Załącznik nr 1 do Zarządzenia Nr 6/2015
Starosty Nowotomyskiego
z dnia 3.04.2015r.

POLITYKA BEZPIECZEŃSTWA SYSTEMÓW INFORMATYCZNYCH SŁUŻĄCYCH DO PRZETWARZANIA DANYCH OSOBOWYCH W STAROSTWIE POWIATOWYM W NOWYM TOMYŚLU

OPRACOWAŁ:

Administrator Bezpieczeństwa Informacji

w NOWYM TOMYŚLU.

POSTANOWIENIA OGÓLNE

§ 1. **Polityka bezpieczeństwa** została opracowana w związku z wymaganiami zawartymi w ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r. poz. 1182) oraz rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024). Dokument został opracowany zgodnie z dyrektywą 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. w sprawie przetwarzania danych osób oraz ochrony prywatności w sektorze komunikacji elektronicznej.

§ 2.1 Polityka określa tryb i zasady ochrony danych osobowych przetwarzanych w Starostwie Powiatowym w Nowym Tomyślu.

§2.2. Polityka bezpieczeństwa podlega raz w roku przeglądom w celu jej dostosowania do potrzeb i zmian występujących w otoczeniu.

§ 3. **Podstawowe definicje polityki bezpieczeństwa**

1. Bezpieczeństwo informacji – to stosowane jednoznacznie procedury, struktury organizacyjne, funkcje nazywane Polityką Bezpieczeństwa Informacji.

2. Polityka Bezpieczeństwa Informacji gwarantuje;

- poufność – właściwość polegającą, na tym, że informacja nie jest udostępniania nieupoważnionym podmiotom.
- dostępność – zapewnienie, że osoby upoważnione mają dostęp do aktywów w wymaganym terminie.
- integralność – właściwość polegająca na zapewnieniu dokładności i kompletności aktywów.

3. Bezpieczeństwo informacji wiąże się z:

- rozliczalnością działań – zapewnienie, ze wszystkie istotne czynności wykonane przy przetwarzaniu informacji zostały zarejestrowane i jest możliwe zidentyfikowanie osoby, która daną czynność wykonała,
- niezawodnością działań – zapewnienie, że wykonywane czynności prowadzą do zamierzonych skutków,
- autentycznością – zapewnienie, ze informacja jest zgodna z prawdą, oryginalna.

§ 4. Ilekroć w Polityce jest mowa o :

1) **Starostwie** – rozumie się przez to Starostwo Powiatowe w Nowym Tomyślu;
2) **zbiorze danych osobowych** - rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie;
3) **danych osobowych** - rozumie się przez to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
4) **przetwarzaniu danych** - rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych;
5) **systemie informatycznym** - rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych;
6) **systemie tradycyjnym** - rozumie się przez to zespół procedur organizacyjnych, związanych z mechanicznym przetwarzaniem informacji, wyposażenia i środków trwałych w celu przetwarzania danych osobowych na papierze;
7) **zabezpieczeniu danych w systemie informatycznym** - rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;

8) **usuwaniu danych** - rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;
9) **Administratorze Danych Osobowych (ADO)** - rozumie się Starostę Nowotomyskiego;
10) **Administratorze Bezpieczeństwa Informacji** zwanym też **ABI** rozumie się osobę wyznaczoną, nadzorującą przestrzeganie zasad ochrony danych osobowych, w szczególności zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem;
11) **Administratorze Systemu Informatycznego** zwanym też **Administratorem Systemu (ASI)** - rozumie się osobę zatrudnioną przez kierownika jednostki upoważnioną do realizacji zadań związanych z zarządzaniem systemem informatycznym;
12) **kierowniku komórki organizacyjnej –** rozumie się również samodzielne stanowisko pracy,
13) **użytkowniku systemu** zwanym też **użytkownikiem systemu informatycznego** - rozumie się przez to upoważnionego przez Starostę, wyznaczonego do przetwarzania danych osobowych w systemie informatycznym pracownika, który odbył szkolenie prowadzone przez ABI w zakresie ochrony tych danych;
14) **zgodzie osoby, której te dane dotyczą** - rozumie się przez to oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie - zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści.

Rozdział I

CELE

Zarząd Powiatu zobowiązuje się do podejmowania niezbędnych działań mających na celu zapewnienie ochrony informacji na pożądanym poziomie, a tym samym spełnienie wymaganego poziomu bezpieczeństwa systemów informacyjnych. Celem systemu jest spełnienie wymagań prawnych, zapewnienie ciągłości działania organizacji, poufności danych wrażliwych i dostępności wymaganych informacji.

§ 5. Celem Starostwa w dziedzinie bezpieczeństwa informacji jest:

1. ochrona zasobów informacyjnych oraz zapewnienie ciągłości działań procesów,
2. zapewnienie szkoleń z zakresu bezpieczeństwa informacji dla użytkowników systemu informacyjnego,
3. zapewnienie rejestracji wszelkiego rodzaju naruszeń bezpieczeństwa informacji,
4. zapewnienie, że wszelkie naruszenia bezpieczeństwa informacji oraz jego słabe punkty są raportowane i badane.

Rozdział II

Klasyfikacja informacji

§ 6. Klasyfikacja została wprowadzona w celu uporządkowania postępowania z informacją. W grupach informacji zebrane zostały dokumenty logicznie ze sobą powiązane o podobnych wymaganiach związanych z bezpieczeństwem.

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

1. informacje jawne- informacje publicznie dostępne,
2. informacje wewnętrznie dostępne – informacje dostępne dla wszystkich pracowników Starostwa,
3. informacje niejawne – informacje do których stosuje się przepisy o ochronie informacji niejawnych lub o ochronie danych osobowych.

W siedzibie Administratora Danych wydzielono strefy bezpieczeństwa, w której dostęp do informacji zabezpieczony jest wewnętrznymi środkami kontroli. W skład tej
strefy wchodzą:

Strefa IV

1) pomieszczenie z serwerem (pokój nr 3 w budynku „C" oraz pokój nr 2 w budynku „ F"), w którym mogą przebywać wyłącznie informatycy , inne osoby upoważnione do przetwarzania danych tylko w towarzystwie tych pracowników, a osoby postronne w ogóle nie mają

dostępu; zabezpieczone wejście kartą dostępu, /w pomieszczeniach serwerowni klimatyzacja /

2) pomieszczenie Wydziału Finansów z sejfem (pokój nr 1 w budynku „D", w którym mogą przebywać pracownicy tego Wydziału, inni użytkownicy danych tylko w towarzystwie tych pracowników, a osoby postronne w ogóle nie mają dostępu;

Strefa III

1. Strefa ochronna - informacje niejawne – informacje, do których stosuje się przepisy o ochronie informacji niejawnych.

Strefa I

W strefie bezpieczeństwa klasy I do danych osobowych mają dostęp wszystkie osoby upoważnione do przetwarzania danych osobowych zgodnie z zakresami upoważnień do ich przetwarzania, a osoby postronne mogą w niej przebywać tylko w obecności pracownika upoważnionego do przetwarzania danych osobowych. Strefa ta obejmuje wszystkie pozostałe pomieszczenia zaliczone do obszaru przetwarzania danych w siedzibie Administratora Danych.

§ 7. Polityka bezpieczeństwa odnosi się swoją treścią do:

- komórek organizacyjnych znajdujących odzwierciedlenie w Regulaminie Organizacyjnym Starostwa Powiatowego w Nowym Tomyślu,
- pomieszczeń, w których przetwarzane są informacje zlokalizowane w budynkach w Nowym Tomyślu przy ul. Poznańskiej 29,30,33,42,
- zasobów informacyjnych (aktywów) zaangażowanych w realizację zadań:
  1. potencjału ludzkiego – czyli wszystkich pracowników Starostwa, stażystów, praktykantów oraz inne osoby mające dostęp do informacji podlegającej ochronie,
  2. dokumentów papierowych i elektronicznych będących własnością Starostwa lub klientów Starostwa, o ile zostały przekazane na podstawie przepisów prawnych lub umów,
  3. sprzętu komputerowego oraz elektronicznych nośników informacji (np. płyty CD-R, pendrive, dyski zewnętrzne), na których znajdują się informacje podlegające ochronie.

§ 8. Celem opracowania Polityki bezpieczeństwa jest ochrona danych osobowych przed niepowołanym dostępem do zgromadzonych i przetwarzanych danych.

§ 9. Procedury i zasady określone w niniejszej Polityce bezpieczeństwa stosuje się do wszystkich pracowników Starostwa Powiatowego, jak i innych osób mających dostęp do danych osobowych przetwarzanych w Starostwie (np. osób realizujących zadania na podstawie umów zlecenia lub o dzieło, stażystów, praktykantów, serwisantów).

§ 10.1. Przetwarzanie danych osobowych do celów związanych z działalnością Administratora Danych jest zgodne z prawem w sytuacji, gdy dane te zostały uzyskane od osoby, której dotyczą i wyraziła ona na ich przetwarzanie zgodę.

2. W sytuacji, gdy dane osobowe nie zostały uzyskane od osoby, której dotyczą, to ich przetwarzanie jest zgodne z prawem, gdy przepis szczególny tak stanowi.

3. Usunięcie danych nie wymaga zgody osoby, której dotyczą.

4. Ocena niezbędności przetwarzania danych do wypełnienia usprawiedliwionych celów Administratora Danych powinna być dokonywana indywidualnie w każdej sytuacji .

§ 11.1. W przypadku zbierania danych osobowych od osoby, której one dotyczą, w wypadkach przewidzianych ustawą należy poinformować tę osobę o:

1) adresie swojej siedziby i pełnej nazwie,
2) celu zbierania danych, a w szczególności o znanych w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców danych,
3) prawie dostępu do treści swoich danych oraz ich poprawiania,
4) dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej.

2. Powyższy obowiązek Administrator Danych nakłada na osoby zatrudnione przy przetwarzaniu danych osobowych.

§ 12.1. W przypadku zbierania danych osobowych nie od osoby, której one dotyczą, Administrator Danych jest obowiązany poinformować tę osobę, bezpośrednio po utrwaleniu zebranych danych, o:

1) adresie swojej siedziby i pełnej nazwie,
2) celu i zakresie zbierania danych, a w szczególności o odbiorcach lub kategoriach odbiorców danych,
3) źródle danych,
4) prawie dostępu do treści swoich danych oraz ich poprawiania,
5) prawie wniesienia pisemnego, umotywowanego żądania zaprzestania przetwarzania jej danych ze względu na jej szczególną sytuację, jeżeli nawet przetwarzanie jest niezbędne do wypełnienia usprawiedliwionych celów administratora danych, a przetwarzanie danych nie narusza praw i wolności osoby, której dane dotyczą,
6) prawie wniesienia sprzeciwu wobec przetwarzania jej danych w przypadkach, gdy przetwarzanie jest niezbędne do wypełnienia usprawiedliwionych celów administratora danych, a przetwarzanie danych nie narusza praw i wolności osoby, której dane dotyczą, gdy administrator danych zamierza je przetwarzać w celach marketingowych lub wobec przekazywania jej danych osobowych innemu administratorowi danych.

