odinstaluje to oprogramowanie bezzwłocznie.
8. Zabrania się powielania oprogramowania dla celów kopii zapasowych lub dodatkowych instalacji
9. Zabrania się sporządzania kopii oprogramowania na dyskach komputerów.
10. Zabrania się przechowywania na dyskach komputerowych oraz na stanowisku pracy oprogramowania lub innych przedmiotów, których używanie jest naruszeniem ustawy o prawie autorskim i prawach pokrewnych.
11. Pracownik korzysta ze sprzętu i oprogramowania komputerowego tylko i wyłącznie do wykonywania swoich obowiązków pracowniczych

§ 13. Zakup sprzętu i oprogramowania komputerowego

1. Zakupy sprzętu i oprogramowania dokonuje się tylko w ilościach odpowiadających potrzebom Urzędu.
2. Wprowadza się centralizację zakupów, poprzez:
   1) Wszystkie zakupy sprzętu i oprogramowania są koordynowane przez ASI w porozumieniu z Sekretarzem Urzędu po uzgodnieniu wydatków ze Skarbnikiem Gminy.
   2) Zakupów sprzętu oprogramowania należy dokonywać tylko u producentów oprogramowania lub w autoryzowanych punktach sprzedaży.
   3) Do zakupów sprzętu komputerowego stosuje się zasady dotyczące zamówień publicznych,
   4) Zakupu sprzętu i oprogramowania komputerowego dokonuje ASI lub osoba przez niego upoważniona
   5) Zlecenia lub umowy zakupu i dostawy sprzętu, zakupu oprogramowania komputerowego podpisuje Wójt.

§ 13. Likwidacja sprzętu i oprogramowania komputerowego

1. Likwidacji podlega sprzęt i oprogramowanie komputerowe, które:
   1) nie są i nie będą mogły być wykorzystywane w realizacji zadań związanych z działalnością jednostki, lub

2) nie nadają się do dalszego użytku ze względu na zły stan techniczny, a ich naprawa byłaby nieopłacalna, lub
3) nie nadaje się do współpracy z pozostałym sprzętem lub/i oprogramowaniem w jednostce, a ich przystosowanie byłoby technicznie i ekonomicznie nieuzasadnione
4) posiadają wady lub uszkodzenia, których naprawa byłaby nieopłacalna, lub
5) podczas przeprowadzonej inwentaryzacji oprogramowania wykryto braki odpowiedniej liczby atrybutów (dot. wyłącznie oprogramowania)

§ 14.Procedura likwidacji sprzętu komputerowego

1. Wymieniany sprzęt komputerowy nie może być z Urzędu zbywany, oddawany lub w inny sposób przekazywany osobom trzecim w całości, z zastrzeżeniem ust. 2.
2. Dopuszcza się jego zbycie, oddanie lub przekazanie pod warunkiem wymontowania nośników informacji (twardych dysków). Procedurę tą nadzoruje ABI sporządzając odpowiednią dokumentację (protokół pozbawienia nośnika informacji, komisyjne zniszczenie nośnika, itp.)
3. Niezdatny do użytku sprzęt komputerowy wraz z wyposażeniem, zgodnie z rozporządzeniem Ministra Środowiska z dnia 27 września 2001r. w sprawie katalogu odpadów (Dz. U. Nr 112 poz.1206), stanowi odpady, musi być zbierany selektywnie i poddany unieszkodliwieniu.
4. W przypadku niezdatnego do dalszego użytku sprzętu komputerowego pracownik merytoryczny lub osoba materialnie odpowiedzialna za ten sprzęt składa informację do ASI o jego wybrakowanie podając przyczynę kasacji.
5. Opinię techniczną sporządza ASI, a w przypadku gdy sprzęt ten objęty jest jeszcze gwarancją wymagana jest opinia niezależnego eksperta spoza Urzędu.
6. Po zaakceptowaniu przez Wójta opinii technicznej, ASI wymontowuje z komputera dyski lub inne elektroniczne nośniki informacji i przekazuje je do ABI za pokwitowaniem, wskazując z jakiej stacji roboczej one pochodzą.
7. Pozbawiony nośników informacji sprzęt komputerowy deponuje się w składzie zużytego sprzętu elektronicznego, do czasu jego odbioru przez firmę dokonującą jego unieszkodliwienia.
8. ASI, o pozbawieniu sprzętu nośników informacji i zdeponowaniu w składzie zużytego sprzętu elektronicznego informuje pracownika merytorycznego prowadzącego ewidencję środków trwałych, wartości niematerialnych i prawnych oraz wyposarzenia w Urzędzie, który dokonuje niezbędnych umorzeń i przeszacowań.
9. Wszelkie czynności związane z przekazaniem odbiorcy zużytego sprzętu elektronicznego nadzoruje ASI. Odbiorcą zlikwidowanego sprzętu komputerowego, zniszczonych urządzeń, dysków lub innych elektronicznych nośników danych oraz rozdrobnionych magnetycznych i optycznych nośników danych może być firma, która uzyskała zezwolenie na prowadzenie działalności na podstawie art. 26 ust. 1 ustawy z dnia 27 kwietnia 2001 r. o odpadach (Dz. U. Nr 62 poz. 628 z późn. zm.)
10. Firma dokonująca unieszkodliwienia sprzętu przy jego odbiorze dokonuje na miejscu jego zważenia i wystawia protokół odbioru sprzętu. Jedna kopia protokołu odbioru pozostaje w Urzędzie.

