WÓJT GMINY SANOK
woj. podkarpackie

Zarządzenie Nr 51 /2013
Wójta Gminy Sanok z dnia 13 maja 2013r.

w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji i Instrukcji Zarządzania Systemem Informatycznym

Na podstawie art. 31 oraz art. 33 ust. 3 w związku z art. 11a ust. 1 pkt 2 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (t. j. w Dz. U. z 2001 r. Nr 142, poz. 1591 ze zm.) oraz § 4 i § 5 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakimi powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024),

zarządza się co następuje:

§ 1

Wprowadza się do użytku służbowego „Politykę Bezpieczeństwa Informacji" w zakresie przetwarzania danych osobowych w Urzędzie Gminy w Sanoku stanowiącą załącznik nr 1 do niniejszego zarządzenia oraz „Instrukcję Zarządzania Systemem Informatycznym" służącym do przetwarzania danych osobowych w Urzędzie Gminy w Sanoku, stanowiącą załącznik nr 2 do zarządzenia.

§ 2

Zobowiązuje się pracowników przetwarzających dane osobowe oraz przebywających w pomieszczeniach biurowych tworzących obszar, w którym przetwarzane są dane osobowe do przestrzegania przepisów zawartych w dokumentach, o których mowa w § 1.

§ 3

Zobowiązuje się Kierowników Jednostek Organizacyjnych korzystających z zasobów informatycznych Urzędu Gminy w Sanoku, w których przetwarzane są dane osobowe do sprawowania nadzoru nad ich ochroną oraz do współpracy z Administratorem Bezpieczeństwa Informacji w tym zakresie.

§ 4

Wykonanie zarządzenia powierza się Kierownikowi Referatu Spraw Obywatelskich i Administracyjnych oraz Administratorowi Bezpieczeństwa Informacji.

§ 5

Traci moc zarządzenie Nr 30/08 Wójta Gminy Sanok z dnia 14 kwietnia 2008 r. w sprawie: wprowadzenia „Polityki Bezpieczeństwa Danych Osobowych" i oraz „Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych"

§ 6

Zarządzenie wchodzi w życie z dniem podpisania.

p.o. WÓJTA GMINY SANOK
mgr [illegible] Hałas

Załącznik nr 1 do Zarządzenia
Wójta Gminy Sanok

POLITYKA BEZPIECZEŃSTWA INFORMACJI W URZĘDZIE GMINY SANOK

Opracował: Grzegorz Łybyk

Zatwierdził:

p.o. WÓJTA GMINY SANOK
mgr Anna Halas

maj 2013

1. Wstęp

O skuteczności działania i rozwoju każdej organizacji świadczy stopień osiągania zamierzonego celu. W procesie tym kluczowe jest stosowanie współczesnych technik i technologii, narzędzi i systemów informatycznych oraz przetwarzania i zarządzania informacją. Informacja jest jednym z najważniejszych zasobów Urzędu , dlatego powinna być chroniona na każdym szczeblu organizacji. Najwyższe kierownictwo Urzędu zobowiązuje się do podejmowania niezbędnych działań mających na celu zapewnienie ochrony informacji na pożądanym poziomie, a tym samym spełnienie wymaganego poziomu bezpieczeństwa systemów informacyjnych.

2. Definicje:

1) Bezpieczeństwo informacji – zachowanie poufności, integralności i dostępności informacji.
2) Ryzyko – prawdopodobieństwo wystąpienia zagrożenia, które wykorzystując podatność(ci) aktywu, może doprowadzić do jego uszkodzenia lub zniszczenia.
3) Szacowanie ryzyka – całościowy proces analizy i oceny ryzyka.
4) Aktyw/zasób – wszystko to, co ma wartość dla organizacji w zakresie informacji (zarówno informacje, jak i środki techniczne oraz organizacyjne do ich przetwarzania).
5) Poufność – zapewnienie dostępu do informacji tylko osobom upoważnionym.
6) Integralność – zapewnienie dostępu do informacji tylko osobom upoważnionym.
7) Dostępność – zapewnienie, że osoby upoważnione będą miały dostęp do informacji tylko wtedy gdy jest to uzasadnione.
8) Postępowanie z ryzykiem – proces wyboru i wdrażania środków modyfikujących ryzyko.
9) Zarządzanie ryzykiem – proces identyfikowania, kontrolowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa, które może dotyczyć systemów informacyjnych, przy zachowaniu akceptowalnego poziomu kosztów.
10) Zdarzenie związane z bezpieczeństwem informacji – określony stan systemu, usługi lub sieci, który wskazuje na możliwe naruszenie polityki bezpieczeństwa informacji, błąd zabezpieczenia lub nieznaną dotychczas sytuację, która może być związana z bezpieczeństwem.
11) Incydent związany z bezpieczeństwem informacji – pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które

stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji.

12) Dane osobowe – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osobą możliwą do zidentyfikowania jest 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. Zakres Systemu Bezpieczeństwa Informacji

Zakresy określone przez dokument Polityki Bezpieczeństwa Informacji mają zastosowanie do całego systemu informacyjnego Urzędu , w szczególności do:

1) wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych oraz papierowych, w których przetwarzane są informacje podlegające ochronie;
2) informacji będących własnością Urzędu;
3) informacji będących własnością klientów Urzędu , uzyskanych na podstawie zawartych umów;
4) wszystkich lokalizacji Urzędu , czyli budynków i pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie;
5) wszystkich pracowników w rozumieniu przepisów Kodeksu Pracy, konsultantów, stażystów i innych osób mających dostęp do informacji podlegających ochronie.

4. Deklaracja Kierownictwa w zakresie bezpieczeństwa informacji w Urzędzie

Podejście do bezpieczeństwa informacji w Urzędzie Gminy Sanok opiera się na trzech kluczowych regułach:

- Reguła poufności informacji - zapewnienie, że informacja jest udostępniana jedynie osobom upoważnionym
- Reguła integralności informacji - zapewnienie zupełnej dokładności i kompletności informacji oraz metod jej przetwarzania
- Reguła dostępności informacji - zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią aktywów tylko wtedy, gdy istnieje taka potrzeba

Priorytetowym celem kierownictwa jest spełnienie wymagań prawnych oraz zapewnienie ciągłości działania organizacji, poufności danych wrażliwych i dostępności wymaganych informacji. Przez bezpieczeństwo informacji w Urzędzie rozumie się zapewnienie dostępności, zabezpieczenie przed nieuprawnionym dostępem, naruszeniem integralności bądź zniszczeniem aktywów związanych z przechowywaniem i przetwarzaniem informacji. Zakres ochrony i podjęte środki są adekwatne do własności aktywów związanych z systemami przetwarzania informacji.

Główne cele stawiane przed systemem zarządzania bezpieczeństwem informacji:

1) zapewnienie spełnienia wymagań prawnych,
2) ochrona systemów przetwarzania informacji przed nieuprawnionym dostępem bądź zniszczeniem,
3) podnoszenie świadomości pracowników,
4) zmniejszenie ryzyka utraty informacji,
5) zaangażowanie wszystkich pracowników w ochronę informacji.

W Urzędzie zapewniamy bezpieczeństwo informacji poprzez:

1) zarządzanie ryzykiem, na które składa się:
   a) klasyfikacja zasobów i ich wartości,
   b) identyfikacja stopnia zagrożeń i ich następstw przy uwzględnieniu następujących kryteriów: skutki utraty informacji, miejsce występowania, ryzyko utraty,
   c) określenie i wdrożenie działań zabezpieczających zasoby.
2) zarządzanie zmianami, na które składa się:
   a) analiza wpływu zmian na poziom bezpieczeństwa,
   b) zapewnienie pełnej koordynacji podczas wprowadzania zmian.
3) zarządzanie ciągłością organizacji poprzez określenie i wdrożenie instrukcji i procedur awaryjnych.

Kierownictwo Urzędu zapewnia środki niezbędne do realizacji Polityki Bezpieczeństwa Informacji.

5. Organizacja bezpieczeństwa informacji w Urzędzie

Odpowiedzialność za bezpieczeństwo informacji w Urzędzie ponoszą wszyscy pracownicy zgodnie z posiadanymi zakresami obowiązków. Wójt Gminy odpowiedzialny jest za

zapewnienie zasobów niezbędnych dla funkcjonowania, utrzymania i doskonalenia systemu zarządzania bezpieczeństwem informacji oraz poszczególnych zabezpieczeń. Wydaje zgodę na użytkowanie urządzeń służących do przetwarzania informacji i zabezpieczeń rekomendowanych przez Instytucje zajmujące się ochroną informacji. Decyduje również o współpracy w zakresie bezpieczeństwa z innymi podmiotami.

Każdy pracownik Urzędu jest zapoznawany z zasadami bezpieczeństwa oraz z aktualnymi procedurami ochrony informacji w swojej komórce organizacyjnej oraz w Urzędzie zawartymi w Instrukcji podstawowych zasad bezpieczeństwa dla pracowników Urzędu. Stażyści oraz praktykanci również są zapoznawani z tymi zasadami. Kierownik komórki organizacyjnej jest odpowiedzialny za ochronę bezpieczeństwa informacji w referacie, a w szczególności za monitorowanie integralności i dostępności posiadanych zasobów informacji, nadzorowanie przestrzegania zasad bezpieczeństwa przez podległych pracowników oraz podejmowanie stosownych działań w razie stwierdzenia wystąpienia incydentu lub sytuacji mogącej prowadzić do wystąpienia incydentu bezpieczeństwa.

