Załącznik Nr 1
do Zarządzenia Nr 5/16
Wójta Gminy Turośl
z dnia 29 grudnia 2016 roku

POLITYKA BEZPIECZEŃSTWA

przetwarzania danych osobowych
w
Urzędzie Gminy Turośl

Podstawa prawna.

-Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2016. 922 t.j. z dnia 2016.06.28 z pózn. 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 pózn. zm.)

-Zarządzenie Nr 143/08 Wójta Gminy Turośl z dnia 23 grudnia 2008 roku;

- Zarządzenie Nr 142/08 Wójta Gminy Turośl z dnia 23 grudnia 2008 roku

1. Definicje

- Zbiór danych osobowych – każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.
- Administrator danych osobowych – zadania administratora danych osobowych wykonuje Wójt Gminy.
- Inspektor Bezpieczeństwa teleinformatycznego – osoba wyznaczona przez administratora danych osobowych, odpowiedzialna za bezpieczeństwo danych osobowych przetwarzanych we wskazanych systemach informatycznych. Na podstawie Zarządzenia Nr 143/08 Wójta Gminy Turośl z dnia 23 grudnia 2008 roku zadania wykonuje Sekretarz Gminy Turośl.
- Administrator systemu teleinformatycznego – osoba odpowiedzialna za sprawność, konserwację oraz wdrażanie technicznych zabezpieczeń systemu informatycznego do przetwarzania danych osobowych w Urzędzie Gminy. Na podstawie Zarządzenia Nr 142/08 Wójta Gminy Turośl z dnia 23 grudnia 2008 roku zadania wykonuje Informatyk – Adam Lewandowski
- System informatyczny – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
- Stacja robocza – stacjonarny lub przenośny komputer wchodzący w skład systemu

informatycznego umożliwiający użytkownikom systemu dostęp do danych osobowych znajdujących się w systemie.

- Bezpieczeństwo systemu informatycznego – wdrożenie przez administratora danych osobowych lub osobę przez niego uprawnioną środków organizacyjnych i technicznych w celu zabezpieczenia oraz ochrony danych przed dostępem, modyfikacją, ujawnieniem, pozyskaniem lub zniszczeniem.
- Przetwarzanie danych osobowych – wykonywanie jakichkolwiek operacji na danych osobowych, takich jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i ich usuwanie.
- Osoba upoważniona – osoba posiadająca upoważnienie wydane przez administratora danych osobowych (lub osobę uprawnioną przez niego) i dopuszczona jako użytkownik do przetwarzania danych osobowych w systemie informatycznym danej komórki organizacyjnej w zakresie wskazanym w upoważnieniu (listę osób upoważnionych do przetwarzania danych osobowych posiada administrator bezpieczeństwa informacji).
- Użytkownik systemu – osoba posiadająca uprawnienia do przetwarzania danych osobowych w systemie informatycznym.
- Osoba uprawniona – osoba posiadająca upoważnienie wydane przez administratora danych osobowych do wykonywania w jego imieniu określonych czynności.
- Ustawa – ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2016. 922 t.j. z dnia 2016.06.28 z pózn. zm.)
- Rozporządzenie - 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 pózn. zm.).

2. Zasady ogólne

Ochrona danych osobowych przetwarzanych w Urzędzie Gminy Turośl obowiązuje wszystkie osoby, które mają dostęp do informacji zbieranych, przetwarzanych oraz przechowywanych w urzędzie, bez względu na zajmowane stanowisko oraz miejsce wykonywania jak również charakter stosunku pracy.

- osoby mające dostęp do danych osobowych są zobligowane do stosowania niezbędnych środków zapobiegających ujawnieniu tych danych osobom nieupoważnionym,
- zachowanie tajemnicy obowiązuje zarówno podczas trwania stosunku pracy jak i po jego ustaniu.
- ADO jest odpowiedzialny za tworzenie, wdrażanie, administrację i interpretację polityki bezpieczeństwa informacji, standardów, zaleceń oraz procedur w całym systemie ,
- polecenia do działań związanych z ochroną w zakresie ochrony informacji i bezpieczeństwa systemu informatycznego muszą być bezwzględnie wykonywane przez wszystkich pracowników i użytkowników systemu.

2.1. Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe zawarty jest w Załączniku nr 1 do niniejszego dokumentu.

2.2. Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych zawarty jest w Załączniku nr 2 do niniejszego dokumentu.

2.3. Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi zawarty jest w Załączniku nr 3 do niniejszego dokumentu

2.4. Sposób przepływu danych pomiędzy poszczególnymi systemami zawarty jest w Załączniku nr 4 do niniejszego dokumentu.

I. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

1. Podstawowymi zagrożeniami w procesie przetwarzania danych osobowych są następujące sytuacje, które mogą doprowadzić do nieautoryzowanego dostępu do danych osobowych :

a) próby naruszenia danych osobowych z zewnątrz :

- dostęp do danych poprzez publiczną sieć Internet
- włamania do systemu,
- podsłuch,
- kradzież danych,

b) próby naruszenia danych osobowych z wewnątrz:

- umyślna lub nieumyślna modyfikacja danych,
- umyślne lub nieumyślne udostępnianie danych osobowych przez osoby zatrudnione przy przetwarzaniu danych osobowych,
- dostęp do pomieszczeń, w których przetwarza się dane osobowe, osób nieuprawnionych,
- dostęp do systemów komputerowych osób nieuprawnionych,
- kradzież danych,

c) programy destrukcyjne :

- wirusy,
- konie trojańskie,
- makra,
- bomby logiczne,

d) awarie sprzętu lub uszkodzenie oprogramowania,

e) kradzież sprzętu lub nośników z ważnymi danymi,

f) usiłowanie zakłócenia działania systemu informatycznego,

g) inne skutkujące utratą danych osobowych, bądź wejściem w ich posiadanie osób nieuprawnionych.

h) zanik zasilania systemów informatycznych w czasie ich pracy.

2. Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych:

a) środki ochrony fizycznej :

- system alarmowy,
- dozór całodobowy (firma ochroniarska),
- zamki patentowe,
- sejfy,
- szafy zamykane na klucz,
- przetwarzanie danych osobowych dokonywane jest w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych,
- osoby zatrudnione przy przetwarzaniu danych są szkolone w tym zakresie podczas szkolenia wstępnego (przed przyjęciem do pracy), oraz uprzedzone o odpowiedzialności z tym związanej,
- przebywanie osób nieuprawnionych w pomieszczeniach, gdzie przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu danych osobowych oraz w warunkach zapewniających bezpieczeństwo tych danych,
- kopie zapasowe/archiwalne zbioru danych osobowych przechowywane są w zamkniętej szafie metalowej.

b) środki sprzętowe, informatyczne i telekomunikacyjne :

- zabezpieczeniu podlegają – komputery, sieć komputerowa wewnętrzna, routery, modemy, system operacyjny,
- zastosowano środki bezpieczeństwa na **poziomie wysokim**, ponieważ co najmniej jedno urządzenie systemu informatycznego, służącego do przetwarzania danych osobowych, połączone jest z siecią publiczną,
- pomieszczenia, w których przetwarza się dane osobowe zabezpieczone są przed skutkami pożaru za pomocą gaśnic ręcznych,
- dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą profesjonalnych niszczarek dokumentów,
- lokalizacja urządzeń komputerowych uniemożliwia osobom nieupoważnionym dostęp do nich oraz wgląd do danych wyświetlanych na monitorach komputerowych
- system operacyjny zapewnia odpowiednie restrykcje w zakresie dostępu do danych i aplikacji,

- zastosowano urządzenia UPS chroniące system informatyczny służący do przetwarzania danych osobowych przed awarią zasilania,
- zastosowano macierz dyskową w serwerach,
- dostęp do sieci internet został zabezpieczony routerem z funkcją NAT (translacji adresów sieciowych), zastosowano sprzętowy firewall,
- zastosowano system IDS,
- zastosowano serwer logów,
- dane osobowe są przesyłane w sieci informatycznej dedykowanej do obsługi systemu informatycznego przetwarzającego te dane (intranet). Sieć ta jest odseparowana od pozostałej infrastruktury teleinformatycznej poprzez fizyczne rozdzielenie infrastruktury ethernetowej (osobna podsieć), udostępniając tylko wybrane porty na serwerach znajdujących się w sieci,
- użytkownik pracuje na koncie systemowym jedynie z uprawnieniami niezbędnymi do wykonywania swojej pracy.

c) środki ochrony w ramach oprogramowania urządzeń teletransmisji :

- proces teletransmisji zabezpieczony jest za pomocą środków uwierzytelnienia (identyfikator, hasło),
- proces teletransmisji zabezpieczony jest za pomocą środków kryptograficznej ochrony danych osobowych,
- używany jest protokół HTTPS

d) środki ochrony w ramach oprogramowania systemu :

- dostęp do zbiorów danych osobowych przetwarzanych za pomocą komputerów zabezpieczony jest za pomocą hasła,
- zastosowano klasyfikację użytkowników w celu określenia odpowiednich praw dostępu do zasobów informatycznych,
- o ile system na to pozwala zastosowano mechanizm wymuszający okresową zmianę haseł (nie rzadziej niż co 30 dni),
- serwery i stanowiska komputerowe służące do przetwarzania danych osobowych oraz systemy komputerowe obsługujące bazy dostępne są wyłącznie po przeprowadzeniu prawidłowego procesu autoryzacji danych (wymóg podania przez użytkownika identyfikatora i hasła dostępu),
- zapewniono rejestrację czasu nieudanych logowań do systemu przetwarzającego dane osobowe,

- zastosowano system rejestracji dostępu do zbioru danych osobowych,
- w celu ochrony antywirusowej stosuje się oprogramowanie antywirusowe z codzienną aktualizacją baz wirusów,
- w komputerach stosuje się jedynie legalne oprogramowanie,
- użytkownicy nie mogą sami instalować oprogramowania.

e) środki ochrony w ramach narzędzi baz danych i innych narzędzi programowych :

- dostęp do zbiorów danych osobowych zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła dostępu,
- zastosowano mechanizm umożliwiający rejestrację identyfikatora użytkownika wprowadzającego lub zmieniającego dane osobowe,
- wykorzystano środki pozwalające na rejestrację dokonanych zmian w zbiorach danych osobowych,
- zastosowano środki umożliwiające określenie praw dostępu do zbioru danych osobowych,
- zastosowano identyfikator i hasło dostępu do danych na poziomie aplikacji,
- dla każdego użytkownika systemu jest ustalony odrębny identyfikator,
- zastosowano mechanizm wymuszający lub przypominający okresową zmianę haseł dostępu do zbioru danych osobowych,

f) środki ochrony w ramach systemu użytkowego

Zastosowano zabezpieczone hasłem wygaszanie ekranu w przypadku dłuższej nieaktywności użytkownika.

g) środki organizacyjne :

- wyznaczono Inspektora Bezpieczeństwa Teleinformatycznego oraz Administratora Systemu Teleinformatycznego,
- opracowano i wdrożono Politykę bezpieczeństwa i Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych,
- wdrożono odpowiedni podział obowiązków i kontroli dostępu,
- do danych osobowych mają dostęp jedynie osoby posiadające upoważnienie nadane przez Administrator Danych Osobowych,
- Inspektor Bezpieczeństwa Teleinformatycznego, w ramach powierzonych przez Administratora Danych Osobowych obowiązków, prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych,