§ 15.Procedura likwidacji oprogramowania:

1. W przypadku gdy oprogramowanie zostało zakupione w licencji OEM, jego likwidacja następuje równocześnie z likwidacją sprzętu z którym zostało zakupione.
2. ASI przekazuje wniosek o likwidację oprogramowania do ABI z podaniem przyczyn nieprzydatności oprogramowania. Po akceptacji przez Wójta wniosku o likwidację oprogramowania, ASI dokonuje odinstalowania oprogramowania ze stacji roboczej komputera.
3. Jeżeli zlikwidowane oprogramowanie było zakupione wraz z nośnikami nośniki te przekazywane są do ABI celem przechowania do czasu ich kasacji (fizycznego zniszczenia).
4. Niszczenie nośników informacji dokonuje w miarę potrzeb, komisja powołana przez Wójta zarządzeniem, składająca się z ABI, ASI i innych pracowników Urzędu. Wraz z fizycznym

zniszczeniem nośników informacji, komisja niszczy również pozostałe atrybuty legalności zlikwidowanego oprogramowania lub w sposób trwały dokonuje adnotacji na tych atrybutach (np. na umowie licencyjnej). Z fizycznego zniszczenia nośników informacji sporządza się protokół.

5. Dokumentację w tej sprawie prowadzi ABI.
6. Na podstawie protokołu kasacji :
   1) ASI zdejmuje oprogramowanie z ewidencji ilościowej – Metryki komputera.
   2) pracownik prowadzący ewidencję środków trwałych, wartości niematerialnych i prawnych oraz wyposarzenia w Urzędzie, dokonuje niezbędnych umorzeń i przeszacowań
7. Zniszczone nośniki przekazywane są do utylizacji wraz ze zlikwidowanym sprzętem komputerowym, na zasadach określonych w § 14 ust. 9 i 10 niniejszej instrukcji.