5.1 Dokumentacja systemu zarządzania bezpieczeństwem informacji

Dokumentacja systemu zarządzania bezpieczeństwem składa się z;

- Polityka Bezpieczeństwa Informacji w Urzędzie ;
- Deklaracja stosowania;
- Procedury i instrukcje bezpieczeństwa, które określają szczegółowo zasady postępowania;

Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania danych zawiera ***załącznik nr 1***. Opis struktury zbiorów danych wskazujący zawartość poszczególnych pół informacyjnych i powiązania między nimi przedstawia ***załącznik nr 2. Załącznik nr 3*** zawiera wykaz budynków i pomieszczeń w których są przetwarzane dane osobowe. Wniosek o nadanie uprawnień do przetwarzania danych osobowych zawiera ***załącznik nr 4***, a ***załącznik nr 5*** przedstawia wzór upoważnienia do przetwarzania danych osobowych.

5.2. Zasady współpracy z osobami trzecimi i stronami zewnętrznymi

Współpraca firmy z innymi spółkami oparta jest na umowach. Zawierając te umowy Urząd gminy ma zawsze na względzie, aby obejmowały one deklarację o zachowanie poufności oraz zobowiązania do działania zgodnie z prawem.
Każdy gość lub osoba, która wykonuje prace zlecone na terenie firmy zobligowana jest do przestrzegania następujących procedur:
· do przestrzegania reguł bhp,
· do przestrzegania reguł bezpieczeństwa przeciwpożarowego.

Dostęp do pomieszczeń wszelkiego personelu technicznego zajmującego się konserwacją sprzętu, ochrony i innych osób jest nadzorowany przez pracowników urzędu. Spółka kieruje się zasadą. Dostęp gości w strefie bezpieczeństwa jest możliwy tylko i wyłącznie w godzinach pracy.

Pomieszczenia komórek organizacyjnych przetwarzających dane osobowe wyposażono w fizyczne bariery (lady) umożliwiające obsługę klientów przy jednoczesnym odseparowaniu go od zasobów informacyjnych. Ponadto znaczna część klientów jest obsługiwana w Sekretariacie, co sprawia, że nie mają oni uzasadnionej potrzeby poruszania się po innych obszarach Urzędu . Ciągi komunikacyjne pozostają pod stałą obserwacją systemu monitoringu.

5.3. Polityka kontroli dostępu do informacji

Dostęp do informacji przechowywanych i przetwarzanych w Urzędzie jest poddany kontroli wynikającej z obowiązujących przepisów prawa powszechnego.
Kontrola polega na:

1) wydzieleniu obszarów przeznaczonych do przechowywania oraz przetwarzania poszczególnych zbiorów danych i zapewnieniu odpowiednich barier fizycznych przeciwdziałających nieuprawnionemu dostępowi;
2) zarządzaniu uprawnieniami poszczególnych użytkowników w sposób zapewniający dostęp wyłącznie do danych wymaganych do wykonywania obowiązków służbowych, jeśli dane te podlegają ochronie z jakiejkolwiek przyczyny;
3) stosowaniu bezpiecznych systemów przetwarzania informacji;
4) nadzorowaniu działalności stron trzecich, mogących wpłynąć na bezpieczeństwo informacji;

5) bieżącym informowaniu pracowników o wszelkich zmianach w zakresie regulacji dotyczących przechowywania, przetwarzania i udostępniania informacji.

Adekwatność i skuteczność stosowanych w Urzędzie środków kontroli dostępu do informacji podlega bieżącej weryfikacji w ramach auditów wewnętrznych, zmian dokumentacji i metod postępowania wynikających z ewolucji uregulowań prawnych oraz systemów przetwarzania danych a także reagowania na zagrożenia ujawnione przez inne strony. Niezależnie od tych środków weryfikacji polityka kontroli dostępu podlega co roku przeglądowi z którego zapis stanowi dane wejściowe do przeglądu systemu przez kierownictwo.

5.4. Klasyfikacja informacji

Klasyfikacja została wprowadzona w celu uporządkowania w Urzędzie postępowania z informacją, która zgodnie z ustawą o ochronie informacji niejawnych stanowi informacje jawne. Informacje te są głównym zasobem informacyjnym Urzędu, w związku z czym został uregulowany sposób postępowania z informacjami, w szczególności tymi, których ujawnienie może narazić Urząd na szkodę.

Podstawowym elementem klasyfikacji są grupy informacji. W grupach informacji zebrane zostały dokumenty logicznie ze sobą powiązane o podobnych wymaganiach związanych z bezpieczeństwem. Do określenia poziomu bezpieczeństwa danej grupy informacji przyjęto wskaźniki definiujące poufność, integralność oraz dostępność danej grupy informacji, wymagane w Urzędzie.

Przez poufność rozumiemy zapewnienie, iż dostęp do informacji mają tylko i wyłącznie osoby uprawnione. Przez integralność rozumiemy zapewnienie, iż informacje nie zostały zmienione lub zniszczone w nieautoryzowany sposób (niezgodny z wewnętrznymi regulacjami Urzędu). Przez dostępność rozumiemy zapewnienie, iż informacje będą udostępniane z zasobów o różnym poziomie bezpieczeństwa z uwagi na miejsce i sposób przechowywania. Ze względu na charakter pracy Urzędu i cel jego funkcjonowania do określenia wskaźników bezpieczeństwa największy nacisk położono na parametr integralności. Zdefiniowano trzy poziomy dla każdego z powyższych wskaźników po to, aby możliwe było powiązanie danej grupy informacji z określonym poziomem zdefiniowanego wskaźnika w skali 1-3.

Struktura klasyfikacji informacji w Urzędzie opiera się na założeniu istnienia trzech poziomów postrzegania informacji:

1) **informacje jawne** – informacje publicznie dostępne,
2) **informacje wewnętrzne** – informacje, których przetwarzanie i udostępnianie podlega restrykcjom z uwagi na szczególne znaczenie dla pracodawcy (właściciela informacji):
    a) informacje **wewnętrzne dostępne** – informacje dostępne dla wszystkich pracowników Urzędu ,
    b) informacje **wewnętrzne wrażliwe** - informacje dostępne dla grupy pracowników upoważnionych z uwagi na realizowane zadania regulaminowe,
    c) informacje **stanowiące tajemnicę pracodawcy** - informacje, których przetwarzanie i udostępnianie może narazić pracodawcę na szkodę;
3) **informacje niejawne** – informacje, do których stosuje się przepisy o ochronie informacji niejawnych lub o ochronie danych osobowych lub innych tajemnic prawnie chronionych.

6. Zarządzanie aktywami i ryzykami

Urząd zarządza swoimi aktywami informacyjnymi poprzez zapewnienie im wymaganego poziomu bezpieczeństwa. Identyfikowane są aktywa informacyjne i klasyfikowane zgodnie ze stawianymi im wymaganiami w zakresie ochrony. Ważnym elementem zarządzania aktywami i bezpieczeństwem informacji jest przeprowadzanie okresowej analizy ryzyka i opracowania planów postępowania z ryzykiem. Analiza jej wyników stanowi podstawę podejmowania wszelkich działań w zakresie doskonalenia ochrony zasobów Urzędu
Na podstawie wyników analizy ryzyka opracowywane są plany postępowania z ryzykiem dla aktywów o ryzykach większych niż ustalony poziom ryzyka akceptowalnego. Ryzyka są przeglądane na przeglądach kierownictwa oraz po zmianach mających wpływ na system bezpieczeństwa informacji.

6.1. Autoryzacja nowych urządzeń

Każde nowe lub zmienione urządzenie służące do przetwarzania informacji lub mogące w jakikolwiek inny sposób wpływać na bezpieczeństwo informacji musi zostać zweryfikowane na zgodność z wymaganiami systemu bezpieczeństwa informacji i zaakceptowane przez wskazaną osobę. O ile nie zostało to określone szczegółowo w innych opracowaniach, za dopuszczenie do użytkowania nowych urządzeń odpowiada Pełnomocnik ds. Bezpieczeństwa Informacji.

Urządzenia służące do przetwarzania informacji nie będące własnością Urzędu mogą być używane (po sprawdzeniu sprzętu pod względem kryteriów bezpieczeństwa) wyłącznie za zgodą osoby upoważnionej.

7. Zarządzanie systemami i sieciami

Urząd dba o przestrzeganie zasad związanych z utrzymywaniem i użytkowaniem systemów informatycznych i sieci. Celem takiego postępowania jest zapewnienie poufności, integralności i dostępności przetwarzanej przez nie informacji własnych. Skuteczna realizacja postawionego celu możliwa jest dzięki:

1) kompetencjom i świadomości pracowników oraz podpisanym umowom ze specjalistycznymi
1) firmami administrującymi zasobami informatycznymi;
2) opracowanym zasadom konserwacji urządzeń w celu zapewnienia ich ciągłej pracy;
3) kontrolowaniu wprowadzania wszelkich zmian do infrastruktury technicznej,
4) prowadzeniu prac rozwojowych i testowych na oddzielnych urządzeniach lub środowiskach w celu zapewnienia bezpieczeństwa systemów produkcyjnych;
5) nadzorowaniu usług dostarczanych przez strony trzecie, w szczególności odbieraniu ich i
6) akceptowaniu w sposób świadomy uwzględniający jego wpływ na istniejący system bezpieczeństwa;
7) wdrożeniu zabezpieczeń chroniących przed oprogramowaniem złośliwym i mobilnym;
8) systematycznemu tworzeniu i testowaniu kopii bezpieczeństwa;
9) przestrzeganiu opracowanych zasad postępowania z nośnikami;
10) bieżącym monitorowaniu aktywów informacyjnych

8. Bezpieczeństwo zasobów ludzkich

Urząd zapewnia kompetentną kadrę pracowniczą do realizacji wyznaczonych zadań. Celem takiego postępowania jest ograniczenie ryzyka błędu ludzkiego, kradzieży, nadużycia lub niewłaściwego użytkowania zasobów. Realizacja postawionego celu możliwa jest dzięki ustanowionym praktykom i podziałowi odpowiedzialności związanemu z weryfikacją kandydatów do pracy podczas naboru, zasadom zatrudniania pracowników oraz ustalonej procedurze rozwiązywania umów o pracę.