2. Powyższy obowiązek Administrator Danych nakłada na osoby zatrudnione przy przetwarzaniu danych osobowych.

§ 13. Bezpośredni nadzór nad przetwarzaniem danych osobowych sprawują Kierownicy komórek organizacyjnych.

§ 13.1 Z zasadami w Polityce bezpieczeństwa obowiązkowo są zapoznawani wszyscy użytkownicy systemów tradycyjnych i informatycznych, składając odpowiednie oświadczenie, którego wzór stanowi załącznik Nr 1 do Polityki.

2. Oświadczenie przechowywane jest w dokumentacji ABI.

3. ABI prowadzi wykaz osób, które zapoznały się z Polityką bezpieczeństwa w Starostwie.

§ 14.1. Do informacji przechowywanych w systemach tradycyjnych jak i informatycznych mają dostęp jedynie upoważnieni pracownicy Starostwa Powiatowego oraz osoby mające imienne zarejestrowane upoważnienie, które zawiera imię, nazwisko nazwę zbioru, postać zbioru, nazwę programu, identyfikator, czas na jaki zostało wydane.

Wszyscy pracownicy zobowiązani są do zachowania tych danych w tajemnicy. Dopuszczalny sposób i zakres przetwarzania danych osobowych regulują zapisy ustaw kompetencyjnych, właściwych dla komórek organizacyjnych.

2. Upoważnienie określone w ust. 1 przechowywane jest w aktach osobowych pracownika, a drugi egzemplarz w dokumentacji ABI;

3. Ewidencję osób uprawnionych do przetwarzania danych osobowych prowadzi Administrator Bezpieczeństwa Informacji;

4. Wzór ewidencji określonej w ust. 2 stanowi załącznik Nr 2 do Polityki bezpieczeństwa.

§ 15.1. Dane osobowe są chronione zgodnie z polskim prawem oraz procedurami obowiązującymi w jednostce organizacyjnej dotyczącymi bezpieczeństwa i poufności przetwarzanych danych.

2. Systemy informatyczne oraz tradycyjne, które przechowują dane osobowe, są chronione odpowiednimi środkami technicznymi.

Rozdział III
ADMINISTRACJA I ORGANIZACJA BEZPIECZEŃSTWA

§ 16.1. Za bezpieczeństwo danych osobowych przetwarzanych w systemach przetwarzania danych osobowych odpowiada Administrator Danych Osobowych (ADO).

2. Administrator danych osobowych realizuje zadania w zakresie ochrony danych osobowych, w tym zwłaszcza;

1) upoważnia poszczególne osoby do przetwarzania danych osobowych w stosownym, indywidualnie określonym zakresie;
2) wyznacza administratora bezpieczeństwa informacji oraz określa zakres jego zadań w zakresie czynności;
3) wyznacza administratora systemów informatycznych oraz określa zakres jego zadań w zakresie czynności;

4) podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia procedur bezpiecznego przetwarzania danych osobowych;
5) podejmuje decyzje o celach i środkach przetwarzania danych osobowych, zwłaszcza z uwzględnieniem zmian w obowiązującym prawie, w organizacji administratora danych oraz technik zabezpieczenia danych osobowych.

§ 17. Administrator Danych Osobowych powołuje Administratora Bezpieczeństwa Informacji, nadzorującego przestrzeganie zasad ochrony. Prowadzi on dokumentację opisującą sposób przetwarzania danych oraz środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych.

§ 18.1. Administrator Bezpieczeństwa Informacji wykonuje wszystkie prace niezbędne do efektywnego oraz bezpiecznego zarządzania systemami informatycznymi i tradycyjnymi.

2. Administrator Bezpieczeństwa Informacji jest zobowiązany do zapewnienia, poprzez zastosowanie odpowiednich środków i metod kontroli dostępu, tak by wyłącznie uprawniony użytkownik miał dostęp do systemów informatycznych i tradycyjnych.

3. Administrator Bezpieczeństwa Informacji posiada bieżącą listę osób upoważnionych do przetwarzania danych osobowych.

4. Szczegółowy zakres odpowiedzialności i obowiązków Administratora Bezpieczeństwa Informacji jest następujący:

1) zapewnianie przestrzegania przepisów o ochronie danych osobowych, w szczególności przez:

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

b) nadzorowanie opracowania i aktualizowania dokumentacji, o której mowa w art. 36 ust. 1 i 2, oraz przestrzegania zasad w niej określonych,

2) prowadzenie rejestru zbiorów danych przetwarzanych przez administratora danych, z wyjątkiem zbiorów, o których mowa w art. 43 ust. 1, zawierającego nazwę zbioru oraz informacje, o których mowa w art. 41 ust. 1 pkt 2–4a i 7.

3) nadzoruje bezpieczeństwo systemów informatycznych i tradycyjnych;
4) nadzoruje przestrzeganie przez wszystkich użytkowników stosowanie obowiązujących procedur;
5) weryfikuje listę autoryzowanych użytkowników systemów informatycznych;
6) doradza użytkownikom w zakresie bezpieczeństwa;
7) dba, aby użytkownicy mający dostęp do systemu posiadali stosowne upoważnienia oraz byli przeszkoleni w zakresie obowiązujących regulacji bezpieczeństwa, prowadzenie szkoleń i działań podnoszących poziom wiedzy;
8) prowadzi kontrolę stanu zabezpieczeń fizycznych i technicznych obszaru przetwarzania danych w zakresie bezpieczeństwa;
9) prowadzi postępowanie wyjaśniające w przypadku naruszenia ochrony danych osobowych;
10) przygotowuje wnioski pokontrolne dla Administratora Danych Osobowych,

§ 19.1. Administrator Danych Osobowych wyznacza Administratora Systemu Informatycznego (ASI), który posiada najwyższe uprawnienia w systemie informatycznym. Tylko ASI jest osobą uprawnioną do instalowania i usuwania oprogramowania systemowego i narzędziowego.

2. Administrator Systemu Informatycznego wykonuje wszystkie prace niezbędne do efektywnego oraz bezpiecznego zarządzania systemem informatycznym. Jest zobowiązany do zapewnienia, poprzez zastosowanie odpowiednich środków i metod kontroli dostępu, w taki sposób, że wyłącznie uprawniony użytkownik ma dostęp do systemów informatycznych.

3. Szczegółowy zakres odpowiedzialności i obowiązków Administratora Systemu Informatycznego jest następujący:

1) zapewnia stałą sprawność urządzeń mających wpływ na bezpieczeństwo danych;
2) odpowiada za bezpieczeństwo systemu informatycznego;

3) zobowiązuje i bieżąco kontroluje stosowanie się użytkowników do obowiązujących procedur;
4) utrzymuje i aktualizuje listę autoryzowanych użytkowników systemu informatycznego;
5) prowadzi nadzór nad przesyłaniem danych osobowych drogą teletransmisji danych;
6) przeciwdziała dostępowi osób niepowołanych do systemu informatycznego w którym przetwarzane są dane osobowe;
7) zapewnia aktualizację dokumentacji technicznej systemu;
8) prowadzi nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisywane są dane osobowe;
9) wykonuje kopie awaryjne/archiwalne /oraz nadzoruje ich przechowywanie oraz okresowo sprawdza pod kątem ich dalszej przydatności;
10) wprowadza i nadzoruje mechanizmy autoryzacji.

§ 20. Kierownicy komórek organizacyjnych obowiązani są zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednie do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinni zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

Kierownik komórki organizacyjnej odpowiada za przestrzeganie ustawy o ochronie danych oraz przepisów wewnętrznych na poszczególnych stanowiskach, a w szczególności:

1) kontroluje sposób zabezpieczenia zbiorów danych osobowych przez pracowników;
2) kontroluje sposób realizacji obowiązku udzielania informacji o jakich mowa w ustawie;
3) zgłasza ABI planowaną rejestrację nowych zbiorów oraz przygotowuje wniosek w tej sprawie;
4) wnioskuje o nadanie upoważnień do przetwarzania danych osobowych pracownikom, Wniosek zawiera imię nazwisko, nazwę zbioru oraz zakres upoważnień- wgląd, wprowadzanie, modyfikacja, usuwanie, postać zbioru – papierowa, elektroniczna, nazwę oprogramowania;

5) zgłasza potrzeby w zakresie zabezpieczenia danych osobowych w Starostwie Powiatowym;
6) w sporządzanych umowach – zleceniach zamieszcza zapis dotyczący przestrzegania przepisów dotyczących ochrony danych osobowych,
7) uczestniczy w szkoleniach organizowanych przez Starostwo z zakresu bezpieczeństwa informacji.

§ 21. Pracownicy są odpowiedzialni za realizacje zadań służbowych, a w szczególności za:

- przestrzeganie tajemnic prawnie chronionych w zakresie przez prawo przewidzianym – pracownicy nowoprzyjęci z chwilą przyjęcia do pracy, natomiast pracownicy już zatrudnieni, poprzez podpisanie stosownych oświadczeń;
- stosowanie się do obowiązującej Polityki Bezpieczeństwa, obowiązujących procedur oraz instrukcji;
- zgłaszanie wszelkich przypadków działań niezgodnych z politykami i regulaminami, mogących być zdarzeniami lub incydentami bezpieczeństwa;
- zgłaszanie przełożonemu propozycji zmian lub uwag do opracowanego dokumentu;
- ochrona identyfikatorów osobistych (loginów do systemów/aplikacji) oraz haseł przed ujawnieniem;
- uczestnictwo w organizowanych przez Starostwo szkoleniach z zakresu bezpieczeństwa informacji;
- przeciwdziałanie próbom naruszenia informacji.

Użytkownik systemu wykonuje wszystkie prace niezbędne do efektywnej oraz bezpiecznej pracy na stanowisku pracy również z wykorzystaniem stacji roboczej. Jest odpowiedzialny przed Administratorem Bezpieczeństwa Informacji za realizację i utrzymanie niezbędnych warunków bezpieczeństwa, w szczególności do przestrzegania procedur dostępu do systemu i ochrony danych osobowych.