§ 16.Inwentaryzacja sprzętu komputerowego i oprogramowania

1. Inwentaryzację sprzętu komputerowego ma na celu:
   1) Określenie liczby komputerów osobistych, notebooków i serwerów używanych przez Urząd.
   2) Nadanie dla każdego z komputerów indywidualnego oznaczenia (zgodnego z ewidencją środków trwałych) oraz sporządzenie dla każdego stanowiska komputerowego „**Metryki Komputera**" wg wzoru określonego **załącznikiem Nr 1** do niniejszej instrukcji.
   3) Kontrolowanie okresów gwarancyjnych na zakupiony sprzęt komputerowy.
2. Inwentaryzacja oprogramowania ma na celu:
   1) Określenie rodzaju i ilości oprogramowania zainstalowanego na każdym komputerze.
   2) Porównanie zebranych informacji z faktycznie posiadaną przez Urząd liczbą licencji - porównanie odbywa się poprzez wskazanie odpowiedniej liczby atrybutów legalności dla każdej licencji.
   3) Zebranie wersji instalacyjnych oprogramowania wraz z jego dokumentacją w teczkach inwentarzowych przechowywanych w jednym centralnym miejscu przez ASI.
   4) Wyjaśnienie wszelkich niedoborów atrybutów legalności.
   5) Zakup niezbędnego, brakującego oprogramowania aby zapewnić wywiązywanie się z umów licencyjnych
   6) Przypisanie oprogramowania do poszczególnych komputerów, sporządzenie charakterystyki oprogramowania i założenie teczek inwentarzowych
3. Inwentaryzacja oprogramowania zainstalowanego na komputerze polega na:
   1) Określeniu rodzajów oprogramowania zainstalowanych na poszczególnych komputerach (stacjach roboczych);
   2) Ustalenia czy komputer chroniony jest hasłem w czasie jego uruchomienia.
   3) Ustalenia, czy zbiory danych osobowych chronione są hasłem.
   4) Zebranie licencji na oprogramowanie znajdujących się w Urzędzie, a jeżeli licencja była aneksowania, również aneksów stanowiących integralną część licencji;
   5) Porównanie zebranych informacji z faktycznie posiadaną przez Urząd liczbą licencji (porównanie odbywa się poprzez wskazanie odpowiedniej liczby atrybutów legalności dla każdej licencji oraz czasu na jaki okres licencja została zakupiona.
   6) Zebranie wersji instalacyjnych oprogramowania zainstalowanego na komputerze.
   7) Sporządzenie **„Charakterystyki zainstalowanego oprogramowania"** – wg wzoru stanowiącego **załącznik Nr 2** do niniejszej instrukcji. Jeżeli zainstalowane na komputerze programy są programami darmowymi (do powszechnego użytku) również odnotowanie tego faktu w karcie „Charakterystyki zainstalowanego oprogramowania".
   8) Zdeponowanie zgromadzonych i wytworzonej dokumentacji, o której mowa w ust. 1 w teczce inwentarzowej.
4. Teczka inwentarzowa dla poszczególnych stacji roboczych (komputerów) zawiera następujące materiały i dokumentacje:
   1) „Metrykę komputera",– prowadzoną wg wzoru kreślonego Załącznikiem Nr do niniejszej instrukcji;
   2) „Charakterystykę zainstalowanego oprogramowania" ;

3) Dokumentację zakupu komputera i urządzeń towarzyszących (np. kserokopie faktur) – jeżeli możliwe jest dotarcie do tych dokumentów;
4) Kart gwarancyjnych – jeżeli komputer objęty jest gwarancją;
5) Nośniki zawierające wersje instalacyjne oprogramowania (np. płyty instalacyjne);
6) Dokumenty potwierdzające zakup licencji oprogramowania, a jeżeli licencja dotyczy kilku stanowisk wskazanie miejsca, w którym są przechowywane licencje (np. inna teczka inwentarzowa).

5. Teczkę inwentarzową przechowuje na stanowisku pracy ASI
6. Inwentaryzację sprzętu komputerowego wraz z oprogramowaniem wykonuje ASI raz w roku w terminie do 30 września każdego, tak aby ewentualne braki lub potrzeby zakupu licencji uwzględnić w projekcie budżetu gminy.
7. Z przeprowadzonej inwentaryzacji ASI sporządza sprawozdanie, które przekazuje Wójtowi i ABI.

§ 17. Audyt wewnętrzny sprzętu i oprogramowania komputerowego

1. Za przeprowadzenie audytu odpowiada ASI.
2. Audyt obejmuje:
   1) kontrolę legalności zainstalowanego oprogramowania poprzez identyfikację zainstalowanych aplikacji na komputerach pracowników Urzędu
   2) skanowanie zawartości dysków w celu wyeliminowania ukrytych zawartości plików
   3) kontrolę modyfikacji sprzętu komputerowego
   4) prowadzenie statystyk w zakresie:
      a) wykorzystywania poszczególnych aplikacji
      b) rzeczywistego czasu pracy poszczególnych stacji roboczych
      c) korzystania z internetu
3. ASI na bieżąco monitoruje wszystkie komputery Urzędu.
4. Jakiekolwiek wykryte działania użytkowników, które stanowią naruszenie niniejszej instrukcji podlegają natychmiastowemu powstrzymaniu /usunięciu.
5. O zdarzeniach opisanych w ust. 4 ASI ma obowiązek informować na bieżąco ABI.