- wprowadzono mechanizmy autoryzacji odpowiednio zabezpieczone przed dostępem osób trzecich,
- wprowadzono procedury alarmowe i informacyjne,
- osoby upoważnione do przetwarzania danych osobowych przed dopuszczeniem do tych danych są szkolone w zakresie obowiązujących przepisów o ochronie danych osobowych, procedur przetwarzania danych oraz informowane o podstawowych zagrożeniach związanych z przetwarzaniem danych osobowych. Osoby te są zobowiązane do podpisania stosownego oświadczenia, którego wzór zawiera Załącznik nr 5 do niniejszego dokumentu
- osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane są do zachowania ich w tajemnicy,
- monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym,
- tymczasowe wydruki z danymi osobowymi są po ustaniu ich przydatności niszczone w profesjonalnych niszczarkach,
- korespondencja prowadzona jest za pomocą listów poleconych,
- zapewniono klauzule poufności z wszystkimi podmiotami zewnętrznymi mającymi dostęp do danych osobowych,
- zapewnia się bezpieczne przechowywanie lub niszczenie uszkodzonych nośników zawierających dane osobowe, szczególnie gdy sprzęt, w którym zamontowany jest nośnik, przekazywany jest do naprawy firmie zewnętrznej,
- dane osobowe z użyciem systemu informatycznego i w formie papierowej są przetwarzane w godzinach pracy Urzędu Gminy Turośl. Poza tymi godzinami wyłącznie w uzasadnionych przypadkach, po uzyskaniu zgody administratora danych i powiadomieniu Inspektora Bezpieczeństwa Teleinformatycznego.
- w obszarze przetwarzania danych osobowych mogą przebywać wyłącznie pracownicy zatrudnieni przy przetwarzaniu danych, osoby zainteresowane przetwarzanymi danymi, Inspektor Bezpieczeństwa Teleinformatycznego, Administrator Systemu Teleinformatycznego oraz inne osoby indywidualnie upoważnione do tego przez Administratora Danych. Przebywanie osób nieuprawnionych do dostępu do danych osobowych w pomieszczeniach znajdujących się wewnątrz obszaru przetwarzania tych danych, jest dopuszczalne tylko w obecności osoby upoważnionej do przetwarzania danych osobowych,

- pomieszczenia w obszarze przetwarzania danych osobowych muszą być zamykane na zamek w czasie nieobecności pracowników. Klucze powinny być przechowywane w sposób uniemożliwiający dostęp do nich przez osoby nieupoważnione do przetwarzania danych osobowych.
- dyski HDD i inne nośniki elektroniczne zawierające dane osobowe a przeznaczone do likwidacji lub naprawy są pozbawiane zapisu lub niszczone fizycznie(likwidacja) jeżeli nie ma innej metody zlikwidowania zapisu.

II Obowiązki pracownicze osób zatrudnionych przy przetwarzaniu danych osobowych wynikające z potrzeby zapewnienia ochrony danych osobowych

1. Obowiązek przestrzegania tajemnicy danych osobowych dotyczy wszystkich pracowników, którzy mają dostęp do zbiorów danych osobowych.
2. Naruszenie zasad ochrony danych osobowych, w szczególności umyślne lub nieumyślne udostępnienie danych osobowych osobie nieupoważnionej, jest naruszeniem obowiązków pracowniczych. W tym przypadku zastosowanie mają przepisy z art. 51 i 52 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych Dz. U. 2016. 922 t.j. z dnia 2016.06.28 z pózn. zm.
3. Administrator Danych Osobowych zobowiązany jest do:
   - kontroli przestrzegania zasad i sposobu wykonywania operacji przetwarzania danych przez podległych pracowników;
   - zapewnienia, że przetwarzania danych osobowych może dokonywać jedynie pracownik upoważniony przez administratora danych, w zakresie indywidualnych obowiązków pracowniczych.
4. Osoba upoważniona przez administratora danych osobowych, jest zobowiązana do:
   - zapoznania się z przepisami prawa w zakresie ochrony danych osobowych;
   - stosowania określonych przez administratora danych procedur i środków, mających na celu zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym;
   - zachowania szczególnej staranności w trakcie wykonywania operacji przetwarzania danych osobowych;
   - przestrzegania ustalonych zasad i procedur w zakresie ochrony danych osobowych.

III Procedury postępowania w przypadku naruszenia bezpieczeństwa danych osobowych

- w przypadku stwierdzenia faktu nieuprawnionego przetwarzania, ujawnienia, kradzieży lub nienależytego zabezpieczenia przed osobami nieuprawnionymi danych osobowych, jak również stwierdzenia istnienia przesłanek wskazujących na prawdopodobieństwo innego naruszenia ochrony danych osobowych, pracownik zobowiązany jest poinformować o tym zdarzeniu ADO/IBT/AST lub osobę go zastępującą, w sytuacji określonej powyżej Administrator Bezpieczeństwa Informacji prowadzi postępowanie wyjaśniające, w toku którego: ustala czas wystąpienia naruszenia, jego zakres, przyczyny, skutki oraz wielkość szkód, które zaistniały, ustala osoby odpowiedzialne za naruszenie, podejmuje działania w kierunku ograniczenia szkód oraz przeciwdziałania podobnym przypadkom w przyszłości,
- IBT prowadzi ewidencję naruszeń bezpieczeństwa danych osobowych wg wzoru załącznika nr 6 do niniejszej Polityki.

Procedura postępowania w przypadkach stwierdzenia słabości systemu:

- w przypadku jakiejkolwiek nieprawidłowości w działaniu systemu, uszkodzenia lub podejrzenia uszkodzenia sprzętu, oprogramowania lub danych należy bezzwłocznie powiadomić Administratora Systemu Informatycznego i Administratora Bezpieczeństwa Informacji,
- w przypadku włamania lub podejrzenia o włamanie do systemu Administrator Systemu Teleinformatycznego podejmuje działania w celu zabezpieczenia systemu i danych :
    - zmienia hasła dostępu,
    - określa rodzaj i sposób włamania,
    - podejmuje działania w celu uniemożliwienia ponownego włamania tego samego typu,
    - szacuje straty w systemie,
    - przywraca stan systemu sprzed włamania,
    - w przypadku uszkodzenia sprzętu lub programów z danymi Administrator Systemu Informatycznego podejmuje działania w celu:
    - określenia przyczyny uszkodzenia,
    - oszacowania strat wynikłych z ww. uszkodzenia,
    - naprawy uszkodzeń, a w szczególności naprawy sprzętu, ponownego

zainstalowania danego programu, odtworzenia jego pełnej konfiguracji oraz wczytania danych z ostatniej kopii zapasowej,

- w przypadku uszkodzenia danych Administrator Systemu Teleinformatycznego podejmuje następujące działania:
    - ustala przyczynę uszkodzenia danych,
    - określa wielkość i jakość uszkodzonych danych,

    podejmuje działania w celu odtworzenia danych z ostatniej kopii zapasowej.