§ 22. Pracownik ds. Kadr na bieżąco informuje ABI o:

- zatrudnieniu określonej osoby lub przyjęciu na staż, praktykę w celu przeszkolenia w zakresie ochrony danych osobowych oraz przepisów, które obowiązują w Starostwie,
- ustaniu zatrudnienia w Urzędzie określonej osoby lub zakończeniu stażu, praktyki, celem kontroli aktywności jego kont w systemie informatycznym,
- przeniesieniu pracownika do innego wydziału Urzędu, celem kontroli jego praw do dostępu do danych osobowych.

Rozdział IV

WYKAZ POMIESZCZEŃ TWORZĄCYCH OBSZAR, W KTÓRYM PRZETWARZANE SĄ DANE OSOBOWE

§ 23.1 Pomieszczeniami tworzącymi obszar, w którym znajdują się przetwarzane dane osobowe są pomieszczenia, w których znajdują się zbiory danych w formie kartotek, rejestrów i innych oraz stacjonarny sprzęt komputerowy, w którym są przetwarzane dane osobowe.

2. Przebywanie w pomieszczeniach znajdujących się wewnątrz obszaru , o którym jest mowa w ust. 1, osób nieuprawnionych jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu tych danych.

3. Pomieszczenia, w których przetwarzane są dane osobowe powinny być zamykane na czas nieobecności w nich osób upoważnionych do przetwarzania danych osobowych.

4. Wykaz budynków i pomieszczeń w których są przetwarzane dane osobowe zawiera załącznik nr 3.

Rozdział V

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

§ 24.1 Dane osobowe są gromadzone, przechowywane i przetwarzane w kartotekach, skorowidzach, księgach, wykazach oraz w innych zbiorach ewidencyjnych poszczególnych komórek organizacyjnych jednostki organizacyjnej w postaci dokumentów

papierowych i w systemie informatycznym, w którym stosowane są pakiety biurowe lub wyspecjalizowane aplikacje (programy).

2. Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania danych zawiera załącznik nr 4. Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych przedstawia załącznik nr 5.

Rozdział VI

SPOSÓB PRZEPŁYWU DANYCH POMIĘDZY POSZCZEGÓLNYMI SYSTEMAMI.

§ 25.1 Dane z systemu „Płatnik" przesyłane są do ZUS w formie przekazu elektronicznego, w którym dane są podpisane certyfikatem kwalifikowanym.

2. System Elektronicznej Bankowości – Multi Cash PKO BP do przesyłania przelewów za pomocą klucza na dyskietce FDD 2,5" wraz z PIN oraz do wykonywania samych transakcji za pomocą specjalnie wygenerowanych haseł.

3. System Quorum - Kadry i Płace umożliwia wymianę danych z systemem Płatnik.

Moduły Płace i Kadry umożliwiają przygotowanie deklaracji zgłoszeniowych i rozliczeniowych w postaci odpowiednich plików w formacie XML, które następnie są importowane w systemie Płatnik.

Moduł Kadry umożliwia przygotowanie plików w formacie XML zawierających deklaracje zgłoszeniowe:

l ZUS ZUA, ZWUA, ZCZA, ZCNA, ZIUA, ZZA.

Moduł Płace umożliwia przygotowanie plików w formacie XML zawierających deklaracje rozliczeniowe:

l ZUS DRA, RCA, RSA, RZA.

4. System Quorum FK – finanse księgowość umożliwia eksport danych budżetowych w formie plików XML i xls do programu Bestia.

5. Program Bestia umożliwia przesyłanie w postaci plików XML informacji budżetowych do aplikacji webowej Wielkopolskiego Urzędu Wojewódzkiego – ISRB (internetowy system raportów budżetowych).

Rozdział VII

ZASADY WSPÓŁPRACY Z OSOBAMI TRZECIMI I STRONAMI ZEWNĘTRZNYMI.

§ 26.1 Administrator danych powierza dane osobowe do przetwarzania w formie usługi zewnętrznej podmiotom zewnętrznym w oparciu o umowę powierzania przetwarzania danych.

a) Podmiot zewnętrzny zobowiązany jest do przetwarzania danych zgodnie z zakresem i celem określonym w umowie przetwarzania danych osobowych. Zawierając umowy Starostwo ma na względzie, aby obejmowały one deklaracje o zachowaniu poufności oraz zobowiązania do działania zgodnie z prawem.

b) Podmiot zewnętrzny zobowiązany jest do stosowania zabezpieczeń określonych w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024).

§26.2 Bezpieczeństwo osobowe

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

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

3. Ryzyko ze strony osób, które potencjalnie mogą w łatwiejszy sposób uzyskać dostęp

do danych osobowych (np. osoby sprzątające pomieszczenia administratora danych), jest minimalizowane przez zobowiązywanie ich do zachowania tajemnicy na podstawie odrębnych, pisemnych oświadczeń.

Rozdział VIII

OPIS ZDARZEŃ NARUSZAJĄCYCH OCHRONĘ DANYCH OSOBOWYCH

§ 27.1. Podział zagrożeń:

1) zagrożenia losowe zewnętrzne (np. klęski żywiołowe, przerwy w zasilaniu), których występowanie może prowadzić do utraty integralności danych, ich zniszczenia 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), w wyniku których może dojść do zniszczenia danych, może zostać zakłócona ciągłość pracy systemu, może nastąpić naruszenie poufności danych,

3) zagrożenia zamierzone, świadome i celowe - najpoważniejsze zagrożenia powodujące naruszenie poufności danych, (zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy), zagrożenia te możemy podzielić na: nieuprawniony dostęp do systemu z zewnątrz (włamanie do systemu), nieuprawniony dostęp do systemu z jego wnętrza, nieuprawniony przekaz danych, pogorszenie jakości sprzętu i oprogramowania, 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) naruszenie lub próba naruszenia integralności systemu lub bazy danych w tym systemie,
7) próba lub modyfikacja danych lub zmiana w strukturze danych bez odpowiedniego upoważnienia (autoryzacji),
8) niedopuszczalna manipulacja danymi osobowymi w systemie,
9) ujawnienie osobom nieupoważnionym danych osobowych lub objętych 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) ujawnienia istnienia nieautoryzowanych kont dostępu do danych lub tzw. "bocznej furtki", itp.,
12) podmiana lub zniszczenie nośników z danymi osobowymi bez odpowiedniego upoważnienia lub w sposób niedozwolony skasowano lub skopiowano dane osobowe,
13) rażące naruszenie dyscypliny 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.).

3. 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 IX

ZABEZPIECZENIE DANYCH OSOBOWYCH

§ 28.1 Administrator danych osobowych jest obowiązany do zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych w systemach informatycznych Urzędu, a w szczególności:

- zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym,
- zapobiegać przed zabraniem danych przez osobę nieuprawnioną,
- zapobiegać przetwarzaniu danych z naruszeniem ustawy oraz zmianie, utracie, uszkodzeniu lub zniszczeniu tych danych.

Rozdział X

OKREŚLENIE ŚRODKÓW TECHNICZNYCH I ORGANIZACYJNYCH NIEZBĘDNYCH DLA ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZETWARZANYCH DANYCH

§ 29.1. Obieg dokumentów zawierających dane osobowe, pomiędzy komórkami organizacyjnymi jednostki, winien się odbywać w sposób zapewniający pełną ochronę przed ujawnieniem zawartych w tych dokumentach danych (informacji).

2. W CELU OCHRONY PRZED UTRATĄ DANYCH W STAROSTWIE POWIATOWYM STOSOWANE SĄ NASTĘPUJĄCE ZABEZPIECZENIA:

A. <u>Środki techniczne:</u>

- dane przetwarzane są przy użyciu stacji roboczych na serwerach sieciowych pracujących wyłącznie w wewnętrznej sieci komputerowej oddzielonej fizycznie od sieci publicznej,

- dane przetwarzane przy użyciu tradycyjnych środków pisarskich gromadzone są w rejestrach, księgach, zeszytach papierowych oraz segregatorach.

B. <u>Środki ochrony fizycznej:</u>

- pomieszczenia, w których przetwarzane są dane osobowe oraz biurka i szafy zawierające nośniki z danymi osobowymi, po godzinach pracy winny być zamykane na klucz. Klucze do biurek i szaf przechowują u siebie pracownicy, natomiast klucze do pomieszczeń przechowywane są w wyznaczonym pomieszczeniu. W przypadku konieczności opuszczenia pomieszczeń, o których mowa wyżej, w trakcie godzin pracy przez zatrudnionych w nich pracowników, pomieszczenia te należy zamykać na klucz bez pozostawienia w nich osób nieupoważnionych,
- urządzenia służące do przetwarzania danych osobowych znajdują się w pomieszczeniach zabezpieczonych zamkami patentowymi,
- dostęp do pokoi nr 3 i 3a w budynku C jest zabezpieczony antywłamaniowymi drzwiami zabezpieczonymi kontrolą dostępu na karty chipowe,
- pokój nr 3 w budynku C jest wyposażony w system klimatyzacyjny,
- dostęp do pokoju 2 w budynku F jest zabezpieczony antywłamaniowymi drzwiami zabezpieczonymi kontrolą dostępu na karty chipowe,
- okna w pokojach nr 61 i 62 w budynku B oraz w pokojach na I piętrze w budynku D są zabezpieczone szybami antywłamaniowymi,
- wejście do pomieszczeń archiwalnych w budynku B oraz D zabezpieczone są dodatkowo kratami,
- zastosowano sejf do przechowywania wymiennych nośników danych,
- w pomieszczeniu w którym znajduje się serwer zamontowano klimatyzację, zapewnia właściwą temperaturę i wilgotność powietrza dla sprzętu komputerowego,

- w pobliżu wejścia do pomieszczenia z serwerem i innymi urządzeniami znajduje się gaśnica, która okresowo jest napełniana i kontrolowana przez specjalistę,
- większość urządzeń w serwerowni umieszczona jest w szafach serwerowych i sieciowych,
- w pomieszczeniach gdzie przebywają osoby postronne monitory stanowisk dostępu do danych osobowych powinny być ustawione w taki sposób, żeby uniemożliwić tym osobom wgląd w dane,
- szczególne zabezpieczenie centrum przetwarzania danych (komputer centralny, serwerownia) poprzez zastosowanie systemu kontroli dostępu,
- wyposażenie pomieszczeń w szafy dające gwarancję bezpieczeństwa dokumentacji.
- osoba użytkująca przenośny komputer, pendrive, dyski zewnętrzne służące do przetwarzania danych osobowych, obowiązana jest zachować szczególną ostrożność podczas transportu i przechowywania tego komputera poza obszarem przewidzianym do przetwarzania, w celu zapobieżenia dostępowi do tych danych osobie niepowołanej, a w szczególności powinna:

  - zabezpieczyć dostęp do komputera hasłem,
  - nie zezwalać na używanie komputera osobom nieupoważnionym do dostępu do danych osobowych.