9. Bezpieczeństwo fizyczne, sprzętu i okablowania, konfiguracji i eksploatacji sieci

W Urzędzie określono następujące kierunkowe standardy:

– standard bezpieczeństwa fizycznego;

– standard bezpieczeństwa sprzętu i okablowania;

– standard konfiguracji i eksploatacji sieci.

Z uwagi na to, że standardy zawierają informacje, których ujawnienie nieuprawnionym stronom trzecim mogłoby w istotnym stopniu obniżyć poziom bezpieczeństwa informacji, są udostępnione tylko pracownikom Urzędu wykonującym zadania określone w standardach.

Przedmiot poszczególnych standardów:

1) standard bezpieczeństwa fizycznego: perymetr bezpieczeństwa fizycznego, kontrola fizycznych wejść, zabezpieczenie biur, pokoi i urządzeń, ochrona przed zagrożeniami zewnętrznymi i środowiskowymi, praca w obszarach zabezpieczonych, obszary ogólnie dostępne,
2) standard bezpieczeństwa sprzętu i okablowania: rozmieszczenie i ochrona sprzętu, urządzenia wspomagające, bezpieczeństwo okablowania, utrzymanie sprzętu, bezpieczeństwo sprzętu znajdującego się poza terenem organizacji, bezpieczne usuwanie sprzętu, wynoszenie majątku;
3) standard konfiguracji i eksploatacji sieci: środki kontroli przeciwko kodowi złośliwemu i mobilnemu, środki kontroli sieci, bezpieczeństwo usług sieciowych, polityki i procedury dotyczące wymiany informacji, Przesyłanie wiadomości drogą elektroniczną, Polityka korzystania z usług sieciowych, identyfikacja sprzętu w sieciach, ochrona portu służącego do zdalnego diagnozowania i konfiguracji, segregacja w sieciach, kontrola połączeń sieci, routing, nadzorowanie słabości technicznych.

10. Zarządzanie ciągłością działania

Urząd dba o zapewnienie ciągłości funkcjonowania usług związanych z przetwarzaniem danych. Celem takiego postępowania jest przeciwdziałanie przerwom w działalności oraz ochrona krytycznych procesów przed rozległymi awariami lub katastrofami. Realizacja postawionego celu możliwa jest dzięki ustanowionym praktykom i podziałowi odpowiedzialności

związanemu z zarządzeniem ciągłością działania tak, aby ograniczać do akceptowalnego poziomu skutki wypadków i awarii.

11. Polityka zarządzania zmianami

Urząd, mając na uwadze konieczność szybkiego dostosowywania się do wymagań klienta i otoczenia, ciągłe zmiany przepisów prawnych oraz dążenie do wzrostu efektywności i wydajności pracy, zapewnia metody postępowania dla skutecznej i terminowej obsługi zmian w infrastrukturze teleinformatycznej przy utrzymaniu pożądanego poziomu bezpieczeństwa przetwarzanych danych i ograniczeniu ryzyka negatywnego wpływu zmiany na obsługę teleinformatyczną organizacji.

Proces zarządzania zmianą w Urzędzie Gminy przebiega w następujących etapach:

1) ustalenie celu zmiany;
2) rozważenie wielkości i ważności zmiany dla organizacji;
3) określenie momentów krytycznych we wdrożeniu zmiany;
4) zainicjowanie zmiany, przeprowadzenie testów, wdrożenie w systemie produkcyjnym;
5) aktywne włączenie pracowników Urzędu w proces zmiany;
6) monitorowanie i raportowanie kolejnych kroków wdrożenia zmiany.

12. Polityka zarządzania kopiami zapasowymi

W Urzędzie przestrzega się poniższych zasad wykonywania kopii zapasowych, w celu zabezpieczenia danych oraz szybkiego odtworzenia pracy systemów w przypadku awarii urządzeń lub oprogramowania:

1) Za wykonanie i nadzorowania wykonania kopii zapasowej odpowiada administrator systemu z którego sporządzana jest kopia.
2) Kopia może być wykonywana przez innego pracownika (operatora) niż administrator odpowiedzialny za system (serwer), w przypadku jego nieobecności w pracy, z zachowaniem rozliczalności. Ww. operatora wyznacza bezpośredni przełożony administratora i kieruje do administratora wniosek o założenie konta z uprawnieniami do wykonywania kopii i kontrolowania ich poprawności.
3) Dostęp fizyczny do sprzętu umieszczonego w serwerowni oraz nośników, w tym nośników z kopiami zapasowymi, możliwy jest jedynie dla upoważnionych pracowników.

4) Wykorzystane nośniki kopii zapasowych muszą zostać zniszczone w sposób uniemożliwiający odtworzenie z nich danych.
5) Za wykonanie procedur odpowiadają administratorzy systemowi oraz operatorzy.

13. Polityka wymiany informacji między Urzędem a jednostkami organizacyjnymi

Urząd oraz wszystkie jednostki organizacyjne posiadają własne rozłączne zbiory danych, którymi administrują. Zbiory danych przechowywane są na rozdzielonych logicznie serwerach w serwerowniach Urzędu oraz jednostek organizacyjnych.
W celu zapewnienia bezpieczeństwa danych, pomiędzy zbiorami danych Urzędu i jednostek organizacyjnych nie występuje bezpośrednia wymiana danych, w szczególności pracownicy poszczególnych gminnych jednostek organizacyjnych i Urzędu nie mają bezpośredniego dostępu do baz danych innych jednostek.

14. Zgodność z wymaganiami prawnymi i innymi

Urząd dba o zapewnienie zgodności zasad postępowania z przepisami obowiązującego prawa, przyjętych uwarunkowań umownych i normatywnych oraz wypracowanych własnych standardów. Celem takiego postępowania jest unikanie naruszania jakichkolwiek przepisów prawnych, zobowiązań wynikających z ustaw, zarządzeń lub umów oraz wymagań bezpieczeństwa.
Realizacja postawionego celu możliwa jest dzięki ustanowionym praktykom i podziałowi odpowiedzialności związanemu z identyfikacją wymagań prawnych w zakresie bezpieczeństwa informacji. Prowadzone są audyty wewnętrzne i zewnętrzne funkcjonowania systemu.

15. Deklaracja ochrony własności intelektualnej

W Urzędzie zostały wdrożone mechanizmy zapobiegające naruszeniom przepisów prawa powszechnego związanych z ochroną własności intelektualnej. Przede wszystkim zabezpieczono stacje robocze przed możliwością instalacji oprogramowania z naruszeniem właściwej licencji, uniemożliwiono (na poziomie punktu wejścia do sieci publicznej) korzystanie z protokołów p2p. W ramach usług active directory wprowadzono filtrowanie plików użytkownika, blokując te z formatów, które nie będąc z założenia wynikającego z funkcjonalności przydatnymi

w pracy zawodowej, mogłyby zarazem być nośnikami treści naruszających prawa autorskie i pokrewne (pliki *.avi, *.mp3 i pokrewne). Prowadzona jest bieżąca ewidencja licencji oprogramowania, co zapewnia, że pracownicy upoważnieni do instalacji oprogramowania działają w granicach praw nabytych przez Urząd .
Nadzorowana jest także własność intelektualna powierzona lub przekazana przez osoby trzecie, zarówno klientów, jak i kontrahentów.

16. Postanowienia końcowe

Urząd wymaga zapoznania się pracowników z dokumentem Polityki Bezpieczeństwa Informacji oraz Instrukcją podstawowych zasad bezpieczeństwa dla pracowników Urzędu . Za złożenie przez nich stosownych oświadczeń o zapoznaniu się z instrukcją odpowiada kierownik każdej komórki organizacyjnej Urzędu . Naruszenia świadome, bądź przypadkowe niniejszej Polityki Bezpieczeństwa Informacji (wraz z wszystkimi dokumentami operacyjnymi) powoduje skutki prawne zgodnie z Regulaminem Pracy, a w przypadkach zastrzeżonych przez ustawodawcę – karne wynikające z odpowiedzialności określonej przez sąd.

Opracował: *Grzegorz Łybyk*	**Zatwierdził:** *Wójt Gminy Sanok*

Załącznik Nr 1 do „Polityki Bezpieczeństwa Informacji w Gminie Sanok"

WYKAZ ZBIORÓW DANYCH OSOBOWYCH WRAZ ZE WSKAZANIEM PROGRAMÓW ZASTOSOWANYCH DO PRZETWARZANIA TYCH DANYCH

L.p.	Nazwa zbioru danych	Nazwa programu zastosowanego do przetwarzania danych osobowych
1.	Dzierżawa i użyczenie gruntów	MS Office, ewidencja papierowa
2.	Sprzedaż nieruchomości należących do Gminy Sanok	MS Office, ewidencja papierowa
3.	Nabycie zamiana gruntów	MS Office, ewidencja papierowa
4.	Ewidencja miejscowości ulic i adresów	EMUA, ewidencja papierowa, EW MAPA
5.	Ewidencja wieczystego użytkowania gruntów	MS Office, ewidencja papierowa
6.	Gospodarka leśna w lasach mienia komunalnego	MS Office, ewidencja papierowa
7.	Komunalizacja mienia	MS Office, ewidencja papierowa
8.	Poświadczenia oświadczeń nabywców nieruchomości rolnych	MS Office, ewidencja papierowa
9.	Zgoda na wejście w teren na założenie urządzeń technicznych	MS Office, ewidencja papierowa
10.	Administrowanie łowiectwem	MS Office, ewidencja papierowa
11.	Wnioski o umorzenie opłat za wyłączenie gruntów z produkcji rolnej i leśnej	MS Office, ewidencja papierowa
12.	Użytkowanie gruntów pokrytych wodami	MS Office, ewidencja papierowa
13.	Naruszenie stosunków wodnych	MS Office, ewidencja papierowa
14.	Rozgraniczanie nieruchomości	MS Office, ewidencja papierowa
15.	Centralna ewidencja i informacja o działalności gospodarczej	portal CEiIDG, ewidencja papierowa
16.	Ewidencja bazy noclegowej	Portal GUS – ewidencja obiektów turystycznych. MS Office
17.	Ewidencja alkoholowa- sklepy bary	MS Office, ewidencja papierowa
18.	Oświadczenia majątkowe	Ewidencja papierowa
19.	Wykaz radnych	MS Office, ewidencja papierowa
20.	Dowody osobiste	SWDO
21.	Ewidencja Ludności	SELWIN
22.	Rejestr posiadaczy nieruchomości lub rzeczy ruchomych zobowiązanych do świadczeń na wypadek zagrożenia państwa	MS Office, ewidencja papierowa
23.	Rejestr osób zobowiązanych do świadczeń osobistych na rzecz obrony państwa	MS Office, ewidencja papierowa
24.	Opinie w sprawie rekultywacji gruntów rolnych	MS Office, ewidencja papierowa
25.	Kontrola umów na odbiór odpadów komunalnych	MS Office, ewidencja papierowa
26.	Wykaz dokumentów o środowisku	Ekoportal, MS Office, ewidencja papierowa
27.	Rejestr zbiorników bezodpływowych	MS Office, ewidencja papierowa
28.	Umowy adopcyjne zwierząt bezdomnych	MS Office, ewidencja papierowa
29.	Wnioski o dofinansowanie usuwania azbestu	MS Office, ewidencja papierowa
30.	Deklaracje o wysokości opłaty za gospodarowanie	BUK Softres SU, ewidencja papierowa