IV Polityka zarzadzania oprogramowaniem

1. Zasady ogóle

a) Urząd Gminy Turośl posiada licencjonowane egzemplarze programów komputerowych różnych producentów oprogramowania. Licencjonowane i zarejestrowane egzemplarze programów zostały zainstalowane na komputerach oraz sporządzono odpowiednie kopie zapasowe oprogramowania zgodnie z warunkami umów licencyjnych. Bez pisemnej zgody producenta oprogramowania nie wolno wykonywać żadnych dodatkowych kopii programów ani też ich dokumentacji.

b) poza oprogramowaniem komercyjnym wykorzystuje się oprogramowanie darmowe, czyli freeware, oraz na licencji GPL.

c) stanowiska komputerowe pracowników zostały wyposażone w legalne oprogramowanie. Używanie oprogramowania pochodzącego z jakiegokolwiek innego źródła, bez konsultacji z AST może stanowić zagrożenie dla bezpieczeństwa Urzędu oraz grozić może wszczęciem postępowania prawnego – używanie takiego oprogramowania jest ściśle zabronione, ,

d) pracownicy są zobowiązani do zapoznania się z odpowiednimi przepisami o ochronie praw autorskich oraz kodeksu karnego przedstawionymi im przez AST lub zawartego w używanych przez nich programach. Przepisy te mówią o odpowiedzialności pracownika w przypadku korzystania z nielegalnego oprogramowania,

e) programy zainstalowane przez pracowników w celu pobierania danych (plików mp3, filmów, itp.) stanowią ogromne zagrożenie dla bezpieczeństwa sieci oraz jej wydajności. Wykorzystywanie tego rodzaju oprogramowania jest zabronione i może stanowić podstawę do wyciągnięcia odpowiedzialności prawnej,

2. Zasady korzystania z komputerów przenośnych

a) Wszyscy pracownicy urzędu korzystający z komputerów przenośnych mogą korzystać z nich poza miejscem pracy zachowując obowiązujące w urzędzie zasady korzystania z sprzętu i oprogramowania.

b) pracownik korzystający z komputera poza miejscem pracy może go wykorzystywać do celów prywatnych z zastrzeżeniem, iż na komputerze nie może przechowywać żadnych danych ani wykorzystywać go do celów niezgodnych z obowiązującym prawem.

c) pracownik może korzystać z oprogramowania stanowiącego jego prywatną własność pod warunkiem iż licencja zezwala na jej wykorzystanie komercyjne (nie jest licencją edukacyjną bądź wyłącznie do użytku domowego) pod warunkiem zachowania następujących zasad:

- Pracodawca musi określić zakres prac służbowych, do jakich będzie wykorzystywać oprogramowanie prywatne.
- Po wyrażeniu zgody przez przełożonych pracownik dostarczy pracodawcy wszelkie dowody stanowiące o legalności oprogramowania, na co osoba przyjmująca dokumentację sporządzi stosowny protokół.
- dokumentacja na to oprogramowanie zostanie dołączona do metryki komputera użytkownika, a po zaprzestaniu korzystania z prywatnego oprogramowania zostanie w całości zwrócona właścicielowi. Fakt zwrócenia musi zostać udokumentowany odpowiednim protokołem, bądź odnotowany w protokole przyjęcia.
- Pracownik wykorzystujący prywatne oprogramowanie na czas jego eksploatacji w miejscu pracy musi odinstalować oprogramowanie w domu, chyba, że licencja programu stanowi inaczej (np. pozwala na korzystanie z dwóch instalacji programu).

3. Dodatkowe kopie

1) W niektórych przypadkach umowa licencyjna pozwala na sporządzenie dodatkowej kopii określonego programu, przeznaczonej do użytkowania na komputerze przenośnym lub komputerze domowym wykorzystywanym do celów służbowych. Pracownicy nie mogą sami bez konsultacji z AST wykonywać dodatkowych kopii oprogramowania lub dokumentacji.
2) łamanie, czy obchodzenie zabezpieczeń oprogramowania jest niedopuszczalne.
3) niedopuszczalne jest wykonanie więcej niż jednej kopii oprogramowania. Chyba, że umowa licencyjna na to pozwala.

4. Wewnętrzna kontrola

1. Urząd Gminy Turośl zastrzega sobie prawo do ochrony swojej reputacji i swoich inwestycji w programy komputerowe poprzez ustanowienie wewnętrznych mechanizmów kontroli zapobiegających wykonywaniu lub użytkowaniu nielegalnych

kopii oprogramowania. Mechanizmy te obejmują kontrole sposobu wykorzystywania oprogramowania, zapowiedziane i niezapowiedziane przeglądy zawartości służbowych komputerów umożliwiające stwierdzenie zgodności zainstalowanego oprogramowania z umowami licencyjnymi, usuwanie wszelkich programów zainstalowanych na służbowych komputerach, dla których nie da się stwierdzić ważności licencji lub przedstawić jej dowodu, a także podjęcie postępowania dyscyplinarnego w stosunku do pracowników naruszających postanowienia niniejszych zasad użytkowania oprogramowania.

5. Procedury zarządzania oprogramowaniem

1. Procedura zgłaszania zapotrzebowania na oprogramowanie.
    a. Zgłoszenie zapotrzebowania na oprogramowanie należy dokonywać do AST,
    b. AST konsultuje zgłoszenie z Sekretarzem Gminy.
    c. Decyzje o zakupie oprogramowania podejmuje Wójt.
2. Procedura zakupu oprogramowania komputerowego.
    a. AST kontaktuje się z dystrybutorem oprogramowania w celu uzgodnienia szczegółów zakupu oprogramowania i licencji.
    b. Dostawca dostarcza nośnik z oprogramowaniem, licencję oraz fakturę zakupu, które stanowią podstawę legalności oprogramowania.
    c. W przypadku przedłużenia licencji, opieki autorskiej bądź aktualizacji oprogramowania AST pisemnie kontaktuje się z odpowiednimi dystrybutorami.
    d. Wszelkie zakupy oprogramowania zatwierdza Wójt lub Sekretarz Gminy.
3. Procedura instalacji oprogramowania.
    a. Proces instalacji dokonuje tylko AST lub pracownik firmy zewnętrznej, ale tylko i wyłącznie w obecności AST.
    b. AST zapoznaje pracownika z nowo zainstalowanym oprogramowaniem i poucza o legalnym wykorzystaniu oprogramowania.
4. Procedura aktualizacji oprogramowania.
    a. W przypadku, kiedy pozwala na to licencja programu aktualizacja może być darmowa. Wykonuje ją pracownik lub AST.
    b. W przypadku programów o określonym czASTe licencji i płatnej aktualizacji, AST wypełnia stosowne wnioski o aktualizacje oprogramowania i dokonuje instalacji.