C. Środki sprzętowe, informatyczne i telekomunikacyjne

- zastosowano niszczarki dokumentów,
- urządzenia wchodzące w skład systemu informatycznego podłączone są do odrębnego obwodu elektrycznego, zabezpieczonego na wypadek zaniku napięcia albo awarii w sieci zasilającej,
- zastosowano sieć lokalną (Ethernet) w topologii gwiazdy,
- dane są przetwarzane w sposób scentralizowany,
- sieć lokalna podłączona do Internetu za pomocą routera,
- kopie awaryjne wykonywane są na serwerach, nośnikach taśmowych i zewnętrznych dyskach w zależności od danego serwera,

- ochrona serwerów przed zanikiem zasilania poprzez stosowanie zasilaczy zapasowych UPS.

D. Środki ochrony w ramach oprogramowania urządzeń teletransmisji

- zastosowano sprzężony firewall na styku z siecią Internet,
- zastosowano program antywirusowy na komputerach użytkowników i firewall,
- zastosowano system wykrywający obecność wirusów w poczcie elektronicznej. W efekcie zapewnione jest:
  - zabezpieczenie sieci przed atakiem z zewnątrz poprzez blokowanie wybranych portów ;
  - filtrowanie pakietów i blokowanie niektórych usług;
  - objęcie ochroną antywirusową wszystkich danych ściąganych z Internetu na stacjach lokalnych.

E. Środki ochrony w ramach oprogramowania systemu

- Konfiguracja systemu umożliwia użytkownikom końcowym dostęp do danych osobowych jedynie za pośrednictwem aplikacji,
- Zastosowano działający w „tle" program antywirusowy na komputerach użytkowników,
- W systemie operacyjnym zastosowano mechanizm wymuszający okresową zmianę haseł dostępu do systemu operacyjnego i programów sieciowych.

F. Środki ochrony w ramach narzędzi baz danych i innych narzędzi programowych

- automatycznie rejestrowany jest identyfikator użytkownika wprowadzającego dane oraz datę pierwszego wprowadzenia tych danych,
- zastosowano identyfikator i hasło dostępu do danych na poziomie aplikacji,
- dla każdego użytkownika systemu jest ustalony odrębny identyfikator,

- zdefiniowano użytkowników i ich prawa dostępu do danych osobowych na poziomie aplikacji,

- w systemie informatycznym Urzędu zastosowano autoryzację użytkownika. uruchamiając program użytkowy, podając login użytkownika i hasło.

G. Środki ochrony w ramach systemu użytkowego

- zastosowano automatyczne wygaszanie ekranu monitora w przypadku dłuższej nieaktywności użytkownika,
- komputer, z którego możliwy jest dostęp do danych osobowych zabezpieczony jest hasłem uruchomieniowym.

H. Środki organizacyjne

- wyznaczono administratora bezpieczeństwa informacji,
- tymczasowe wydruki z danymi osobowymi są po ustaniu ich przydatności zniszczone w stopniu uniemożliwiającym ich odczytanie,
- osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane są do zachowania ich w tajemnicy
- osoby upoważnione do przetwarzania danych osobowych są przed dopuszczeniem ich do tych danych szkolone w zakresie obwiązujących przepisów o ochronie danych osobowych, procedur przetwarzania danych oraz informowane o podstawowych zagrożeniach związanych z przetwarzaniem danych w systemie informatycznym
- przeszkolenie osób upoważnionych w zakresie bezpiecznej obsługi urządzeń i programów związanych z przetwarzaniem i ochroną danych osobowych,
- 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,
- prowadzona jest ewidencja osób upoważnionych do przetwarzaniu danych osobowych,
- ustalono instrukcję zarządzania systemem informatycznym,
- zdefiniowano procedury postępowania w sytuacji:

a) naruszenia ochrony danych osobowych,

b) słabości systemu,

c) niewłaściwego funkcjonowania oprogramowania;

- w przypadku, gdy zachodzi konieczność naprawy sprzętu poza siedzibą Starostwa, należy wymontować z niego nośniki informacji zawierające dane osobowe,
- 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
- każdy pracownik składa oświadczenie dotyczące przestrzegania przepisów o korzystaniu z legalnego oprogramowania teleinformatycznego wg wzoru stanowiącego załącznik **nr 6**.

I. Zabezpieczenia we własnym zakresie przez osobę upoważnioną do przetwarzania danych osobowych

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

1. ustawiania ekranów komputerowych tak, by osoby niepowołane nie mogły oglądać ich zawartości, a zwłaszcza nie naprzeciwko wejścia do pomieszczenia,
2. niepozostawiania bez kontroli dokumentów, nośników danych i sprzętu w hotelach i innych miejscach publicznych oraz w samochodach,
3. dbania o prawidłowość wentylacji komputerów (nie można zasłaniać kratek wentylatorów meblami, zasłonami lub stawiać komputerów tuż przy ścianie),
4. niepodłączania do listew podtrzymujących napięcie przeznaczonych dla sprzętu komputerowego innych urządzeń, szczególnie tych łatwo powodujących spięcia (np. grzejniki, czajniki, wentylatory),
5. pilnego strzeżenia akt, dyskietek, pamięci przenośnych i komputerów przenośnych, kasowania po wykorzystaniu danych na dyskach przenośnych,
6. niezapisywania hasła wymaganego do uwierzytelnienia się w systemie na papierze lub innym nośniku,

7. powstrzymywania się przez osoby upoważnione do przetwarzania danych osobowych od samodzielnej ingerencji w oprogramowanie i konfigurację powierzonego sprzętu (szczególnie komputerów przenośnych), nawet gdy z pozoru mogłoby to usprawnić pracę lub podnieść poziom bezpieczeństwa danych,
8. przestrzegania przez osoby upoważnione do przetwarzania danych osobowych swoich uprawnień w systemie, tj. właściwego korzystania z baz danych, używania tylko własnego identyfikatora i hasła oraz stosowania się do zaleceń administratora bezpieczeństwa informacji,
9. opuszczania stanowiska pracy dopiero po aktywowaniu wygaszacza ekranu lub po zablokowaniu stacji roboczej w inny sposób uniemożliwiający jego użytkowanie,
10. kopiowania tylko jednostkowych danych (pojedynczych plików). Obowiązuje zakaz robienia kopii całych zbiorów danych lub takich ich części, które nie są konieczne do wykonywania obowiązków przez pracownika. Jednostkowe dane mogą być kopiowane na nośniki magnetyczne, optyczne i inne po ich zaszyfrowaniu i przechowywane w zamkniętych na klucz szafach. Po ustaniu przydatności tych kopii dane należy trwale skasować lub fizycznie zniszczyć nośniki, na których są przechowywane,
11. udostępniania danych osobowych pocztą elektroniczną tylko w postaci zaszyfrowanej,
12. nie wynoszenia na jakichkolwiek nośnikach całych zbiorów danych oraz szerokich z nich wypisów, nawet w postaci zaszyfrowanej,
13. wykonywania kopii roboczych baz danych, aplikacji i dokumentów na stacjach roboczych przez użytkowników systemu na których pracuje się lokalnie, tak często, aby zapobiec ich utracie,
14. kończenia pracy polegającej na prawidłowym wylogowaniu się użytkownika i wyłączeniu komputera oraz odcięciu napięcia w UPS i listwie,
15. niszczenia w niszczarce lub chowania do szaf zamykanych na klucz wszelkich wydruków zawierających dane osobowe przed opuszczeniem miejsca pracy, po zakończeniu dnia pracy,

16. niepozostawiania osób postronnych w pomieszczeniu, w którym przetwarzane są dane osobowe, bez obecności osoby upoważnionej do przetwarzania danych osobowych,
17. zachowania tajemnicy danych, w tym także wobec najbliższych,
18. chowania do zamykanych na klucz szaf wszelkich akt zawierających dane osobowe przed opuszczeniem miejsca pracy, po zakończeniu dnia pracy,
19. umieszczania kluczy do szaf w ustalonym, przeznaczonym do tego miejscu po zakończeniu dnia pracy,
20. zamykania okien w razie opadów czy innych zjawisk atmosferycznych, które mogą zagrozić bezpieczeństwu danych osobowych, zwłaszcza po zakończeniu dnia pracy,
21. uszkodzone nośniki przed ich wyrzuceniem należy zniszczyć fizycznie w niszczarce służącej do niszczenia nośników.

Zabrania się powtórnego używania do sporządzania brudnopisów pism jednostronnie zadrukowanych kart, jeżeli zawierają one dane chronione. Zaleca się natomiast dwustronne drukowanie brudnopisów pism i sporządzanie dwustronnych dokumentów.

Po wykorzystaniu wydruki zawierające dane osobowe należy codziennie przed zakończeniem pracy zniszczyć w niszczarce. O ile to możliwe, nie należy przechowywać takich wydruków w czasie dnia na biurku ani też wynosić poza siedzibę Administratora Danych.

5. Niezależnie od niniejszych zasad opisanych w dokumencie „Polityka bezpieczeństwa w Starostwie Powiatowym" 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.

Rozdział XI

KONTROLA PRZESTRZEGANIA ZASAD ZABEZPIECZENIA DANYCH OSOBOWYCH

§ 30.1 Administrator danych - Starosta lub osoba przez niego wyznaczona, którą jest „Administrator Bezpieczeństwa Informacji" sprawuje nadzór nad przestrzeganiem zasad ochrony danych osobowych wynikających z ustawy o ochronie danych osobowych oraz zasad

ustanowionych w niniejszym dokumencie.

2. Administrator Bezpieczeństwa Informacji sporządza roczne plany kontroli zatwierdzone przez Administratora Danych i zgodnie z nimi przeprowadza kontrole oraz dokonuje analizy i oceny przestrzegania przepisów i stanu bezpieczeństwa danych osobowych.

3. Na podstawie zgromadzonych materiałów, o których mowa w pkt. 2, Administrator Bezpieczeństwa sporządza roczne sprawozdanie i przedstawia Administratorowi danych – Staroście Nowotomyskiemu.