	odpadami komunalnymi	
31.	Utrzymywanie i eksploatacja sieci kanalizacyjnych	MS Office, ewidencja papierowa
32.	Utrzymywanie i eksploatacja sieci wodociągowych	MS Office, ewidencja papierowa
33.	Wypisy i wyrysy ze studium uwarunkowań i kierunków zagospodarowania przestrzennego	MS Office, ewidencja papierowa
34.	Wypisy i wyrysy z miejscowych planów zagospodarowania przestrzennego	MS Office, ewidencja papierowa
35.	Zaświadczenia o przeznaczeniu terenu w miejscowym planie zagospodarowania przestrzennego	MS Office, ewidencja papierowa
36.	Decyzje o warunkach zabudowy	MS Office, ewidencja papierowa
37.	Decyzje o ustaleniu lokalizacji inwestycji celu publicznego	MS Office, ewidencja papierowa
38.	Rejestr pozwoleń na budowę	
39.	Ewidencja podatkowa	BUK Softres SU, papierowa
40.	Nagrody wójta dla nauczycieli i dyrektorów szkół	MS Office, ewidencja papierowa
41.	Pracownicy obecnie zatrudnieni oraz byli pracownicy	MS Office, ewidencja papierowa
42.	Kierownicy jednostek organizacyjnych	MS Office, ewidencja papierowa
43.	Kandydaci do pracy	MS Office, ewidencja papierowa, Acrobat leader
44.	Praktykanci i stażyści	MS Office, ewidencja papierowa
45.	Wykaz osób realizujących Gminny program przeciwdziałaniu alkoholizmowi i narkomani	MS Office, ewidencja papierowa
46.	Gminna komisja rozwiązywania problemów alkoholowych	MS Office, ewidencja papierowa
47.	Wykazy członków zarządu klubów sportowych	MS Office, ewidencja papierowa
48.	Uczestnicy projektu PEFS (podsystem monitorowania europejskiego funduszu społecznego 2007)	MS Office, ewidencja papierowa
49.	Dofinansowanie kosztów kształcenia młodocianych pracowników	MS Office, ewidencja papierowa
50.	Zgoda na przejście przez gminne drogi	MS Office, ewidencja papierowa
51.	Zgoda na przyłączenie do sieci wodociągowej i kanalizacyjnej	MS Office, ewidencja papierowa
52.	Dodatki mieszkaniowe	MS Office, ewidencja papierowa
53.	Rejestr umów najmu, dzierżawy, użyczenia lokali	MS Office, ewidencja papierowa
54.	Umowy zlecenia na prace remontowe lokali	MS Office, ewidencja papierowa
55.	Zezwolenie na zajęcie pasa drogowego i uzgodnienia dotyczące lokalizacji w pasie drogowym urządzeń infrastruktury	MS Office, ewidencja papierowa
56.	Ewidencja wypadków przy pracy	Ewidencja wyłącznie papierowa
57.	Ewidencja wypadków w drodze do pracy lub z pracy	Ewidencja wyłącznie papierowa
58.	Obowiązek służby wojskowej	MS Office, ewidencja papierowa
59.	Kierowcy Ochotniczych Straży Pożarnych	MS Office, ewidencja papierowa
60.	Ewidencja korespondencji	MS Office, ewidencja papierowa

Załącznik Nr 2 do „Polityki Bezpieczeństwa Informacji w Gminie Sanok"

OPIS STRUKTURY ZBIORÓW DANYCH WSKAZUJĄCY ZAWARTOŚĆ POSZCZEGÓLNYCH PÓL INFORMACYJNYCH I POWIĄZANIA MIĘDZY NIMI

L.p.	Nazwa zbioru danych	Nazwa programu zastosowanego do przetwarzania danych osobowych
1.	Dzierżawa i użyczenie gruntów	1. Nazwiska i imiona. 2. Adres zamieszkania lub pobytu.
2.	Sprzedaż nieruchomości należących do Gminy Sanok	1. Nazwiska i imiona. 2. Adres zamieszkania lub pobytu.
3.	Nabycie zamiana gruntów	1. Nazwiska i imiona. 2. Adres zamieszkania lub pobytu.
4.	Ewidencja miejscowości ulic i adresów	1. Nazwiska i imiona. 2. Imiona rodziców. 3. Adres zamieszkania lub pobytu. 4. Numer ewidencyjny PESEL. Inne dane: numer obrębu, działki, numer księgi wieczystej.
5.	Ewidencja wieczystego użytkowania gruntów	1. Nazwiska i imiona. 2. Adres zamieszkania lub pobytu.
6.	Gospodarka leśna w lasach mienia komunalnego	1. Nazwiska i imiona. 2. Adres zamieszkania lub pobytu.
7.	Komunalizacja mienia	1. Nazwiska i imiona. 2. Adres zamieszkania lub pobytu.
8.	Stwierdzanie okresów pracy w indywidualnym gospodarstwie rolnym.	1. Nazwiska i imiona. 2. Data urodzenia. 3. Adres zamieszkania lub pobytu. 4. Miejsce pracy. 5. Seria i numer dowodu osobistego. 6. Wielkość i oznaczenie działki nieruchomości w ewidencji gruntów. 7. Rodzaj pracy wykonywanej. 8. Okres pracy w gospodarstwie rolnym. 9. Stanowisko na jakim osoba była zatrudniona. 10. Rodzaj wykonywanej pracy. 11. Charakter zatrudnienia tj. czy praca była stała, sezonowa, czy dorywcza. 12. Wymiar czasu pracy. 13. Informacja czy osoba była ubezpieczona. 14. Informacja czy osoba wnioskująca posiadała inne źródło utrzymania. 15. Stosunek pokrewieństwa lub powinowactwa świadka z osobą wnioskującą.
9.	Poświadczenia oświadczeń nabywców nieruchomości rolnych	1. Nazwiska i imiona. 2. Adres zamieszkania lub pobytu.

		3. Numer ewidencyjny PESEL. 4. Seria i numer dowodu osobistego. 5. Położenie gospodarstwa rolnego. 6. Ogólna powierzchnia gospodarstwa rolnego. 7. Powierzchnia użytków rolnych gospodarstwa rolnego.
10.	Zgoda na wejście w teren na założenie urządzeń technicznych	1. Nazwiska i imiona. 2. Adres zamieszkania lub pobytu. 3. Numer ewidencyjny PESEL. **Inne dane osobowe:** numer uprawnień zawodowych., NIP.
11.	Administrowanie łowiectwem	1. Nazwiska i imiona. 2. Adres zamieszkania lub pobytu. **Inne dane osobowe:** Nr działki, nr obrębu, nr księgi wieczystej lub innego dokumentu własności, wielkość udziału we własności, powierzchnia działki, opis użytku, oznaczenie użytku.
12.	Wnioski o umorzenie opłat za wyłączenie gruntów z produkcji rolnej i leśnej	1. Nazwiska i imiona. 2. Adres zamieszkania lub pobytu. **Inne dane osobowe:** Nr działki, nr obrębu, nr księgi wieczystej lub innego dokumentu własności, wielkość udziału we własności, powierzchnia działki, opis użytku, oznaczenie użytku.
13.	Użytkowanie gruntów pokrytych wodami	1. Nazwiska i imiona. 2. Imiona rodziców. 3. Adres zamieszkania lub pobytu. **Inne dane osobowe:** Nr działki, nr obrębu, nr księgi wieczystej lub innego dokumentu własności, wielkość udziału we własności, powierzchnia działki, opis użytku, oznaczenie użytku.
14.	Naruszenie stosunków wodnych	1. Nazwiska i imiona. 2. Imiona rodziców. 3. Adres zamieszkania lub pobytu. **Inne dane osobowe:** Nr działki, nr obrębu, nr księgi wieczystej lub innego dokumentu własności, wielkość udziału we własności, powierzchnia działki, opis użytku, oznaczenie użytku.
15.	Rozgraniczanie nieruchomości	1. Nazwiska i imiona. 2. Imiona rodziców. 3. Adres zamieszkania lub pobytu. **Inne dane osobowe:** Nr działki, nr obrębu, nr księgi wieczystej lub innego dokumentu własności, wielkość udziału we własności, powierzchnia działki, opis użytku, oznaczenie użytku.
16.	Centralna ewidencja i informacja o działalności gospodarczej	1. Nazwiska i imiona. 2. Adres zamieszkania lub pobytu. 3.Rodzaj prowadzonej działalności gospodarczej
17.	Ewidencja bazy noclegowej	1. Nazwiska i imiona. 2. Adres zamieszkania lub pobytu. 3. Rodzaj obiektu, ilość pokoi, standart
18.	Ewidencja alkoholowa- sklepy bary	1. Nazwiska i imiona. 2. Imiona rodziców. 3. Data urodzenia. 4. Adres zamieszkania lub pobytu. 5. Miejsce pracy. 6. Zawód.
19.	Oświadczenia majątkowe	1. Nazwiska i imiona. 2. Adres zamieszkania lub pobytu.
20.	Wykaz radnych	1. Nazwiska i imiona. 2. Adres zamieszkania lub pobytu.