5. Procedura likwidacji oprogramowania.
    a. W przypadku licencji OEM, program jest likwidowany razem ze sprzętem komputerowym.
    b. Nośniki programów, które są uważane za nieprzydatne mogą zostać zlikwidowane po trzech latach ich nieużytkowania.
6. Procedura audytu\inwentaryzacji oprogramowania.
    a. Procedura inwentaryzacji oprogramowania odbywa się raz do roku. Przeprowadza ją AST, a wyniki przedstawia IBT/ADO.

Załącznik Nr 1
do Polityki Bezpieczeństwa

Wykaz
budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane

L.p.	Miejsce przetwarzania	Nr pomieszczenia	Nazwa zbioru	Postać
1.	Urząd Gminy Turośl, ul. Jana Pawła II 49, 18- 525 Turośl,	pokój Nr 2	Podatki i opłaty lokalne, Auta, Księgowość Podatkowa, Ewidencja upomnień i tytułów wykonawczych, Zwrot podatku akcyzowego, Podatek od środków transportowych	Papierowa/ elektroniczna
2.		Pokój Nr 5	Zaopatrzenie ludności w wodę i kanalizację	Papierowa/ elektroniczna
3.		pokój Nr 6	Akty Stanu Cywilnego, Ewidencja Ludności, Rejestr Wyborców, Dowody Osobiste, Ewidencja działalności gospodarczej, Zezwolenia na sprzedaż napojów alkoholowych	Papierowa/ elektroniczna
4.		pokój Nr 8	Czystość i porządek Opłaty Komunalne Rejestr Skarg i Wniosków Ewidencja Radnych Oświadczenia Majątkowe Umowy przekazanych Gospodarstw Rolnych Teczki Osobowe pracowników	Papierowa/ elektroniczna

5.		Pokój Nr 10	Ustalenie lokalizacji inwestycji celu publicznego, Zaświadczenia o przeznaczeniu terenu w planie zagospodarowania przestrzennego, Zajęcie pasa drogowego, Ustalenie warunków zabudowy i zagospodarowania terenu, Numeracja porządkowa nieruchomości Decyzje zatwierdzające projekt podziału nieruchomości, Rejestr osób korzystających z dodatków mieszkaniowych Zezwolenia na wycinkę drzew	Papierowa/elektroniczna
6.		pokój Nr 12	Dane osobowe i ubezpieczeniowe pracowników,	Papierowa/ elektroniczna
7.		pokój Nr 16	Ochotnicza Straż Pożarna , Rejestracja i kwalifikacja wojskowa, Świadczenia Osobiste i Rzeczowe na rzecz obrony Kopie Zapasowe CD/DVD	Spakowane pliki bazodanowe na CD/DVD/dysk zewnętrzny
8		Archiwum (piwnica Urzędu Gminy)	Teczki Archiwalne	Papierowa
9		Serwerownia (piwnica Urzędu Gminy)	Elektroniczny System Obiegu Dokumentów	elektroniczna

Załącznik Nr 2
do Polityki Bezpieczeństwa

Wykaz

zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych

Lp.	Nazwa zbioru danych osobowych	Forma gromadzenia danych	Nazwa programu zastosowanego do przetwarzania danych	Autor programu
1.	Rejestr skarg i wniosków	Papierowa	N/D	N/D
2.	Ewidencja radnych	papierowa	N/D	N/D
3.	Oświadczenia majątkowe	papierowa	N/D	N/D
4.	Archiwum zakładowe	papierowa	N/D	N/D
5.	Ewidencja upomnień i tytułów wykonawczych	Papierowa/ elektroniczna	KSZOB	U.I. INFO-SYSTEM Sp. J.
6.	Ochotnicza Straż Pożarna	papierowa	N/D	N/D

7.	Rejestracja i kwalifikacja wojskowa	Papierowa/elektroniczna	MS Office	Microsoft
8.	Zwrot podatku akcyzowego	Papierowa/elektroniczna	MS Office Excell	Microsoft
9.	Podatek od środków transportowych	Papierowa/elektroniczna	AUTA	U.I. INFO-SYSTEM Sp. J.
10.	Zaświadczenia w sprawach podatkowych	Papierowa/elektroniczna	Podatki	U.I. INFO-SYSTEM Sp. J.
11.	Ewidencja działalności gospodarczej	Papierowa/elektroniczna	Platforma CEIDG serwer Min. Gospodarki	Ministerstwo Gospodarki (połączenie szyfrowane)
12.	Ustalenie lokalizacji inwestycji celu publicznego	Papierowa	N/D	N/D
13.	Zaświadczenia o przeznaczeniu terenu w planie zagospodarowania przestrzennego	Papierowa	N/D	N/D
14.	Zajęcie pasa drogowego	Papierowa	N/D	N/D

15.	Czystość i porządek	Papierowa/elektroniczna	GOMING-Odpady/ Kszob	ARISCO Sp. z o.o. U.I. INFO-SYSTEM Sp.J.
16.	Zaopatrzenie ludności w wodę i kanalizację	Papierowa/elektroniczna	WODA	U.I. INFO-SYSTEM Sp. J.
17.	Ustalenie warunków zabudowy i zagospodarowania terenu	Papierowa	N/D	N/D
18.	Numeracja porządkowa nieruchomości	Papierowa/elektroniczna	eGmina iMPA	PUH „GEO-SYSTEM" Sp. z o.o.
19.	Opłaty komunalne	Papierowa/elektroniczna	KSZOB	U.I. INFO-SYSTEM Sp. J.
20.	Decyzje zatwierdzające projekt podziału nieruchomości	Papierowa/elektroniczna	N/D	N/D
21.	Podatki i opłaty lokalne	Papierowa/elektroniczna	Podatki,	U.I. Infosystem
22.	Umowy przekazanych gospodarstw rolnych	Papierowa	N/D	N/D
23.	Zezwolenia na sprzedaż napojów alkoholowych	Papierowa	N/D	N/D
24.	Rejestr osób korzystających z dodatków mieszkaniowych	Papierowa	N/D	N/D