ROZDZIAŁ XII

POSTĘPOWANIE W PRZYPADKU NARUSZENIA OCHRONY DANYCH OSOBOWYCH

§ 31.1. W przypadku stwierdzenia naruszenia:

- zabezpieczenia systemu informatycznego,
- technicznego stanu urządzeń,
- zawartości zbioru danych osobowych,
- ujawnienia metody pracy lub sposobu działania programu,
- jakości transmisji danych w sieci telekomunikacyjnej mogącej wskazywać na naruszenie zabezpieczeń tych danych,
- innych zdarzeń mogących mieć wpływ na naruszenie danych osobowych

(np. zalanie, pożar, itp.)

<u>każda osoba zatrudniona przy przetwarzaniu danych osobowych jest obowiązana niezwłocznie powiadomić o tym fakcie Administratora Bezpieczeństwa.</u>

2. W razie niemożliwości zawiadomienia Administratora Bezpieczeństwa lub osoby przez niego upoważnionej, należy powiadomić bezpośredniego przełożonego.

3. Do czasu przybycia na miejsce naruszenia ochrony danych osobowych Administratora Bezpieczeństwa lub upoważnionej przez niego osoby, należy:

- niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych

skutków zaistniałego naruszenia, o ile istnieje taka możliwość, a następnie uwzględnić w działaniu również ustalenie przyczyn lub sprawców,

- rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia,
- zaniechać - o ile to możliwe - dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić udokumentowanie i analizę,
- podjąć inne działania przewidziane i określone w instrukcjach technicznych i technologicznych stosownie do objawów i komunikatów towarzyszących naruszeniu,
- podjąć stosowne działania, jeśli zaistniały przypadek jest określony w dokumentacji systemu operacyjnego, dokumentacji bazy danych lub aplikacji użytkowej,
- zastosować się do innych instrukcji i regulaminów, jeżeli odnoszą się one do zaistniałego przypadku,
- udokumentować wstępnie zaistniałe naruszenie,
- nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia Administratora Bezpieczeństwa lub osoby upoważnionej.

4. Po przybyciu na miejsce naruszenia lub ujawnienia ochrony danych osobowych, Administrator Bezpieczeństwa lub osoba go zastępująca:

- zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metody dalszego postępowania mając na uwadze ewentualne zagrożenia dla prawidłowości pracy Urzędu,
- może żądać dokładnej relacji z zaistniałego naruszenia od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem,
- rozważa celowość i potrzebę powiadamia o zaistniałym naruszeniu Administratora danych,

- nawiązuje bezpośredni kontakt, jeżeli zachodzi taka potrzeba, ze specjalistami spoza Urzędu.

5. Administrator Bezpieczeństwa dokumentuje zaistniały przypadek naruszenia oraz sporządza raport wg wzoru stanowiącego załącznik **nr 7**, który powinien zawierać w szczególności:

- wskazanie osoby powiadamiającej o naruszeniu oraz innych osób zaangażowanych lub odpytanych w związku z naruszeniem,
- określenie czasu i miejsca naruszenia i powiadomienia,
- określenie okoliczności towarzyszących i rodzaju naruszenia,
- wyszczególnienie wziętych faktycznie pod uwagę przesłanek do wyboru metody postępowania i opis podjętego działania,
- wstępną ocenę przyczyn wystąpienia naruszenia,
- ocenę przeprowadzonego postępowania wyjaśniającego i naprawczego.

6. Raport, o którym mowa w pkt 5, Administrator Bezpieczeństwa niezwłocznie przekazuje Administratorowi danych, a w przypadku jego nieobecności osobie uprawnionej.
7. Po wyczerpaniu niezbędnych środków doraźnych po zaistniałym naruszeniu Administrator Bezpieczeństwa zasięga niezbędnych opinii i proponuje postępowanie naprawcze, a w tym ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń oraz terminu wznowienia przetwarzania danych.
8. Zaistniałe naruszenie może stać się przedmiotem szczegółowej, zespołowej analizy prowadzonej przez Kierownictwo urzędu, Administratora Bezpieczeństwa Informacji.
9. Analiza, o której mowa w ust. 8, powinna zawierać wszechstronną ocenę zaistniałego naruszenia, wskazanie odpowiedzialnych, wnioski co do ewentualnych przedsięwzięć proceduralnych, organizacyjnych, kadrowych i technicznych, które powinny zapobiec podobnym naruszeniom w przyszłości.

ROZDZIAŁ XIII

SZKOLENIA UŻYTKOWNIKÓW

§32.1. Każdy użytkownik przed dopuszczeniem do pracy z systemem informatycznym przetwarzającym dane osobowe lub zbiorami danych osobowych w wersji papierowej winien być poddany przeszkoleniu w zakresie ochrony danych osobowych zgodnie z nadawanym upoważnieniem.

2. Za przeprowadzenie szkolenia odpowiada ABI. Pracownik wydziału kadr ma obowiązek zawiadomienia o przyjęciu nowego pracownika, stażysty, praktykanta.

3. Zakres szkolenia powinien obejmować zaznajomienie użytkownika z przepisami ustawy o ochronie danych osobowych oraz wydanymi na jej podstawie aktami wykonawczymi oraz instrukcjami obowiązującymi u ADO, a także o zobowiązaniu się do ich przestrzegania.

4. Szkolenie zostaje zakończone podpisaniem przez słuchacza Oświadczenia o wzięciu udziału w szkoleniu i jego zrozumieniu oraz zobowiązaniu się do przestrzegania przedstawionych w trakcie szkolenia zasad ochrony danych osobowych.

Rozdział XIV

PRZEPISY KOŃCOWE

§ 33. Za naruszenie obowiązków wynikających z niniejszej Polityki Bezpieczeństwa oraz przepisów ustawy o ochronie danych osobowych może być uznane za ciężkie naruszenie obowiązków pracowniczych, podlegające sankcjom dyscyplinarnym oraz sankcjom karnym w szczególności wynikającym z przepisów tejże ustawy.

§ 34. W sprawach nie uregulowanych w niniejszej Polityce bezpieczeństwa mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r. poz. 1182, z późn. zm.) oraz rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024).

Załącznik nr 1
do Załącznika nr 1 do Zarządzenia Nr 6/2015
Starosty Nowotomyskiego
„Oświadczenie o zapoznaniu z przepisami
dotyczącymi ochrony danych osobowych„

Nowy Tomyśl, dnia .....

OŚWIADCZENIE

Oświadczam, że przed przystąpieniem do pracy przy przetwarzaniu danych osobowych zostałam/em zaznajomiona/ny z przepisami dotyczącymi ochrony danych osobowych, w tym z ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2002 r. Nr 101, poz. 926 ze zm.) oraz rozporządzeniami wykonawczymi wydanymi na jej podstawie.

Zapoznałam/em się i rozumiem zasady dotyczące ochrony danych osobowych opisane w:

- Polityce bezpieczeństwa w Starostwie Powiatowym w Nowym Tomyślu,
- Instrukcji zarządzania systemem informatycznym w Starostwie Powiatowym w Nowym Tomyślu,

a także innymi dokumentami regulującymi zasady przetwarzania danych osobowych przez Starostwo Powiatowe w Nowym Tomyślu oraz zobowiązuję się do ich przestrzegania.

W związku z:

1. ustaniem mojego zatrudnienia w Starostwie Powiatowym w Nowym Tomyślu/*
2. cofnięciem mi upoważnienia dostępu do danych osobowych w systemie/*

zobowiązuję się do zachowania w tajemnicy informacji w trakcie dokonywania operacji związanych z przetwarzaniem danych osobowych podczas mojej pracy.

.....

podpis pracownika

* - niepotrzebne skreślić

Załącznik nr 2

do Załącznika nr 1 do Zarządzenia

Nr OG. 120.6.2015

Rejestr osób i wydanych upoważnień do przetwarzania danych osobowych prowadzonych przez ABI

Lp.	Imię i nazwisko	Komórka organizacyjna stanowisko	Identyfikator użytkownika	Zakres przydzielonych uprawnień	Data przeszkolenia	Nr upoważnienia imiennego	Data nadania upoważnienia	Data ustania upoważnienia	Zakres Upoważnienia

Zakres upoważnień:

Wgląd,przeglądanie	D
wprowadzanie	W
modyfikacja	M
Usuwanie	U

Załącznik nr 3
do Załącznika do Zarządzenia
Nr OG.120.6.2015

Wykaz budynków oraz pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe.

Miejscem przetwarzania danych osobowych są pomieszczenia pracy komórek organizacyjnych Starostwa Powiatowego w Nowym Tomyślu

Lp.	Budynek	Lokalizacja	Nr Pokoju	Nazwa wydziału	Uwagi
1.	Budynek „B" ul.Poznańska 33	Parter	8	Starosta	
2.	Budynek „B" ul.Poznańska 33	Parter	6	Wicestarosta	
3.	Budynek „B" ul.Poznańska 33	Parter	10	Sekretarz	
4.	Budynek „B" ul.Poznańska 33	Parter	7	Sekretariat	
4.	Budynek „B" ul.Poznańska 33	Parter	5	Kancelaria	
5.	Budynek „B" ul.Poznańska 33	Parter	4	Wydział Organizacyjno – Gospodarczy	
6.	Budynek „B" ul.Poznańska 33	I piętro	67a	Wydział Organizacyjno – Gospodarczy	
7.	Budynek „B" ul.Poznańska 33	I piętro	67	Wydział Organizacyjno – Gospodarczy	
8.	Budynek „B" ul.Poznańska 33	I piętro	72	Radca Prawny	
9.	Budynek „B" ul.Poznańska 33	I piętro	73	Powiatowy Rzecznik Konsumentów	
10.	Budynek „B" ul.Poznańska 33	I piętro	74	Wydział Organizacyjno – Gospodarczy	
11.	Budynek „B" ul.Poznańska 33	II piętro	86	Wydział Geodezji, Kartografii, Katastru i Gospodarce Nieruchomościami	
12.	Budynek „C" ul. Poznańska 33	Parter	3	Wydział Organizacyjno – Gospodarczy	
13.	Budynek „C" ul. Poznańska 33	Parter	3a	Wydział Organizacyjno – Gospodarczy	