21.	Dowody osobiste	1.Nazwiska i imiona. 2. Imiona rodziców. 3. Data urodzenia. 4. Adres zamieszkania lub pobytu. 5. Numer ewidencyjny PESEL. 6. Miejsce pracy. 7. Zawód. 8. Wykształcenie. 9. Seria i numer dowodu osobistego. **Inne dane osobowe:** nazwisko rodowe, nazwisko po zawarciu małżeństwa: mężczyzny, kobiety, dzieci, nazwiska rodowe rodziców, miejsce urodzenia, data i miejsce zawarcia małżeństwa, imiona i nazwiska świadków, płeć, stan cywilny, fotografia, karta stałego pobytu.
22.	Ewidencja Ludności	1. Nazwiska i imiona. 2. Imiona rodziców. 3. Data urodzenia. 4. Adres zamieszkania lub pobytu. 5. Numer ewidencyjny PESEL. 6. Miejsce pracy. 7. Zawód. 8. Wykształcenie. 9. Seria i numer dowodu osobistego. **Inne dane osobowe:** nazwisko: z poprzedniego małżeństwa, rodowe, imiona i nazwiska rodowe rodziców, stan cywilny, miejsce i kraj urodzenia, adres poprzedniego miejsca pobytu stałego, data zameldowania, wymeldowania (pobyt stały, czasowy), adres, stosunek do powszechnego obowiązku obrony, właściwa WKU, stopień wojskowy, numer książeczki wojskowej, seria, numer, wystawca dokumentu tożsamości , dzieci do 18-go roku życia i osoby pozostające pod prawną lub faktyczną opieką, obywatelstwo, data przekroczenia granicy, wiza: numer, rodzaj, miejsce wydania, płeć, grupa krwi RH, numer ewidencyjny ojca i matki, USC i numer aktu urodzenia, nazwisko i imię współmałżonka, numer ewidencyjny współmałżonka, data zawarcia małżeństwa, USC i numer aktu małżeństwa, data zgonu, USC i numer aktu zgonu.
23.	Rejestr posiadaczy nieruchomości lub rzeczy ruchomych zobowiązanych do świadczeń na wypadek zagrożenia państwa	1. Nazwiska i imiona. 2. Adres zamieszkania lub pobytu. 3. PESEL
24.	Rejestr osób zobowiązanych do świadczeń osobistych na rzecz obrony państwa	1. Nazwiska i imiona. 2. Adres zamieszkania lub pobytu. 3. PESEL
25.	Opinie w sprawie rekultywacji gruntów rolnych	1. Nazwiska i imiona. 2. Adres zamieszkania lub pobytu.
26.	Kontrola umów na odbiór odpadów komunalnych	1. Nazwiska i imiona. 2. Adres zamieszkania lub pobytu. 3. PESEL
27.	Wykaz dokumentów o środowisku	1. Nazwiska i imiona. 2. Imiona rodziców. 3. Adres zamieszkania lub pobytu. 4. Numer ewidencyjny PESEL. 5. NIP. 6. Seria i numer dowodu osobistego. 7. Nr telefonu.

		8. Oznaczenie działki nieruchomości w ewidencji gruntów. 9. Nr księgi wieczystej
28.	Rejestr zbiorników bezodpływowych	1. Nazwiska i imiona. 2. Adres zamieszkania lub pobytu.
29.	Umowy adopcyjne zwierząt bezdomnych	1. Nazwiska i imiona. 2. Adres zamieszkania lub pobytu.
30.	Wnioski o dofinansowanie usuwania azbestu	1. Nazwiska i imiona. 2. Adres zamieszkania lub pobytu.
31.	Deklaracje o wysokości opłaty za gospodarowanie odpadami komunalnymi	1. Nazwiska i imiona. 2. Adres zamieszkania lub pobytu. 3. PESEL
32.	Utrzymywanie i eksploatacja sieci kanalizacyjnych	1. Nazwiska i imiona. 2. Adres zamieszkania lub pobytu.
33.	Utrzymywanie i eksploatacja sieci wodociągowych	1. Nazwiska i imiona. 2. Adres zamieszkania lub pobytu.
34.	Wypisy i wyrysy ze studium uwarunkowań i kierunków zagospodarowania przestrzennego	1. Nazwiska i imiona. 2. Adres zamieszkania lub pobytu.
35.	Wypisy i wyrysy z miejscowych planów zagospodarowania przestrzennego	1. Nazwiska i imiona. 2. Adres zamieszkania lub pobytu.
36.	Zaświadczenia o przeznaczeniu terenu w miejscowym planie zagospodarowania przestrzennego	1. Nazwiska i imiona. 2. Adres zamieszkania lub pobytu.
37.	Decyzje o warunkach zabudowy	1. Nazwiska i imiona. 2. Adres zamieszkania lub pobytu.
38.	Decyzje o ustaleniu lokalizacji inwestycji celu publicznego	1. Nazwiska i imiona. 2. Adres zamieszkania lub pobytu.
39.	Rejestr pozwoleń na budowę	1. Nazwiska i imiona. 2. Imiona rodziców. 3. Data urodzenia. 4. Miejsce urodzenia. 5. Adres zamieszkania lub pobytu. 6. Miejsce pracy. 7. Zawód.
40.	Ewidencja podatkowa	1. Nazwiska i imiona. 2. Imiona rodziców. 3. Data urodzenia. 4. Adres zamieszkania lub pobytu. 5. Numer ewidencyjny PESEL. 6. Miejsce pracy. **Inne dane osobowe:** numer konta, położenie, powierzchnia użytkowa nieruchomości, nr rejestracyjny pojazdu.
41.	Nagrody wójta dla nauczycieli i dyrektorów szkół	1. Nazwiska i imiona. 2. Adres zamieszkania lub pobytu.
42.	Pracownicy obecnie zatrudnieni oraz byli pracownicy	**1. Pracownik:** rejestracja danych z kwestionariusza osobowego tj. jednostka, PESEL, NIP, płeć, imiona, nazwisko, nazwisko rodowe, data urodzenia, miejsce urodzenia, obywatelstwo, imię ojca i matki, nazwisko rodowe matki, wykształcenie, tytuł, adres – poczta, miejscowość, kod, ulica, nr domu i lokalu, kwalifikacje – nazwa szkoły, kierunek, wydział, specjalność, rok ukończenia, języki – stopień znajomości, kwalifikacje dodatkowe, rodzina, imię i nazwisko, data urodzenia, płeć, pokrewieństwo. **2. Zatrudnianie:** data przyjęcia, sposób przyjęcia, typ umowy, stanowisko, zawód, jednostka organizacyjna, wymiar etatu, kategoria zaszeregowania i wysokość wynagrodzenia zasadniczego, wysokość premii, wysokość dodatku funkcyjnego i specjalnego.

		3. Przebieg pracy w innych zakładach: nazwa zakładu pracy, adres zakładu, stanowisko, sposób rozwiązania stosunku pracy, okres zatrudnienia zaliczany do: stażowego, jubileuszu, emerytury, urlopu, stażu w urzędzie liczony w latach, miesiącach i dniach, okres zatrudnienia od-do, wyłączenia ze stażu liczone w latach, miesiącach i dniach . **4. Uprawnienia urlopowe i stażowe:** obliczanie stażu: lata szkoły, lata pracy, wymiar urlopu, wymiar urlopu wypoczynkowego, wymiar urlopu szkolnego, ilość dni urlopu zaległego, pozostała do wykorzystania ilość dni urlopu, staże: do dodatku stażowego, procent stażowego, do jubileuszu, do emerytury staż w urzędzie, staż na stanowisku, liczone w latach oraz data zmiany, chorobowe: wykorzystane dni chorobowego, urlopu okolicznościowego- opieki nad dzieckiem, opieki nad chorym, staż pracy pracownika, jubileusz, staż w urzędzie, liczone w latach, miesiącach i dniach. **5. Nieobecności:** absencje pracowników od do (dzień, miesiąc, rok). **6. Badania lekarskie:** rodzaj badania, data badania, data ważności. **7. Dane do ZUS** – dane do ubezpieczenia społecznego i zdrowotnego: sposób zatrudnienia pracownika, uprawnienia do emerytury, nr renty/emerytury, stopień niepełnosprawności, data przystąpienia do NFZ, wykształcenie.
43.	Kandydaci do pracy	1. Nazwiska i imiona. 2. Data urodzenia. 3. Adres zamieszkania. 4. Numer ewidencyjny PESEL . 5. NIP. 6. Seria i numer dowodu osobistego. 7. Wykształcenie
44.	Praktykanci i stażyści	1. Imię i nazwisko. 2. Numer ewidencyjny PESEL, NIP . 4. Kierunek studiów. 5. Nazwa i adres uczelni..
45.	Wykaz osób realizujących Gminny program przeciwdziałaniu alkoholizmowi i narkomani	1. Nazwiska i imiona. 2. Data urodzenia. 3. Adres zamieszkania. 4. Numer ewidencyjny PESEL . 5. NIP. 6. Seria i numer dowodu osobistego.
46.	Gminna komisja rozwiązywania problemów alkoholowych	1. Nazwiska i imiona. 2. Data urodzenia. 3. Adres zamieszkania. 4. Numer ewidencyjny PESEL . 5. NIP. 6. Seria i numer dowodu osobistego.
47.	Wykazy członków zarządu klubów sportowych	1. Nazwiska i imiona. 2. Data urodzenia. 3. Miejsce urodzenia. 4. Adres zamieszkania lub pobytu.
48.	Uczestnicy projektu PEFS (podsystem monitorowania europejskiego funduszu społecznego 2007)	1. Nazwiska i imiona. 2.PESEL 2. Data urodzenia. 3. Miejsce urodzenia. 4. Adres zamieszkania lub pobytu.
49.	Dofinansowanie kosztów kształcenia młodocianych pracowników	1. Nazwiska i imiona. 2.PESEL 2. Data urodzenia. 3. Miejsce urodzenia.