25.	Akta Stanu Cywilnego	Papierowa/ elektroniczna	USCWIN	ARAM S.C.
26.	Ewidencja Ludności i wyborców Gminy Turośl	Papierowa/ elektroniczna	SELWIN/RWWIN	ARAM S.C.
27.	Dane osobowe i ubezpieczeniowe pracowników	Papierowa/ elektroniczna	Płatnik/Druki IPS	Prokom S.A. Przedsiębiorstwo Informatyczne IPS
28.	Teczki Osobowe pracowników	Papierowa/ Elektroniczna	Druki IPS	Przedsiębiorstwo Informatyczne IPS
29.	Dane płacowe	Papierowa/ elektroniczna	Płace	U.I. Infosystem
30.	Dowody osobiste	Papierowa/ elektroniczna	Dowody osobiste (ŹRÓDŁO)	MSWIA
31.	Świadczenia Osobiste i Rzeczowe na rzecz obrony	papierowa	N/D	N/D
32.	Zezwolenia na wycinkę drzew	papierowa	N/D	N/D

WÓJT
mgr Piotr Niedbała

Załącznik Nr 3
do Polityki Bezpieczeństwa

Opis struktury zbiorów danych osobowych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między zbiorami

Przetwarzanie odbywa się częściowo na serwerze, częściowo na stacjach roboczych użytkowników (dostęp możliwy wyłącznie ze specjalizowanego oprogramowania klienckiego).

SWDO (System Wydawania Dowodów Osobistych) jest obsługiwany poprzez aplikację ŹRÓDŁO przez dedykowaną sieć komputerową. Dostęp mają osoby upoważnione przez MSWiA i posiadające karty chipowe.

L.p	Nazwa zbioru	Zawartość zbioru
1.	Rejestr skarg i wniosków	Imię i nazwisko, dane adresowe, kontaktowe
2.	Ewidencja radnych	Imię i nazwisko, dane adresowe, kontaktowe
3.	Oświadczenia majątkowe	dane adresowe oraz miejsce położenia innych posiadanych nieruchomości. - Sytuacja majątkowa, posiadane zasoby pieniężne, ruchomości, nieruchomości, prawa majątkowe, pieniężne, miejsca zatrudnienia, źródła dochodów.
4.	Archiwum zakładowe	Imię i nazwisko, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, numer PESEL, NIP, miejsce pracy, zawód, wykształcenie, seria i numer dowodu osobistego, numer telefonu
5.	Ewidencja upomnień i tytułów wykonawczych	Struktura zbioru zawiera dane niezbędne do ustalenia zobowiązania podatkowego podatnika gminy : - imię i nazwisko, dane adresowe, PESEL, REGON, NIP, własność nieruchomości,
6.	Ochotnicza Straż Pożarna	Imię i nazwisko, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, numer PESEL, seria i numer dowodu osobistego, numer telefonu

7.	Rejestracja i kwalifikacja wojskowa	Struktura zbioru zawierająca informacje osób podlegających stawiennictwu do kwalifikacji wojskowej : - imię i nazwisko, nazwisko rodowe, miejsce urodzenia, dane adresowe, nr pesel, seria i numer dowodu osobistego,
8.	Zwrot podatku akcyzowego	Imię i nazwisko, , data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, numer PESEL, seria i numer dowodu osobistego, numer telefonu
9.	Podatek od środków transportowych	Imię i nazwisko, imiona rodziców, data urodzenia, adres zamieszkania lub pobytu, numer PESEL, NIP, seria i numer dowodu osobistego, numer telefonu
10.	Zaświadczenia w sprawach podatkowych	Imię i nazwisko, imiona rodziców, data urodzenia, adres zamieszkania lub pobytu, numer PESEL, NIP, wielkość gospodarstwa, członkowie rodziny, dochód z gospodarstwa
11.	Ewidencja działalności gospodarczej	Nazwa firmy, imię nazwisko, dane adresowe, telefon, NIP, REGON, seria i nr dowodu osobistego, kod PKD
12.	Ustalenie lokalizacji inwestycji celu publicznego	Imię i nazwisko, adres zamieszkania lub pobytu, numer telefonu
13.	Zaświadczenia o przeznaczeniu terenu w planie zagospodarowania przestrzennego	Imię i nazwisko, adres zamieszkania lub pobytu, numer telefonu
14.	Zajęcie pasa drogowego	Imię i nazwisko, adres zamieszkania lub pobytu, numer telefonu
15.	Czystość i porządek	Imię i nazwisko, adres zamieszkania lub pobytu, numer telefonu, informacje o zawartej umowie na wywóz odpadów stałych Szczegółowy opis struktury danych systemu komputerowego używanego do przetwarzania danych (GOMIG oraz KSZOB)jest przedstawiony w załączniku Nr 4.
16.	Zaopatrzenie ludności w wodę i kanalizację	Imię i nazwisko, adres zamieszkania lub pobytu, numer ewidencyjny nieruchomości