14.	Budynek „C" ul. Poznańska 33	Parter	17	Biuro Obsługi Mieszkańca	
15.	Budynek „C" ul. Poznańska 33	I piętro	58	Wydział Rolnictwa, Leśnictwa i Ochrony Środowiska	
16.	Budynek „C" ul. Poznańska 33	I piętro	58a	Wydział Rolnictwa, Leśnictwa i Ochrony Środowiska	
17.	Budynek „C" ul. Poznańska 33	I piętro	59	Wydział Spraw Obywatelskich i Zarządzania Kryzysowego	
18.	Budynek „C" ul. Poznańska 33	I piętro	60	Wydział Spraw Obywatelskich i Zarządzania Kryzysowego	
	Budynek „C" ul. Poznańska 33	I piętro	61	Wydział Spraw Obywatelskich i Zarządzania Kryzysowego	
19.	Budynek „C" ul. Poznańska 33	I piętro	62	Wydział Spraw Obywatelskich i Zarządzania Kryzysowego	
20.	Budynek „C" ul. Poznańska 33	I piętro	64	Wydział Rolnictwa, Leśnictwa i Ochrony Środowiska	
21.	Budynek „C" ul. Poznańska 33	I piętro	66	Wydział Rolnictwa, Leśnictwa i Ochrony Środowiska	
22.	Budynek „C" ul. Poznańska 33	II piętro	76	Wydział Budownictwa i Inwestycji	
23.	Budynek „C" ul. Poznańska 33	II piętro	77	Wydział Budownictwa i Inwestycji	
24.	Budynek „C" ul. Poznańska 33	II piętro	78	Wydział Budownictwa i Inwestycji	
25.	Budynek „C" ul. Poznańska 33	II piętro	79	Wydział Budownictwa i Inwestycji	
26.	Budynek „C" ul. Poznańska 33	II piętro	80	Wydział Geodezji, Kartografii, Katastru i Gospodarce Nieruchomościami	
27.	Budynek „C" ul. Poznańska 33	II piętro	81	Wydział Geodezji, Kartografii, Katastru i Gospodarce Nieruchomościami	

28.	Budynek „C" ul. Poznańska 33	II piętro	82	Wydział Geodezji, Kartografii, Katastru i Gospodarce Nieruchomościami	
29.	Budynek „C" ul. Poznańska 33	II piętro	83	Wydział Geodezji, Kartografii, Katastru i Gospodarce Nieruchomościami	
30.	Budynek „C" ul. Poznańska 33	II piętro	84	Zamówienia Publiczne	
31.	Budynek „ D" ul. Poznańska 29	parter	1	Wydział Finansów	
32.	Budynek „ D" ul. Poznańska 29	parter	2	Wydział Finansów	
33	Budynek „ D" ul. Poznańska 29	parter	3	Wydział Finansów	
34.	Budynek „ D" ul. Poznańska 29	parter	4	Wydział Finansów	
35.	Budynek „ D" ul. Poznańska 29	parter	5	Wydział Finansów	
36.	Budynek „ D" ul. Poznańska 29	parter	6	Wydział Finansów	
37.	Budynek „ D" ul. Poznańska 29	parter	6a	Wydział Finansów	
38.	Budynek „ D" ul. Poznańska 29	parter	7	Wydział Finansów	
39.	Budynek „ D" ul. Poznańska 29	I piętro	10	Wydział Komunikacji	
40.	Budynek „ D" ul. Poznańska 29	I piętro	11	Wydział Komunikacji	
41.	Budynek „ D" ul. Poznańska 29	I piętro	11a	Wydział Komunikacji	
42.	Budynek „ D" ul. Poznańska 29	I piętro	12	Wydział Komunikacji	
43.	Budynek „ D" ul. Poznańska 29	I piętro	13	Wydział Komunikacji	
44.	Budynek „ D" ul. Poznańska 29	I piętro	14	Wydział Komunikacji	
45.	Budynek „ D" ul. Poznańska 29	I piętro	15	Wydział Komunikacji	
46.	Budynek „ E" ul. Poznańska 30	parter	5	**Powiatowy Zespół do Spraw Orzekania o Niepełnosprawności**	
47.	Budynek „ E" ul. Poznańska 30	parter	7	**Powiatowy Zespół do Spraw Orzekania o Niepełnosprawności**	
48.	Budynek „ E" ul. Poznańska 30	parter	15	**Powiatowy Zespół do Spraw Orzekania o Niepełnosprawności**	

49.	Budynek „ E" ul. Poznańska 30	II piętro	21	Wydział Edukacji i Rozwoju	
50.	Budynek „ E" ul. Poznańska 30	II piętro	22	Wydział Edukacji i Rozwoju	
51.	Budynek „ E" ul. Poznańska 30	II piętro	23	Wydział Edukacji i Rozwoju	
52.	Budynek „ E" ul. Poznańska 30	II piętro	24	Wydział Dróg Powiatowych	
53.	Budynek „ E" ul. Poznańska 30	II piętro	25	Wydział Dróg Powiatowych	
54.	Budynek „ E" ul. Poznańska 30	II piętro	27	Wydział Edukacji i Rozwoju	
55.	Budynek „ E" ul. Poznańska 30	II piętro	28	Wydział Edukacji i Rozwoju	
56.	Budynek „ E" ul. Poznańska 30	II piętro	29	Wydział Edukacji i Rozwoju	
57.	Budynek „ E" ul. Poznańska 30	II piętro	32	Wydział Edukacji i Rozwoju	
58.	Budynek „ F" ul. Poznańska 42	parter	1	Wydział Geodezji, Kartografii, Katastru i Gospodarce Nieruchomościami Powiatowy Ośrodek Dokumentacji Geodezyjnej i Kartograficznej	
59.	Budynek „ F" ul. Poznańska 42	parter	2	Wydział Geodezji, Kartografii, Katastru i Gospodarce Nieruchomościami Powiatowy Ośrodek Dokumentacji Geodezyjnej i Kartograficznej	
60.	Budynek „ F" ul. Poznańska 42	parter	4	Wydział Geodezji, Kartografii, Katastru i Gospodarce Nieruchomościami Powiatowy Ośrodek Dokumentacji Geodezyjnej i Kartograficznej	
61.	Budynek „ F" ul. Poznańska 42	parter	5a	Wydział Geodezji, Kartografii, Katastru i Gospodarce Nieruchomościami Powiatowy Ośrodek Dokumentacji Geodezyjnej i Kartograficznej	

62.	Budynek „ F" ul. Poznańska 42	parter	5b	Wydział Geodezji, Kartografii, Katastru i Gospodarce Nieruchomościami Powiatowy Ośrodek Dokumentacji Geodezyjnej i Kartograficznej	
63.	Budynek „ F" ul. Poznańska 42	parter	5c	Wydział Geodezji, Kartografii, Katastru i Gospodarce Nieruchomościami Powiatowy Ośrodek Dokumentacji Geodezyjnej i Kartograficznej	
64.	Budynek „ F" ul. Poznańska 42	parter	7	Wydział Geodezji, Kartografii, Katastru i Gospodarce Nieruchomościami Powiatowy Ośrodek Dokumentacji Geodezyjnej i Kartograficznej	
65.	Budynek „ F" ul. Poznańska 42	parter	8	Wydział Geodezji, Kartografii, Katastru i Gospodarce Nieruchomościami Powiatowy Ośrodek Dokumentacji Geodezyjnej i Kartograficznej	
66.	Budynek „ F" ul. Poznańska 42	parter	9	Wydział Geodezji, Kartografii, Katastru i Gospodarce Nieruchomościami Powiatowy Ośrodek Dokumentacji Geodezyjnej i Kartograficznej	
67.	Budynek „ F" ul. Poznańska 42	parter	10	Wydział Geodezji, Kartografii, Katastru i Gospodarce Nieruchomościami Powiatowy Ośrodek Dokumentacji Geodezyjnej i Kartograficznej	
68.	Budynek „ F" ul. Poznańska 42	parter	11	Wydział Geodezji, Kartografii, Katastru i	

				Gospodarce Nieruchomościami Powiatowy Ośrodek Dokumentacji Geodezyjnej i Kartograficznej	
69.	Budynek „ F" ul. Poznańska 42	parter	12	Wydział Geodezji, Kartografii, Katastru i Gospodarce Nieruchomościami Powiatowy Ośrodek Dokumentacji Geodezyjnej i Kartograficznej	
70	Budynek „ B" Budynek „E"	Piwnica		Archiwum zakładowe	

Załącznik nr 4
do Załącznika nr 1 do Zarządzenia
Nr. OG.120.6.2015

Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do ich przetwarzania

Lp.	Nazwa zbioru danych	Nazwa wydziału	Budynek Nr pokoju	Rejestracja zbioru w GIODO	Nazwa programu komp.służącego do przetwarzania danych	Sposób prowadzenia	Numer księgi Rok
1.	Mienie zabużańskie	GN	B 87 ul. Poznańska 33	TAK	Microsoft Office	Forma papierowa	045217 1999
2.	Plany urządzania lasów	RŚ	C p. 59a ul. Poznańska 33	TAK	Microsoft Office	Forma papierowa Forma elektroniczna	043626 1999
3.	Ewidencja kierowców powiatu nowotomyskiego	KM	D p 12 ul. Poznańska 29	TAK	CEPIK	Forma papierowa Forma elektroniczna	049874 1999
4.	Ewidencja właścicieli pojazdów powiatu nowotomyskiego	KM	D p.11 ul. Poznańska 29	TAK	CEPIK	Forma papierowa Forma elektroniczna	049872 1999
5.	Ewidencja instruktorów nauki jazdy powiatu nowotomyskiego	KM	D P 14 ul. Poznańska 29	TAK	Portal Starosty	Forma papierowa Forma elektroniczna	049873 1999
6.	Ewidencja płatników opłat za użytkowanie	FN	D p. 8 ul. Poznańska 29	TAK	QNT – moduł F-K Systemu Quorum	Forma papierowa Forma elektroniczna	034176 1999
7.	Decyzje o zmianie imion i nazwisk	SOZK	C p. 60 ul. Poznańska 33	TAK	Microsoft Office	Forma papierowa Forma elektroniczna	1999 029062 Arch