§ 18.Korzystanie z internetu, sieci wewnętrznej i skrzynek e-mail.

1. Każdemu pracownikowi zatrudnionemu na stanowiskach urzędniczych i kierowniczych stanowiskach urzędniczych, Urząd zapewnia:
   1) możliwość korzystania z internetu.
   2) możliwość korzystania z sieci wewnętrznej
2. Użytkownicy mogą korzystać z dostępu do internetu tylko w celach służbowych, w celu poprawy ich wiedzy zawodowej, dostępu do informacji prawnych, naukowych, technicznych i innych informacji na tematy, które maja związek z wykonywaniem obowiązków służbowych.
3. Zabrania się przeglądania stron zawierających treści niezgodne z prawem oraz o charakterze pornograficznym, rasistowskim, niemoralnym, nieetycznym, propagujących przemoc lub nienawistne zachowania.
4. Praca w sieci internet nie może zagrażać bezpieczeństwu systemów informatycznych. Pracodawca może wprowadzić kategoryzacje stron internetowych, oraz zablokować dostęp do wybranych kategorii,
5. Zabrania się;
   1) wykorzystywania sieci Internet w sposób, który mógłby narazić Pracodawcę na utratę dobrego imienia,
   2) pobierania filmów, plików muzycznych i instalowania programów (w tym wersji darmowych, do których zainstalowania na komputerze uprawniony jest wyłącznie ASI.
   3) udostępniania łącza internetowego dostarczonego przez pracodawcę innym osobom,
   4) instalowania urządzeń udostępniających Internet na sprzęcie Pracodawcy bez zgody ASI

§ 19.Korzystanie ze skrzynek e-mail.

1. Pracownikom, o których mowa w ust. 1, Urząd nadaje służbowe adresy poczty e-mail.

2. Pracownik jest zobowiązany do korzystania z przyznanego adresu poczty elektronicznej do wszelkiej korespondencji z innymi pracownikami oraz klientami bądź kontrahentami.
3. Poczta elektroniczna może być wykorzystywana tylko do celów służbowych uwzględniając ogólnie przyjęte zasady netykiety. Zabrania się rozsyłania m.in.:
   1) ogłoszeń komercyjnych,
   2) tzw, łańcuszków szczęścia (listów, które wykorzystując elementy socjotechniki generują niepożądany ruch na serwerach poczty elektronicznej).
   3) treści wulgarnych,
   4) materiałów erotycznych,
   5) treści niezgodnych z obowiązującymi przepisami prawa,
4. Korespondencja, którą przechowuje i dostarcza system pocztowy jest własnością Pracodawcy.
5. W przypadku podejrzenia naruszenia zasad korzystanie ze służbowej poczty elektronicznej Pracodawca w celach dowodowych oraz bezpieczeństwa systemów ma prawo:
   1) w obecności pracownika do kontroli skrzynek pocztowych użytkowników.
   2) w uzasadnionych przypadkach natychmiastowej blokady skrzynki pocztowej.
6. Pracownik nie powinien otwierać linków oraz załączników poczty elektronicznej ze źródeł niewiadomego pochodzenia. Po pojawieniu się nieoczekiwanych listów lub załączników powinno się informować informatyka.
7. W przypadku dostępu do poczty elektronicznej z sieci Internet należy przeczytać uważnie pojawiające się w przeglądarce komunikaty o alertach bezpieczeństwa i nigdy nie ignorować ostrzeżeń.
8. Skrzynki pocztowe posiadają ograniczoną wielkość. Użytkownik zobowiązany jest do okresowej archiwizacji wiadomości oraz usuwanie zbędnych wiadomości.
9. Pracownik ma prawo korzystać ze służbowej poczty elektronicznej w celach prywatnych wyłącznie okazjonalnie, gdzie jest to uzasadnione stosownymi okolicznościami.
10. Za administrację skrzynkami e-mail odpowiada ASI.
11. Postanowienia § 5 ust. 2 do 13 niniejszej instrukcji stosuje się odpowiednio do haseł poczty elektronicznej.

§ 20.Korzystanie z sieci wewnętrznej.