WÓJT
mgr Piotr Niedbała

		Szczegółowy opis struktury danych systemu komputerowego używanego do przetwarzania danych (WODA, Rejestr VAT, KSZOB)jest przedstawiony w załączniku Nr 4.
17.	Ustalenie warunków zabudowy i zagospodarowania terenu	Imię i nazwisko, adres zamieszkania lub pobytu, numer telefonu
18.	Numeracja porządkowa nieruchomości	Imię i nazwisko, adres nieruchomości, dane kontaktowe.
19.	Odpady komunalne	Imię i nazwisko, Pesel, adres zamieszkania lub pobytu, adres nieruchomości, nr telefonu, Liczba osób zamieszkujących
20.	Decyzje zatwierdzające projekt podziału nieruchomości	Imię i nazwisko, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, numer PESEL, miejsce pracy, zawód, wykształcenie, seria i numer dowodu osobistego
21.	Podatki i opłaty lokalne	imię i nazwisko, dane adresowe, PESEL, data urodzenia, seria i nr dowodu osobistego telefon, e-mail, nr KW, własność nieruchomości według numerów nieruchomości,
22.	Umowy przekazanych gospodarstw rolnych	Imię i nazwisko, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, numer PESEL, seria i numer dowodu osobistego
23.	Zezwolenia na sprzedaż napojów alkoholowych	Imię i nazwisko, adres zamieszkania lub pobytu, numer NIP, numer telefonu, Adres wykonywania działalności gospodarczej, numer KRS lub wpis do ewidencji działalności gospodarczej
24.	Rejestr osób korzystających z dodatków mieszkaniowych	Imię i nazwisko, imiona rodziców , data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, numer PESEL, miejsce pracy, seria i numer dowodu osobistego, informacja o dochodach i wydatkach na utrzymanie lokalu, akt własności, zaświadczenie o powierzchni lokalu i stanie majątkowym
25.	Akta Stanu Cywilnego	<u>Akty urodzenia:</u> System zawiera dane osobowe dotyczące urodzeń, uzupełnienia i aktualizację danych w księgach stanu cywilnego. Struktura zbioru zawiera:

		- imię i nazwisko dziecka, miejsce urodzenia, godzina urodzenia, płeć dziecka, imię i nazwisko rodowe ojca dziecka, imię i nazwisko rodowe matki dziecka, nr pesel rodziców, seria i nr dowodu osobistego rodziców, daty i miejsca urodzenia rodziców dziecka, miejsca zamieszkiwania rodziców dziecka, dane osobowe osoby zgłaszającej urodzenie, wzmianki dodatkowe, przypiski. <u>Akty małżeństwa:</u> Struktura zbioru zawiera informacje dotyczącą aktów małżeństwa oraz aktualizację i uzupełnienia danych w księgach stanu cywilnego: - nr pesel, seria i nr dowodu osobistego, imiona i nazwiska małżonków, nazwiska rodowe, daty urodzenia, miejsce zamieszkania, data zawarcia związku małżeńskiego, nazwiska i nazwiska rodowe rodziców, nazwiska noszone po zawarciu związku małżeńskiego, adnotacje o ustaniu, unieważnieniu małżeństwa lub separacji, nazwiska i imiona świadków, wzmianki dodatkowe, przypiski. <u>Akty zgonu:</u> Struktura zbioru zawiera informacje dotyczące zgonów oraz zmiany, uzupełnienia i aktualizacje danych w księgach stanu cywilnego: - nr pesel, seria i nr dowodu osobistego, nazwisko i imię zmarłego, nazwisko rodowe zmarłego, stan cywilny, data urodzenia, miejsce urodzenia, ostatnie miejsce zamieszkania, data, godzina i miejsce zgonu, data, godzina i miejsce znalezienia zwłok, nazwisko i imię oraz nazwisko rodowe małżonka osoby zmarłej, imię i nazwisko rodowe ojca osoby zmarłej, imię i nazwisko rodowe matki osoby zmarłej, dane dotyczące osoby zgłaszającej zgon, wzmianki dodatkowe, przypiski.
26.	Ewidencja Ludności i wyborców Gminy Turośl	imię i nazwisko, nazwisko rodowe, imię i nazwisko rodowe ojca, imię i nazwisko rodowe matki, stałe miejsce zamieszkania, czasowe miejsce zamieszkania, nr pesel, seria i nr dowodu osobistego, data wymeldowania, data i miejsce zawarcia związku małżeńskiego, adnotacje o rozwodzie, adnotacja o zgonie, adnotacja o zmianie imion i nazwisk.

27.	Dane osobowe i ubezpieczeniowe pracowników	Imię i nazwisko, imiona rodziców, dane członków rodziny, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, numer PESEL, seria i numer dowodu osobistego, dane o okresach pracy, kwoty składek ubezpieczeniowych
28.	Teczki Osobowe pracowników	- imię i nazwisko, data i miejsce urodzenia, imiona rodziców, stopień niepełnosprawności, dane adresowe, imiona rodziców, nr pesel, nr NIP, miejsce zatrudnienia, staż pracy, wynagrodzenie, premie, dodatek z tytułu lat pracy, urlopy, zwolnienia lekarskie, awans zawodowy, dane o otrzymanych nagrodach, karach i odznaczeniach, składniki wynagrodzenia, potrącenia z wynagrodzeń, nr konta osobistego, wykształcenie, badania lekarskie, szkolenia
29.	Dane płacowe	imię i nazwisko, data i miejsce urodzenia, imiona rodziców, stopień niepełnosprawności, dane adresowe, imiona rodziców, nr pesel, nr NIP, miejsce zatrudnienia, staż pracy, wynagrodzenie, premie, dodatek z tytułu lat pracy, urlopy, zwolnienia lekarskie, awans zawodowy, dane o otrzymanych nagrodach, karach i odznaczeniach, składniki wynagrodzenia, potrącenia z wynagrodzeń, nr konta osobistego, wykształcenie, badania lekarskie, szkolenia
30.	Dowody osobiste	nr pesel, imię i nazwisko, nazwisko rodowe, data i miejsce urodzenia, seria i nr dowodu osobistego, miejsce zamieszkania stałe i czasowe, data i miejsce zawarcia związku małżeńskiego.
31.	Świadczenia Osobiste i Rzeczowe na rzecz obrony	Imię i nazwisko, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, miejsce pracy, zawód, seria i numer dowodu osobistego, numer telefonu, rodzaj przeznaczonych świadczeń
32.	Zezwolenia na wycinkę drzew	Imię i nazwisko adres zamieszkania lub pobytu, własność nieruchomości