8.	Uzgadnianie dokumentacji projektowej	GN	F p.4 ul. Poznańska 42	TAK	Zasób geodezyjno – kartograficzny	Forma papierowa Forma elektroniczna	1999 049999
9.	Przyjmowanie podań i oświadczeń o zmianie obywatelstwa	SOZK	F p. ul. Poznańska33	TAK	Microsoft Office	Forma papierowa Forma elektroniczna	029054 1999 Arch
10.	Poborowi z Powiatu Nowy Tomyśl - orzecznictwo	SOZK	C 60 ul. Poznańska 33	TAK	Microsoft Office	Forma papierowa Forma elektroniczna	030811 1999
11.	Karty wędkarskie	RŚ	C p.64 ul. Poznańska 33	TAK	Microsoft Office	Forma papierowa Forma elektroniczna	049785 1999
12.	Ewidencja gruntów i budynków	GN	C P81,82,83,86 F p.2,3,4,5,9,11 ul. Poznańska 33 ul. Poznańska 42	TAK	EGB-2000 system ewidencji gruntów i budynków	Forma papierowa Forma elektroniczna	029378 1999
13.	Sprzęt pływający do połowu ryb	RŚ	C p.64 ul. Poznańska 33	TAK	Microsoft Office	Forma papierowa Forma elektroniczna	029961 1999
14.	Gospodarowanie nieruchomościami Skarbu Państwa	GN	C p.83 ul. Poznańska33	TAK	Microsoft Office	Forma papierowa Forma elektroniczna	044688 1999
15.	Zasób geodezyjno-kartograficzny	GN	C p.80,81,82,83,86 F p.1,2,3,4,9,11 ul. Poznańska 30 ul. Poznańska 42	TAK	GEOBID	Forma papierowa Forma elektroniczna	049868 1999
16.	Rejestr ewidencja rozpoczynanych i	BI	C p. 77,78,79	TAK	Microsoft Office	Forma papierowa Forma elektroniczna	048214 1999

	oddawanych do użytkowania obiektów budowlanych		ul. Poznańska 33				
17.	Rejestr decyzji o pozwoleniu na budowę	BI	C p.77,78,79 ul. Poznańska 33	TAK	Microsoft Office	Forma papierowa Forma elektroniczna	049784 1999
18.	Ewidencja wydanych licencji i zaświadczeń na transport drogowy	KM	D p.14 ul. Poznańska 29	TAK	Foris	Forma papierowa Forma elektroniczna	2003
19.	Rejestr – spis zaświadczeń	BI	C p.78,79 ul. Poznańska 33	TAK	Microsoft Office	Forma papierowa Forma elektroniczna	073269 2007
20.	Rejestr – spis decyzji odmownych dot. decyzji pozwolenie na budowę	BI	C p.78,79 ul. Poznańska 33	TAK	Microsoft Office	Forma papierowa Forma elektroniczna	073271 2007
21.	Rejestr wniosków o pozwolenie na budowę	BI	C p.77,78,79, ul. Poznańska 33	TAK	Microsoft Office	Forma papierowa Forma elektroniczna	078395 2007
22.	Zezwolenia o dopuszczenie reproduktora do użytkowania w punkcie kopulacyjnym na podstawie ustawy o organizacji hodowli i rozrodzie zwierząt gospodarskich	RŚ	C p.58 ul. Poznańska 33	TAK	Microsoft Office	Forma papierowa Forma elektroniczna	075570 2007 Arch
23.	Rejestr dzienników budowy	BI	C p.77,78,79 ul. Poznańska 33	TAK	Microsoft Office	Forma papierowa Forma elektroniczna	073272 2007
24.	Rejestr posiadaczy zwierząt przetrzymywanych lub hodowanych na podstawie	RŚ	C 59a ul. Poznańska 33	TAK	Microsoft Office	Forma papierowa Forma elektroniczna	073690 2007

	ustawy o ochronie przyrody						
25.	Rejestr – spis zgłoszeń budów, robót budowlanych, rozbiórek	BI	C p. 78 ul. Poznańska33	TAK	Microsoft Office	Forma papierowa Forma elektroniczna	073273 2007
26.	Sprawy sądowe dotyczące uregulowania stanów prawnych	GN	C p. 80 ul. Poznańska 33	TAK	Microsoft Office	Forma papierowa Forma elektroniczna	080456 2007
27.	Wynagradzanie pracowników Starostwa Powiatowego w Nowym Tomyślu	OG	B p.67 ul. Poznańska 33 D p. 3 ul. Poznańska 29	NIE	QNT – moduł Kadry Systemu Quorum QNT – moduł Płace Systemu Quorum	Forma papierowa Forma elektroniczna	-
28.	Ewidencja dokumentów księgowych	FN	D p. 1,2,3,4,5,6,7 ul. Poznańska 29	NIE	QNT – moduł F-K Systemu Quorum	Forma papierowa Forma elektroniczna	-
29.	System kadrowy	OG	B p. 67 ul. Poznańska 33	NIE	QNT – moduł Kadry Systemu Quorum	Forma papierowa Forma elektroniczna	-
30.	Rejestr legitymacji osób niepełnosprawnych	PZON	E P5 Ul. Poznańska 30	TAK	Microsoft Office	Forma papierowa Forma elektroniczna	078847 2008
31.	Wypłata ekwiwalentu przyznanego osobom fizycznym na podstawie ustawy o wspieraniu rozwoju obszarów wiejskich	RŚ	C p.77 ul. Poznańska 33	TAK	Microsoft Office	Forma papierowa Forma elektroniczna	088806 2009
32.	Zezwolenia na przetrzymywanie zwierzyny leśnej oraz hodowanie chartów	RŚ	C p.58 ul. Poznańska 33	TAK	Microsoft Office	Forma papierowa Forma elektroniczna	079016 2009

	rasowych						
33	Spis kart informacyjnych dot. przedsięwzięć mogących znacząco oddziaływać na środowisko	RŚ	C p.59 ul. Poznańska 33	NIE	Microsoft Office	Forma papierowa Forma elektroniczna	081535 2009
34.	Oświadczenia majątkowe	SOZK OG	C p. 59 B p. 67 ul. Poznańska 33	TAK	Microsoft Office	Forma papierowa	079912 2009
35.	Zbiór danych dotyczących osób ubiegających się o orzeczenie o niepełnosprawności i stopniu niepełnosprawności	PZON	E p.5 ul. Poznańska 30	TAK	Krajowy Monitoring Osób Orzekających o Niepełnosprawności	Forma papierowa Forma elektroniczna	080271 2009
36.	Rejestr skarg i wniosków	OG	B p.7 ul Poznańska 33	TAK	Microsoft Office	Forma papierowa Forma elektroniczna	079916 2009
37.	Klasyfikacja gruntów	GN	C p.80 ul. Poznańska 30	TAK	Microsoft Office	Forma papierowa Forma elektroniczna	081535 2009
38.	Nadawanie na własność działek emerytalnych oraz pod budynkami	GN	C p.80 ul. Poznańska 30	TAK	Microsoft Office	Forma papierowa Forma elektroniczna	082204 2009
39.	Lista stypendystów	ER	E p. 24 ul. Poznańska 30	TAK	Microsoft Office	Forma papierowa Forma elektroniczna	079291 2009
40.	Ustalanie odszkodowań za grunty zajęte pod drogi	GN	B p.80 ul. Poznańska33	TAK	Microsoft Office	Forma papierowa Forma elektroniczna	079018 2009
41.	Wykaz radnych powiatu nowotomyskiego	OG	B p. 67 ul. Poznańska 33	NIE	Microsoft Office	Forma papierowa Forma elektroniczna	079914 2009
42.	System informacji	ER	E	TAK	System Informacji	Forma papierowa	0831109

	oświatowej		p.24 ul. Poznańska 33		Oświatowej	Forma elektroniczna	2009
43.	Skierowania do MOS i MOW	ER	E p.30	TAK	Ogólnopolski System Kierowania Nieletnich do MOW i MOS	Forma papierowa Forma elektroniczna	079610 2009
44.	Uczniowie zakwalifikowani do kształcenia specjalnego	ER	E. 30 ul. Poznańska 30	TAK	Microsoft Office	Forma papierowa Forma elektroniczna	079082 2009
45.	Arkusze organizacji szkół i placówek oświatowych	ER	E p.24 ul. Poznańska 30	TAK	Arkusz Optivum	Forma papierowa Forma elektroniczna	081732 2009
46.	Ochrona interesów konsumentów	PRK	B p.70 ul .Poznańska 33	TAK	Microsoft Office	Forma papierowa Forma elektroniczna	079910 2009
47.	Awans zawodowy nauczycieli	ER	E p.24 ul. Poznańska 30	TAK	Microsoft Office	Forma papierowa Forma elektroniczna	079081 2009
48.	Decyzja o umieszczeniu chorych w Zakładzie Opiekuńczo -Leczniczym	SOZK	C p.60 ul. Poznańska 33	TAK	Microsoft Office	Forma papierowa Forma elektroniczna	079619 2009
49.	Rejestr decyzji wydawanych przez Wojewodę	BI	C p.77,78,79 ul. Poznańska 33	TAK	Microsoft Office	Forma papierowa Forma elektroniczna	090701 2009
50.	Rejestr zgłoszeń zmiany sposobu użytkowania obiektu	BI	C p.77,78,79	TAK	Microsoft Office	Forma papierowa Forma elektroniczna	081537 2009
51.	Pozwolenia wodno prawne	RŚ	B p.59 ul. Poznańska 33	TAK	Microsoft Office	Forma papierowa Forma elektroniczna	105477 2011
52.	Rejestr posiadaczy	RŚ	C	TAK	Microsoft Office	Forma papierowa	104972

	działalność w zakresie zbierania, transportu, odzysku lub unieszkodliwiania		ul. Poznańska 33				
53.	Uczniowie zakwalifikowani do nauczania indywidualnego	ER	E. p.21 ul. Poznańska 30	TAK	Microsoft Office	Forma papierowa Forma elektroniczna	104662 2011
54.	Zadrzewienia i zieleń przydrożna	DP	E p.26 ul. Poznańska 30	TAK	Microsoft Office	Forma papierowa Forma elektroniczna	117827 2012
55.	Odszkodowania drogowe	DP	E p.26 ul. Poznańska 30	TAK	Microsoft Office	Forma papierowa Forma elektroniczna	117833 2012
56.	Decyzje lokalizacyjne i zajecie pasa drogowego	DP	E p.26 ul. Poznańska 30	TAK	Microsoft Office	Forma papierowa Forma elektroniczna	117825 2012
57.	Decyzja na urządzenia obce	DP	E p.26 ul. Poznańska 30	TAK	Microsoft Office	Forma papierowa Forma elektroniczna	117816 2012
58.	Zbiór danych osób ubiegających się o wydanie karty parkingowej	PZON	E p.5 ul. Poznańska 30	TAK	Microsoft Office	Forma papierowa Forma elektroniczna	2014
59.	Kluby uczniowskie i stowarzyszenia	SOZK	C p.59 ul. Poznańska 33	NIE	Microsoft Office	Forma papierowa Forma elektroniczna	150689 2014
60.	Obieg korespondencji	OG	B p.5 ul. Poznańska 33	NIE	Elektroniczne Zarządzanie Dokumentacją Sidas Doc Flow	Forma papierowa Forma elektroniczna	2015
61.	Zamówienia publiczne	ZP	C p.84 ul. Poznańska 33	NIE	Microsoft Office	Forma papierowa	2015