		4. Adres zamieszkania lub pobytu.
50.	Zgoda na przejście przez gminne drogi	1. Nazwiska i imiona. 2. Adres zamieszkania lub pobytu.
51.	Zgoda na przyłączenie do sieci wodociągowej i kanalizacyjnej	1. Nazwiska i imiona. 2. Adres zamieszkania lub pobytu.
52.	Dodatki mieszkaniowe	1. Nazwiska i imiona. 2. Imiona rodziców. 3. Data urodzenia. 4. Miejsce urodzenia. 5. Adres zamieszkania lub pobytu. 6. Numer ewidencyjny PESEL. 7. NIP. 8. Miejsce pracy. 9. Zawód. 10. Wykształcenie. 11. Seria i numer dowodu osobistego. 12. Numer telefonu. **Inne dane osobowe:** numer rachunku bankowego, deklaracja i zaświadczenia o dochodach.
53.	Rejestr umów najmu, dzierżawy, użyczenia lokali	1. Nazwiska i imiona. 2. Adres zamieszkania lub pobytu. 3. Numer ewidencyjny PESEL 4. NIP. 5. Miejsce pracy. 6. Seria i numer dowodu osobistego. **Inne dane osobowe:** nazwa firmy prowadzonej przez najemcę lokalu. liczba osób uprawnionych, dane charakteryzujące warunki mieszkaniowe, wielkość dochodów.
54.	Umowy zlecenia na prace remontowe lokali	1. Nazwiska i imiona. 2. Adres zamieszkania lub pobytu. 3. PESEL
55.	Zezwolenie na zajęcie pasa drogowego i uzgodnienia dotyczące lokalizacji w pasie drogowym urządzeń infrastruktury	1. Nazwiska i imiona. 2. Adres zamieszkania lub pobytu. 3. PESEL
56.	Ewidencja wypadków przy pracy	1. Nazwiska i imiona. 2. Imiona rodziców. 3. Data urodzenia. 4. Miejsce urodzenia. 5. Adres zamieszkania lub pobytu. 6. Numer ewidencyjny PESEL. 7. NIP. 8. Miejsce pracy. 9. Zawód. 10. Seria i numer dowodu osobistego.
57.	Ewidencja wypadków w drodze do pracy lub z pracy	1. Nazwiska i imiona. 2. Imiona rodziców. 3. Data urodzenia. 4. Miejsce urodzenia. 5. Adres zamieszkania lub pobytu. 6. Numer ewidencyjny PESEL. 7. NIP. 8. Miejsce pracy. 9. Zawód. 10. Seria i numer dowodu osobistego.

58.	Obowiązek służby wojskowej	1. Nazwiska i imiona. 2. Imiona rodziców. 3. Data urodzenia. 4. Miejsce urodzenia. 5. Adres zamieszkania lub pobytu. 6. Numer ewidencyjny PESEL. 7. Seria i numer dowodu osobistego. **Inne dane osobowe:** numer i seria książeczki wojskowej, przynależność do WKU, kategoria zdrowia.
59.	Kierowcy Ochotniczych Straży Pożarnych	1. Nazwiska i imiona. 2. Data urodzenia. 3. Miejsce urodzenia. 4. Adres zamieszkania lub pobytu. 5. PESEL 6. Miejsce pracy.
60.	Ewidencja Korespondencji	1. Nazwiska i imiona. 2. Adres zamieszkania lub pobytu.

Załącznik Nr 3 do „Polityki Bezpieczeństwa Informacji w Gminie Sanok"

Wykaz pomieszczeń, w których przetwarzane są dane osobowe

Budynek – Urząd Gminy Sanok, ul. Kościuszki 23, 38-500 Sanok

Lp.	Numer pomieszczenia	Piętro	Referat / komórka organizacyjna
1	108, 109	I	Referat Rolnictwa Leśnictwa i Gospodarki Gruntami
2	103, 107	I	Referat Ochrony Środowiska
3	203	II	Sekretariat
4	203, 204, 205, 206	II	Księgowość
5	207, 208	II	Referat Administracyjny
6	210	II	Skarbnik
7	210, 212	II	Księgowość / podatki
8	301, 306, 312	III	Referat Administracyjny
9	308	III	Referat Gospodarki Komunalnej i Inwestycji
10	404	IV	Informatyk
11	401, 406, 411, 412	IV	Referat Gospodarki Komunalnej i Inwestycji

Załącznik Nr 4 do „Polityki Bezpieczeństwa Informacji w Gminie Sanok"

Sanok, ...

Administrator Bezpieczeństwa Informacji
Biuro Bezpieczeństwa Informacji
w/m

w n i o s k u j ę o udzielenie

Pani /Panu/ .....**

upoważnienia do przetwarzania danych osobowych w:

.....
(nazwa jednostki organizacyjnej Urzędu, nazwa komisji, itp.)

z powodu: /przyjęcia do pracy, przejścia na inne stanowisko, zmiany zakresu czynności/* lub innego (jakiego?): ....

Upoważnienie dotyczy:

1. **Nazwa: / zbioru danych osobowych, zbioru danych osobowych tworzonych doraźnie w celach technicznych, rodzaju spraw związanych z przetwarzaniem danych osobowych poza zbiorem w systemach informatycznych w celach edycji/***
   .....
   .....
   .....
   .....
2. **Zakres uprawnień:** .....
   .....
   .....
3. **Sposób przetwarzania danych osobowych:** papierowy/ w systemie informatycznym/*
4. **Miejsce przetwarzania danych osobowych** (adres siedziby, piętro, nr pokoju)
   .....

.....
(pieczątka i podpis kierownika jednostki organizacyjnej urzędu, lub jego przełożonego)

/* właściwe podkreślić
/** właściwe skreślić

Załącznik Nr 5 do „Polityki Bezpieczeństwa Informacji w Gminie Sanok"

Sanok, dnia .....

U P O W A Ż N I E N I E

NR .....

na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2002 r. Nr 101 poz. 926 z późniejszymi zmianami)

upoważniam

Panią/ Pana* .....

do przetwarzania danych osobowych

w ramach

.....

(nazwa zbioru danych osobowych, nazwa zbioru tworzonego doraźnie do celów technicznych, nazwa rodzaju spraw związanych z przetwarzaniem danych osobowych poza zbiorem w systemach informatycznych w celu edycji/**)

Przetwarzanie danych osobowych może odbywać się przy wykorzystaniu: .....

.....

(systemu informatycznego, systemu w postaci papierowej)

w zakresie

.....

.....

(nazwa uprawnień w zakresie przetwarzania danych)

Upoważnienie jest ważne w czasie zatrudnienia użytkownika u Administratora lub do zmiany zakresu obowiązków użytkownika, lub do ustania realizacji zadań z których wynika brak potrzeby przetwarzania danych osobowych w zbiorze lub zakresie określonym upoważnieniem.

.....

(Administrator Danych Osobowych)

/* niepotrzebne skreślić
/ właściwe podkreślić**

Załącznik nr 2 do Zarządzenia
Wójta Gminy Sanok

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM URZĘDU GMINY W SANOKU

Opracował: Grzegorz Łybyk

Zatwierdził:

maj 2013

I. Podstawa prawna.

ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz.U. z 2002 r. Nr 101, poz. 926 z późn. zm.) oraz 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 z późn. zm.)

II. Przepisy ogólne.

1. Instrukcja zarządzania systemem informatycznym w Urzędzie Gminy zwana dalej instrukcją, opisuje sposoby nadawania uprawnień użytkownikom, określa sposób pracy w systemie informatycznym, procedury zarządzania oraz czynności mające wpływ na zapewnienie bezpieczeństwa systemu informatycznego Urzędu Gminy
2. Niniejsza instrukcja realizuje „Politykę bezpieczeństwa systemu informatycznego" obowiązującą w Urzędzie Gminy w Sanoku

III. Definicje.

1. Ilekroć w niniejszym dokumencie jest mowa o:
   a) Urzędzie – należy przez to rozumieć Urząd Gminy
   b) Administratorze Danych – należy przez to rozumieć Wójta Gminy ,
   c) Administratorze Bezpieczeństwa Informacji – należy przez to rozumieć wyznaczonego pracownika do nadzorowania przestrzegania zasad ochrony danych osobowych ustanowionego zgodnie z Polityką bezpieczeństwa przetwarzania danych osobowych Urzędu,
   d) Administratorze Systemu Informatycznego – należy przez to rozumieć osobę odpowiedzialną za funkcjonowanie systemu informatycznego Urzędu oraz stosowanie technicznych i organizacyjnych środków ochrony,
   e) użytkowniku systemu – należy przez to rozumieć osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym Urzędu.
   f) sieci lokalnej – należy przez to rozumieć połączenie systemów informatycznych Urzędu wyłącznie dla własnych potrzeb przy wykorzystaniu urządzeń i sieci telekomunikacyjnych,
   g) sieci rozległej – należy przez to rozumieć sieć publiczną w rozumieniu ustawy z dnia 21 lipca 2000r. – Prawo telekomunikacyjne (Dz. U. Nr 73, poz. 852, z późn. zm.)
2. W Urzędzie Gminy Sanok funkcję Administratora Systemu Informatycznego pełni Administrator Bezpieczeństwa Informacji

IV. Procedury nadawania i zmiany uprawnień do przetwarzania danych.

1. Każdy użytkownik systemu przed przystąpieniem do przetwarzania danych osobowych musi zapoznać się z: Ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 Nr 101, poz. 926 z późn.zm.), Polityką bezpieczeństwa przetwarzania danych

osobowych systemu informatycznego, niniejszym dokumentem, oraz posiadać upoważnienie do przetwarzania danych osobowych.