1. Pracownikom, o których mowa w ust. 1, Urząd nadaje służbowe adresy poczty wewnętrznej.
2. Skrzynki poczty wewnętrznej służą do:
   1) przesyłania dokumentów elektronicznych wewnątrz Urzędu (z pominięciem sieci publicznej).
   2) Zamieszczania przepisów wewnętrznych, informacji, ogłoszeń itp.
   3) Wymiany dokumentów między pracownikami Urzędu.
3. Pracownik korzystający z wewnętrznej poczty publikuje lub zamieszcza dokumenty wyłącznie na własnej skrzynce.
4. Zabrania się:
   1) Zamieszczania lub publikowania dokumentów na skrzynkach innych pracowników,
   2) Przechowywania w poczcie wewnętrznej (skrzynce) dokumentów zawierających dane osobowe lub zbiory danych osobowych.
5. W przypadku publikowania dokumentów lub zbiorów danych zawierających dane osobowe niezbędnych w pracy na innym stanowisku, obowiązkiem pracownika, po udostępnieniu, jest niezwłoczne usunięcie dokumentu (zbioru) z własnej skrzynki.
6. Za administrację skrzynkami poczty wewnętrznej odpowiada ASI.
7. Przyjmuje się, nazwy skrzynek identyczne z pierwszym członem adresu poczty elektronicznej.
8. ABI dokonuje okresowego przeglądu zawartości poczty wewnętrznej (skrzynek) pod kątem zamieszczanych tam informacji.

§ 21. Postanowienia końcowe

1. W sprawach nieuregulowanych niniejszą Instrukcją należy stosować postanowienia Polityki bezpieczeństwa, a także instrukcje obsługi i zalecenia producentów aktualnie wykorzystywanych urządzeń i programów oraz umów serwisowych.
2. Każda osoba upoważniona do przetwarzania danych osobowych jest zobowiązana zapoznać się z niniejszą Instrukcją przed dopuszczeniem do przetwarzania danych oraz złożyć stosowne oświadczenie, potwierdzające znajomość jej treści.
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 kp. 2.
4. 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.

WÓJT
Andrzej Twardowski

Załącznik Nr 1
do instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych
w Urzędzie Gminy w Szczutowie

WZÓR

KARTA METRYKI KOMPUTERA

Dane techniczne komputera

Komputer				CPU	RAM	HDD	Karta		
Nazwa	Numer seryjny	Typ SR – Stacja robocza S – serwer N- notebok	lokalizacja				graficzna	sieciowa	inna
1	2	3	4	5	6	7	8	9	10

Urządzenia towarzyszące:

Monitor		Drukarka		Skaner		UPS	Listwa	Klawiatura	Mysz
Typ-model ze znakiem: K-kineskopowy P- Płaski	Numer seryjny	Typ - model	Numer seryjny	Typ - model	Numer seryjny	T-Tak N-Nie	T-Tak N-Nie	T-Tak N - Nie	T-Tak N-Nie
11	12	13	14	15	16	17	18	19	20

Dane uzupełniające:

Inne dane komputera i urządzeń towarzyszących , nie wymienione w kolumnach 1 – 20	Uwagi
21	22

Kartę sporządziła /sporządził :

.....
/ Imię i nazwisko – stanowisko służbowe/

....
/data/ / podpis/

Załącznik Nr 1
do instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych
w Urzędzie Gminy w Szczutowie

WZÓR

KARTA

CHARAKTERYSTYKI ZAINSTALOWANEGO OPROGRAMOWANIA

Komputer				
Nazwa	Numer seryjny	Typ SR – Stacja robocza S – serwer N- natebok	lokalizacja	Ochrona hasłem w czasie uruchamiania T-Tak N-Nie
1	2	3	4	5

Na wymienionym wyżej komputerze zainstalowane jest następujące oprogramowanie:

Lp.	Pełna nazwa zainstalowanego na komputerze oprogramowania	Wykaz atrybutów legalności (ze wskazaniem ich lokalizacji)	Uwagi (np. zabezpieczenie hasłem, inne)
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			

Kartę sporządziła /sporządził :

.....
/ Imię i nazwisko – stanowisko służbowe/

....
/data/ / podpis/