Załącznik nr 5
do załącznika nr 1do Zarządzenia
Nr. OG.120.5.2015

Opis struktury
Zbiorów danych osobowych, zawartości pól informacyjnych oraz powiązań pomiędzy nimi

Lp.	Nazwa zbioru	Zakres zawartości pól informacyjnych																Powiązanie ze zbiorem	Sposób przetwarzania danych T-tradyc. E-elektr.	Uwagi
		Nazwisko	Imię (imiona)	Imiona rodziców	Nazwisko rodowe panieńskie	Data urodzenia	Miejsce urodzenia	PESEL	Seria i nr d.o.	Seria i nr paszportu	Zawód	Wykształcenie	Miejsce pracy	Karalność	Kategoria prawa jazdy	Adres zamieszkania	Inne			
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
1.	Mienie zabużańskie	X	X													X			T	
2.	Plany urządzania lasów	X	X													X			T,E	
3.	Ewidencja kierowców powiatu nowotomyskiego	X	X	X		X		X	X					X	X	X			T, E	
4.	Ewidencja właścicieli pojazdów powiatu nowotomyskiego															X			T, E	
5.	Ewidencja instruktorów nauki jazdy powiatu nowotomyskiego	X	X			X		X			X	X		X		X	X Stan zdrowia		T, E	
6.	Ewidencja płatników opłat za użytkowanie	X	X													X			T, E	

7.	Decyzje o zmianie imion i nazwisk	X	X	X		X	X									X			T,E	
8.	Uzgadnianie dokumentacji projektowej	X	X													X	X NIP		T, E	
9.	Przyjmowanie podań i oświadczeń o zmianie obywatelstwa	X	X	X	X	X	X	X	X							X			T	
10.	Poborowi z Powiatu Nowy Tomyśl – orzecznictwo	X	X	X	X	X		X								X	X kategoria zdrowia		T,E	
11.	Karty wędkarskie	X	X			X	X									X			T, E	
12.	Ewidencja gruntów i budynków	X	X													X			T,E	
13.	Sprzęt pływający do połowu ryb	X	X													X			T, E	
14.	Gospodarowanie nieruchomościami Skarbu Państwa	X	X													X			T	
15.	Zasób geodezyjno-kartograficzny	X	X	X		X										X			T	
16.	Rejestr ewidencja rozpoczynanych i oddawanych do użytkowania obiektów budowlanych	X	X													X	Adres budowy, nr Ew. działki		T	
17.	Rejestr decyzji o pozwoleniu na budowę	X	X													X	Adres budowy, nr Ew. działki		T	
18.	Ewidencja wydanych licencji i zaświadczeń na transport drogowy	X	X			X	X	X						X		X	X NIP		T, E	

19.	Rejestr – spis zaświadczeń	X	X													X	Adres budowy, nr Ew. działki		T	
20.	Rejestr spis decyzji odmownych dot. decyzji pozwolenie na budowę	X	X													X	Adres budowy i nr Ew. działki		T	
21.	Rejestr wniosków o pozwolenie na budowę	X	X													X	Adres budowy i nr Ew. działki		T	
22.	Zezwolenia o dopuszczenie reproduktora do użytkowania w punkcie kopulacyjnym na podstawie ustawy o organizacji hodowli i rozrodzie zwierząt gospodarskich	X	X													X			T	
23.	Rejestr – dzienników budowy	X	X													X	Adres budowy i nr Ew. działki		T	
24.	Rejestr posiadaczy zwierząt przetrzymywanych lub hodowanych na podstawie ustawy o ochronie przyrody	X	X													X			T	
25.	Rejestr – spis zgłoszeń budów, robot budowlanych, rozbiórek	X	X													X			T	
26.	Sprawy sądowe dotyczące regulowania stanów prawnych	X	X	X					X							X	Numer telefonu		T	

27.	Wynagradzanie pracowników Starostwa Powiatowego Nowy Tomyśl	X	X					X					X			X			T, E	
28.	Nabór na wolne stanowisko pracy	X	X	X												X				
29.	System kadrowy	X	X			X	X				X	X	X			X			T	
30.	Rejestr legitymacji osób niepełnosprawnych	X	X			X	X	X	X							X			T, E	
31.	Wypłata ekwiwalentu przyznanego osobom fizycznym na podstawie ustawy o wspieraniu rozwoju obszarów wiejskich	X	X													X				
32.	Zezwolenie na przetrzymywanie zwierzyny leśnej oraz hodowanie chartów rasowych	X	X													X				
33.	Spis kart informacyjnych dot. Przedsięwzięć mogących znacząco oddziaływać na środowisko	X	X													X			T	
34.	Oświadczenia majątkowe	X	X			X	X				X	X				X	Numer telefonu		T	

35.	Zbiór danych dotyczących osób ubiegających się o orzeczenie o niepełnosprawności i stopniu niepełnosprawności	X	X	X		X	X	X	X		X	X	X			X	Nr telefonu, stan cywilny, stan rodzinny		T, E	
36.	Rejestr skarg i wniosków	X	X													X			T	
37.	Klasyfikacja gruntów	X	X													X	Numer telefonu		T	
38.	Nadawanie na własność działek emerytalnych oraz gruntu pod zabudowaniami	X	X	X					X							X	Numer telefonu		T	
39.	Lista stypendystów	X	X	X												X				
40.	Ustalanie odszkodowań za grunty zajęte pod drogi	X	X													X			T	
41.	Wykaz radnych powiatu nowotomyskiego	X	X								X	X				X	Numer telefonu		T	
42.	System informacji oświatowej	X	X					X			X	X	X			X	Płeć, rok ur., dane o wymiarze zatrudnienia, stopień awansu zawodowego, staż		T,E	

43.	Skierowania do MOW i MOS	X	X			X	X	X								X			T,E	
44.	Uczniowie zakwalifikowani do kształcenia specjalnego	X	X			X										X			T	
45.	Arkusze organizacji szkół i placówek oświatowych	X	X									X	X				Stopień awansu zawodowego		T	
46.	Ochrona interesów konsumentów	X	X													X	Numer telefonu		T	
47.	Awans zawodowy nauczycieli	X	X			X	X					X				X			T	
48.	Decyzja o umieszczaniu chorych w Zakładzie Opiekuńczo-Leczniczym	X	X													X				
49.	Rejestr decyzji wydawanych przez Wojewodę	X	X													X	Adres budowy i nr Ew. działki		T	
50.	Rejestr zgłoszeń zmiany sposobu użytkowania obiektu	X	X													X			T	
51.	Pozwolenie wodno-prawne	X	X													X				
52.	Rejestr posiadaczy odpadów prowadzących działalność w zakresie zbierania, transportu, odzysku lub unieszkodliwiania	X	X													X				
53.	Uczniowie	X	X			X										X			T	

	zakwalifikowani do nauczania indywidualnego																			
54.	Zadrzewienia i zieleń przydrożna	X	X													X				
55.	Odszkodowania drogowe	X	X													X				
56.	Decyzje lokalizacyjne i zajęcie pasa drogowego	X	X													X				
57.	Decyzje na urządzenia obce	X	X													X				
58.	Zbiór danych osób ubiegających się o wydanie karty parkingowej	X	X													X				
59.	Kluby uczniowskie i stowarzyszenia	X	X													X				
60.	Obieg korespondencji	X	X													X			T	
61.	Zamówienia publiczne	x	x													X				

Załącznik nr 6
do Załącznika nr 1 do Zarządzenia Nr 6/2015
Starosty Nowotomyskiego
„Oświadczenie pracownika dotyczące przestrzegania przepisów o korzystaniu z legalnego oprogramowania teleinformatycznego„

OŚWIADCZENIE*

o odpowiedzialności za powierzony sprzęt komputerowy

Po kontroli przeprowadzonej w dniu ..... oświadczam, iż oprogramowanie zainstalowane na wymienionym komputerze w pełni legalne.

.....
(podpis Administratora Systemu Informatycznego)

Komputer wymieniony powyżej powierzam pod nadzór i użytkowanie:

p. .....

- Na powierzonym komputerze może być wykorzystywane wyłącznie oryginalne, licencjonowane oprogramowanie, zainstalowane przez ASI.
- Nie wolno instalować, kopiowa, uruchamiać programów nielicencjonowanych (z dysku, dyskietek, CD-ROM-u lub innego nośnika).
- Nie wolno kopiować i przechowywać na dysku komputera plików i programów niezwiązanych z wykonywanymi obowiązkami służbowymi, w szczególności dotyczy to: plików muzycznych i filmowych łamiących prawa autorskie, programów rozrywkowych (gry, komunikatory internetowe itp.)
- Wszelkie wątpliwości związane z legalnością oprogramowania należy wyjaśniać z ABI.

.....
(podpis Administratora Bezpieczeństwa Informacji)

*Oświadczam, iż powierzony mi sprzęt komputerowy będę wykorzystywać zgodnie z jego przeznaczeniem oraz biorę pełną odpowiedzialność za legalność zainstalowanego przeze mnie na nim oprogramowania.

.....
(miejscowość i data)

.....
(czytelny podpis pracownika)

* Oświadczenie dotyczy umów cywilnoprawnych.

	Zestaw komputerowy	Monitor	UPS	Drukarka
Nazwa				
Nr. inwentarzowy				
Miejsce zainstalowania: Starostwo Powiatowe w Nowym Tomyślu ul. Poznańska ….. , pok. nr: ….				
Zainstalowane oprogramowanie:	…… ……			

Załącznik nr 7
do Załącznika nr 1 do Zarządzenia
Nr. OG.120.6.2015

W z ó r

R a p o r t
z naruszenia bezpieczeństwa systemu informatycznego w Starostwie Powiatowym w Nowym Tomyślu

1. Data: ..... Godzina: .....
(dd.mm.rrrr) *(00:00)*

2. Osoba powiadamiająca o zaistniałym zdarzeniu:

.....
(Imię, nazwisko, stanowisko służbowe, nazwa użytkownika (jeśli występuje))

3. Lokalizacja zdarzenia:

.....
(np. nr pokoju, nazwa pomieszczenia)

4. Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące:

.....
.....

5. Podjęte działania:

.....
.....

6. Przyczyny wystąpienia zdarzenia:

.....
.....

7. Postępowanie wyjaśniające:

.....
.....

.....
data, podpis Administratora
Bezpieczeństwa Informacji