2. Zapoznanie się z powyższymi informacjami pracownik potwierdza własnoręcznym podpisem na oświadczeniu, którego wzór stanowi załącznik nr 1.
3. Administrator Systemu Informatycznego przyznaje uprawnienia w zakresie dostępu do systemu informatycznego na podstawie pisemnego upoważnienia (wniosku) określającego zakres uprawnień pracownika, którego wzór stanowi załącznik nr 2, z wyłączeniem osób kierujących Urzędem.
4. 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.
5. Hasło ustanowione podczas przyznawania uprawnień przez Administratora Systemu Informatycznego należy zmienić na indywidualne podczas pierwszego logowania się w systemie.
6. Pracownik ma prawo do wykonywania tylko tych czynności, do których został upoważniony.
7. Pracownik ponosi odpowiedzialność za wszystkie operacje wykonane przy użyciu jego identyfikatora i hasła dostępu.
8. W systemie informatycznym stosuje się uwierzytelnianie dwustopniowe: na poziomie dostępu do sieci lokalnej oraz dostępu do aplikacji.
9. Identyfikator użytkownika w aplikacji (o ile działanie aplikacji na to pozwala), powinien być tożsamy z tym, jaki jest mu przydzielany w sieci lokalnej.
10. Odebranie uprawnień pracownikowi następuje na pisemny wniosek przełożonego, któremu pracownik podlega z podaniem daty oraz przyczyny odebrania uprawnień.
11. Kierownicy komórek organizacyjnych zobowiązani są pisemnie informować Administratora o każdej zmianie dotyczącej podległych pracowników mającej wpływ na zakres posiadanych uprawnień w systemie informatycznym.
12. 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.
13. Administrator Systemu Informatycznego zobowiązany jest do prowadzenia ewidencji osób upoważnionych do przetwarzania danych osobowych który stanowi załącznik nr 3.

V. Zasady posługiwania się hasłami.

1. Bezpośredni dostęp do systemu informatycznego może mieć miejsce wyłącznie po podaniu identyfikatora i właściwego hasła.
2. Hasło użytkownika powinno być zmieniane co najmniej raz w miesiącu.
3. Identyfikator użytkownika nie powinien być zmieniany bez wyraźnej przyczyny, a po wyrejestrowaniu użytkownika z systemu informatycznego nie powinien być przydzielany innej osobie.
4. Pracownicy są odpowiedzialni za zachowanie poufności swoich haseł.
5. Hasła użytkownika utrzymuje się w tajemnicy również po upływie ich ważności.
6. Hasło należy wprowadzać w sposób, który uniemożliwia innym osobom jego poznanie.
7. W sytuacji, kiedy zachodzi podejrzenie, że ktoś poznał hasło w sposób nieuprawniony, pracownik zobowiązany jest do natychmiastowej zmiany hasła.
8. Przy wyborze hasła obowiązują następujące zasady: minimalna długość hasła - 6 znaków,
9. **zakazuje się stosować haseł:**

a) które użytkownik stosował uprzednio w okresie minionego roku, swojej nazwy użytkownika w jakiejkolwiek formie (pisanej dużymi literami, w odwrotnym porządku, dublując każdą literę, itp.), swojego imienia,
b) drugiego imienia, nazwiska, przezwiska, pseudonimu w jakiejkolwiek formie, imion (w szczególności imion osób z najbliższej rodziny), 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. wyrazów słownikowych, przewidywalnych sekwencji znaków z klawiatury np.: QWERTY","12345678",itp.

10. **należy stosować**:
    a) hasła zwierające kombinacje liter i cyfr,
    b) hasła zawierające znaki specjalne: znaki interpunkcyjne, nawiasy, symbole @, #, &, itp. o ile system informatyczny na to pozwala, hasła, które można zapamiętać bez zapisywania,
    c) hasła łatwe i szybkie do wprowadzenia, po to by trudniej było podejrzeć je osobom trzecim,
    d) Zmiany hasła nie wolno zlecać innym osobom.
    e) W systemach, które umożliwiają opcję zapamiętania nazw użytkownika lub jego hasła nie należy korzystać z tego ułatwienia.
    f) Hasło użytkownika o prawach administratora powinno znajdować się w zalakowanej kopercie w zamykanej na klucz szafie metalowej, do której dostęp mają: Administrator Bezpieczeństwa Informacji, Wójt, Sekretarz lub inna upoważniona osoba.

VI. Procedury rozpoczęcia, zawieszenia i zakończenia pracy w systemie.

1. Przed rozpoczęciem pracy w systemie komputerowym należy zameldować się do systemu przy użyciu indywidualnego identyfikatora oraz hasła.
2. Przy opuszczeniu stanowiska pracy na odległość uniemożliwiającą jego obserwację należy wykonać opcję wymeldowania z systemu (zablokowania dostępu), lub jeżeli taka możliwość nie istnieje wyjść z programu.
3. Osoba udostępniająca stanowisko komputerowe innemu upoważnionemu pracownikowi zobowiązana jest wykonać funkcję wymeldowania z systemu.
4. Przed wyłączeniem komputera należy bezwzględnie zakończyć pracę uruchomionych programów, wykonać zamknięcie systemu i jeżeli jest to konieczne wymeldować się z sieci komputerowej
5. Niedopuszczalne jest wyłączanie komputera przed zamknięciem oprogramowania oraz zakończeniem pracy w sieci.

VII. Procedury tworzenia zabezpieczeń.

A. Za systematyczne przygotowanie kopii bezpieczeństwa odpowiada Administrator Systemu Informatycznego.
B. Kopie bezpieczeństwa wykonywane są codzienne po zakończeniu pracy wszystkich użytkowników w sieci komputerowej.
C. Kopie bezpieczeństwa wykonywane są na Serwerze Backupowym oraz dodatkowo na innym nośniku,
D. W każdy piątek kopia bezpieczeństwa jest nagrywana na płytę DVD.
E. Dodatkowe zabezpieczenie wszystkich programów i danych wykonywane jest w pierwszym dniu każdego miesiąca w postaci zapisu na płytach CD-R, DVD-R lub innych nośnikach

VIII. Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz wydruków.

A. Elektroniczne nośniki informacji.

1. Dane osobowe w postaci elektronicznej - za wyjątkiem kopii bezpieczeństwa - zapisane na dyskietkach, dyskach magnetooptycznych czy dyskach twardych nie są wynoszone poza siedzibę Urzędu.
2. Wymienne elektroniczne nośniki informacji są przechowywane w pokojach stanowiących obszar przetwarzania danych osobowych, określony w Polityce bezpieczeństwa przetwarzania danych osobowych.
3. Po zakończeniu pracy przez użytkowników systemu, wymienne elektroniczne nośniki informacji są przechowywane w zamykanych szafach biurowych lub kasetkach.
4. Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do likwidacji, pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie.
5. Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do przekazania innemu podmiotowi, nieuprawnionemu do otrzymywania danych osobowych pozbawia się wcześniej zapisu tych danych.
6. Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do naprawy, pozbawia się przed naprawą zapisu tych danych albo naprawia sieje pod nadzorem osoby upoważnionej.

B. Kopie zapasowe.

1. Kopie bezpieczeństwa są przechowywane w szafie metalowej w pokoju 207 w budynku Urzędu.
2. Dostęp do danych opisanych w punkcie 1 ma Administrator Systemu Informatycznego oraz upoważnieni pracownicy.

C. Wydruki.

1. W przypadku konieczności przechowywania wydruków zawierających dane osobowe należy je przechowywać w miejscu uniemożliwiającym bezpośredni dostęp osobom niepowołanym.
2. Pomieszczenie, w którym przechowywane są wydruki robocze musi być należycie zabezpieczone po godzinach pracy.
3. Wydruki, które zawierają dane osobowe i są przeznaczone do usunięcia, należy zniszczyć w stopniu uniemożliwiającym ich odczytanie.

IX. Środki ochrony systemu przed złośliwym oprogramowaniem i wirusami komputerowymi.

1. Na każdym stanowisku komputerowym musi być zainstalowane oprogramowanie antywirusowe pracujące w trybie monitora.
2. Każdy e-mail wpływający do Urzędu musi być sprawdzony pod kątem występowania wirusów przez bramę antywirusową.
3. Definicje wzorców wirusów aktualizowane są nie rzadziej niż raz w miesiącu.
4. Zabrania się używania nośników niewiadomego pochodzenia bez wcześniejszego sprawdzenia ich programem antywirusowym. Sprawdzenia dokonuje użytkownik, który nośnik zamierza użyć.
5. Zabrania się pobierania z Internetu plików niewiadomego pochodzenia. Każdy plik pobrany z Internetu musi być sprawdzony programem antywirusowym. Sprawdzenia dokonuje użytkownik, który pobrał plik.
6. Zabrania się odczytywania załączników poczty elektronicznej bez wcześniejszego sprawdzenia ich programem antywirusowym. Sprawdzenia dokonuje pracownik, który pocztę otrzymał.
7. Administrator Systemu Informatycznego przeprowadza cykliczne kontrole antywirusowe na wszystkich komputerach ***-minimum co trzy miesiące***.
8. Kontrola antywirusowa przeprowadzana jest również na wybranym komputerze w przypadku zgłoszenia nieprawidłowości w funkcjonowaniu sprzętu komputerowego lub oprogramowania.
9. W przypadku wykrycia wirusów komputerowych sprawdzane jest stanowisko komputerowe na którym wirusa wykryto oraz wszystkie posiadane przez użytkownika nośniki.

X. Zasady i sposób odnotowywania w systemie informacji o udostępnieniu danych osobowych.

1. Dane osobowe z eksploatowanych systemów mogą być udostępniane wyłącznie osobom uprawnionym.
2. Udostępnienie danych osobowych nie może być realizowane drogą telefoniczną.
3. Aplikacje wykorzystywane do obsługi baz danych osobowych powinny zapewniać odnotowanie informacji o udzielonych odbiorcom danych. Zakres informacji powinien obejmować co najmniej: dane odbiorcy, datę wydania, zakres udostępnionych danych.

XI. Procedury wykonywania przeglądów i konserwacji systemu.

A. Przeglądy i konserwacja urządzeń.

1. Przeglądy i konserwacja urządzeń wchodzących w skład systemu informatycznego powinny być wykonywane w terminach określonym przez producenta sprzętu.
2. Nieprawidłowości ujawnione w trakcie tych działań powinny być niezwłocznie usunięte, a ich przyczyny przeanalizowane. O fakcie ujawnienia nieprawidłowości należy zawiadomić Administratora Bezpieczeństwa Informacji.

B. Przegląd programów i narzędzi programowych.

1. Konserwacja baz danych przeprowadzana jest zgodnie z zaleceniami twórców poszczególnych programów.
2. Administrator Bezpieczeństwa Informacji zobowiązany jest uaktywnić mechanizm zliczania nieudanych prób zameldowania się do systemu oraz ustawić blokadę konta użytkownika po wykryciu trzech nieudanych prób, we wszystkich systemach posiadających taką funkcję.
3. Wszystkie logi opisujące pracę systemu, zameldowania i wymeldowania użytkowników oraz rejestr z systemu śledzenia wykonywanych operacji w programie należy przed usunięciem zapisać na płytę CD-R/DVD-R.

C. Rejestracja działań konserwacyjnych, awarii oraz napraw.

1. Administrator Bezpieczeństwa Informacji prowadzi „Dziennik systemu informatycznego Urzędu Gminy". Wzór i zakres informacji rejestrowanych w dzienniku określony jest w Załączniku Nr 4.
2. Wpisów do dziennika może dokonywać Administrator Danych, Administrator Bezpieczeństwa Informacji lub osoby przez nich wyznaczone.

XII. Połączenie do sieci Internet.

Połączenie lokalnej sieci komputerowej Urzędu z Internetem jest dopuszczalne wyłącznie po zainstalowaniu mechanizmów ochronnych (firewal) oraz oprogramowania antywirusowego.

XIII. Zasilanie systemów informatycznych

W budynku Urzędu gminy istnieje dedykowana elektryczna instalacja zasilająca przeznaczona do zasilania wyłącznie sprzętu komputerowego. Wydzielona sieć elektryczna jest zabezpieczona zasilaczem UPS chroniącym przed brakiem/spadkami napięcie elektrycznego. Dodatkowo gniazda odbiorcze (DATA) są zaopatrzone w klucze pozwalające na podłączenie tylko dedykowanych urządzeń.

Załącznik nr 1
do Instrukcji Zarządzania
Systemem Informatycznym

Sanok, dn. .....

.....
(nazwisko i imię)

.....
(stanowisko)

OŚWIADCZENIE

Oświadczam, że zapoznałam(em) się z przepisami dotyczącymi ochrony danych osobowych i zobowiązuję się do przestrzegania:

1. Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jedn. Dz. U. z 2002 r. Nr 101 poz. 926 z późniejszymi zmianami).
2. Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie określenia podstawowych 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. Polityki bezpieczeństwa informacji dotyczącej sposobu przetwarzania danych osobowych w Urzędzie Gminy w Sanoku.
4. Instrukcji zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych w Urzędzie Gminy w Sanoku.

Jednocześnie w czasie wykonywania swoich obowiązków służbowych zobowiązuję się do:

a) zapewnienia ochrony danych osobowych przetwarzanych w Urzędzie Gminy w Sanoku, a w szczególności zapewnienia ich bezpieczeństwa przed udostępnianiem osobom nieuprawnionym, zabraniem, uszkodzeniem oraz nieuprawnioną modyfikacją lub zniszczeniem,
b) zachowania w tajemnicy, także po ustaniu stosunku pracy, wszelkich informacji dotyczących ochrony fizycznej, technicznej i organizacyjnej danych osobowych, funkcjonowania systemów i urządzeń służących do przetwarzania danych osobowych w Urzędzie Gminy w Sanoku,
c) zachowania w tajemnicy hasła dostępu do systemów informatycznych, przetwarzających dane osobowe w Urzędzie Gminy w Sanoku, również po upływie jego ważności,
d) natychmiastowego zgłaszania przełożonemu i Administratorowi Bezpieczeństwa Informacji stwierdzenia na swoim stanowisku pracy próby lub faktu naruszenia zabezpieczenia fizycznego pomieszczenia, bezpieczeństwa danych osobowych lub systemu informatycznego, w którym przetwarzane są dane osobowe.

.....
(podpis pracownika)

Sanok, dnia .....

Załącznik nr 2
do Instrukcji Zarządzania
Systemem Informatycznym

WNIOSEK
O NADANIE UPRAWNIEŃ W SYSTEMIE INFORMATYCZNYM

Nowy użytkownik		Modyfikacja uprawnień		Odebranie uprawnień w systemie informatycznym	

Imię i nazwisko użytkownika	Referat / dział
Opis zakresu uprawnień użytkownika w systemie informatycznym	
Data wystawienia	Podpis bezpośredniego przełożonego użytkownika systemu
	Akceptacja Administratora Bezpieczeństwa Informacji

Załącznik nr 3
do Instrukcji Zarządzania
Systemem Informatycznym

EWIDENCJA OSÓB
UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

L.p.	Imię i nazwisko	Referat	Data nadania upoważnienia	Data ustania upoważnienia	Zakres upoważnienia (czynności)	Uwagi
1	Agnieszka Haduch	Skarbnik gminy			Podatki i opłaty lokalne, dodatki mieszkaniowe, rejestr przedpoborowych, Ewidencja ludności i dowody osobiste, ewidencja korespondencji, odpady komunalne, wykaz dokumentów o środowisku, Ewidencja gruntów i budynków, System Informacji Oświatowej, Zwrot podatku akcyzowego	
2	Maria Preficz	księgowość			FK	
3	Mariola Kasprzak	SAO			Ewidencja korespondencji	
4	Iwona Chrząszcz	księgowość			FK	
5	Genowefa Węgrzyniak	księgowość			Podatki i opłaty lokalne, dodatki mieszkaniowe, rejestr przedpoborowych, Ewidencja ludności i dowody osobiste, ewidencja korespondencji, odpady komunalne, wykaz dokumentów o środowisku, Ewidencja gruntów i budynków, System Informacji Oświatowej, Zwrot podatku	

					akcyzowego	
6	Bernadeta Grządziel	księgowość			FK	
7	Irena Bereżańska	księgowość			Płace, Kadry	
8	Dorota Januszczak	księgowość			Podatki i opłaty lokalne	
9	Renata Kiczorowska	księgowość			Podatki i opłaty lokalne	
10	Zbigniew Bartkowski	Księgowość podatkowa			Podatki i opłaty lokalne, Ewidencja Gruntów i budynków	
11	Agata Wroniak	Księgowość podatkowa			Podatki i opłaty lokalne, Ewidencja Gruntów i budynków	
12	Ewa Wicińska	SAO			Ewidencja Ludności i dowody osobiste, Rejestracja Przedpoborowych	
13	Piotr Olbert	SAO			Ewidencja Ludności i dowody osobiste, Rejestracja Przedpoborowych	
14	Sabina Garbowska	SAO			Ewidencja Ludności i dowody osobiste, Rejestracja Przedpoborowych	
15	Jolanta Serwońska	SAO			Dane Kadrowe, Płacowe	
16	Bożena Wydrzyńska	GKiI			Dodatki Mieszkaniowe	
17	Anna Kata	GKiI			Decyzje o ustaleniu lokalizacji dla celu publicznego	
18	Danuta Florczak	GKiI			Decyzje o ustaleniu lokalizacji dla celu publicznego	
19	Anna Malinowska	RGG			Zwrot podatku akcyzowego	
24	Karolina Żywicka	SAO			Ewidencja korespondencji	

22	Jadwiga Gembalik	ROŚ			Odpady komunalne,	
23	Edyta Poznańska	Księgowość podatkowa			Podatki i opłaty lokalne, Ewidencja Gruntów i budynków	
24	Dariusz Mitadis	ROŚ			Odpady komunalne	
25	Iwona Hryszko	SAO - archiwista			Podatki i opłaty lokalne, dodatki mieszkaniowe, rejestr przedpoborowych, Ewidencja ludności i dowody osobiste, ewidencja korespondencji, odpady komunalne, wykaz dokumentów o środowisku, Ewidencja gruntów i budynków, System Informacji Oświatowej, Zwrot podatku akcyzowego	
26	Bogusława Kaczmarska	SAO			Ewidencja korespondencji	
27	Agnieszka Marszałek	ROŚ			Wykaz dokumentów o środowisku	
28	Iwona Marcinik	ROŚ			Wykaz dokumentów o środowisku	
29	Marzena Wróbel	ROŚ			Wykaz dokumentów o środowisku	
30						
31						
32						
33						

34						
35						
36						
37						
38						
39						
40						
41						
42						
43						

Załącznik Nr 4
do Instrukcji Zarządzania
Systemem Informatycznym

Dziennik zawiera opisy wszystkich zdarzeń istotnych dla działania systemu informatycznego w szczególności:
- w przypadku awarii- opis awarii, przyczyna awarii, szkody wynikłe na skutek awarii, sposób usunięcia awarii, wnioski,
- w przypadku konserwacji systemu- opis podjętych działań, wnioski

DZIENNIK SYSTEMU INFORMATYCZNEGO URZEDU GMINY

Lp.	Data i godzina zdarzenia	Opis zdarzenia	Podjęte działania/wnioski	Podpis