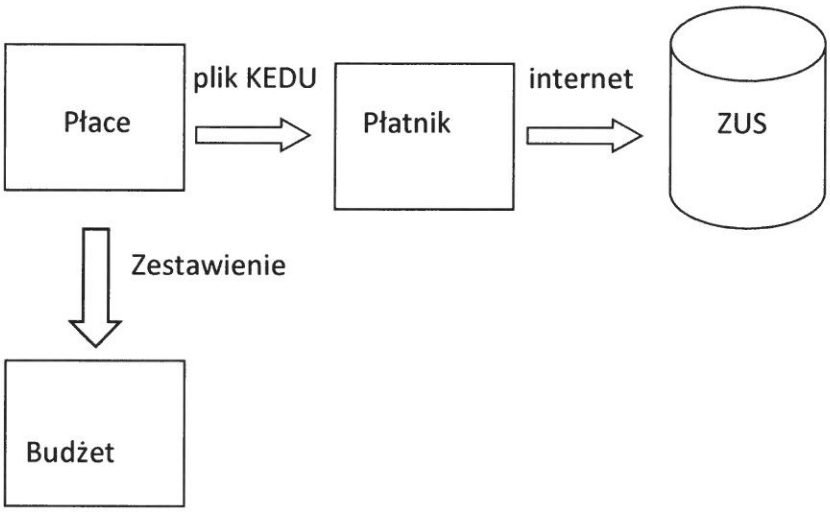
WÓJT
mgr Piotr Niedbała

Załącznik Nr 4
do Polityki Bezpieczeństwa

Przepływ danych pomiędzy poszczególnymi systemami

1. System **Płace – Płatnik – Budżet**

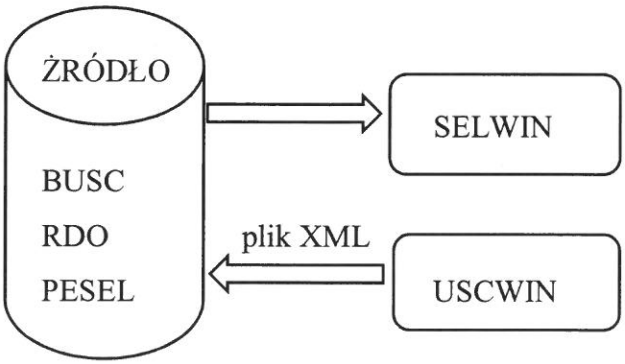
   Z systemu Płace do Programu Płatnik eksportowane są dane w postaci pliku KEDU. Transmisja danych do ZUS odbywa się przez teletransmisję, poprzez SDWI z wykorzystaniem certyfikatu kwalifikowanego. Do programu Budżetowego dane przekazywane są w formie zestawień papierowych zawierającej jedynie dane liczbowe.



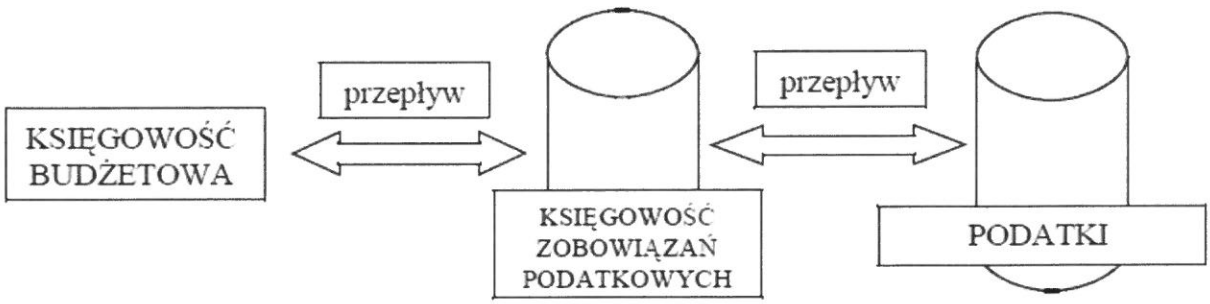
2. System **Źródło–Selwin-USCWIN**

   Źródło–Selwin moduły sytemu komunikują się wewnątrz odrębnej sieci zarządzanej przez MSW w ramach projektu Źródło. System SELWIN jest zASTlany danymi z rejestru PESEL.

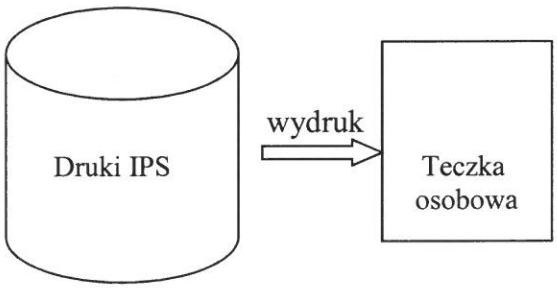
   Program USCWIN może zasilić zgromadzonymi danymi system BUSC, poprzez eksport do pliku XML i zaczytanie go w systemie ŹRÓDŁO.



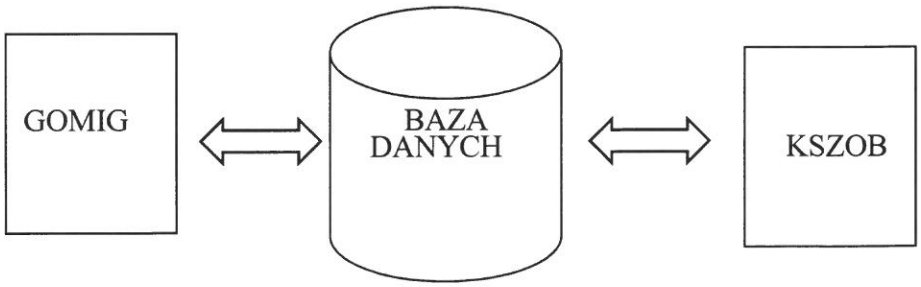
3. **System Podatki/AUTA/ Księgowość Podatkowa/księgowość Budżetowa**
   Przepływ danych między systemem podatków i opłat a systemem księgowym, odbywa się w wersji papierowej. Elektronicznie dane wprowadzane są do systemu podatków i opłat przez pracowników merytorycznych i przekazywane do system księgowości zobowiązań podatkowych w postaci elektronicznej.
   Z systemu księgowości podatkowej dane przekazywane są w postaci papierowej do księgowości budżetowej gdzie pracownik merytoryczny wprowadza dane do systemu.



4. **Druki IPS - umowy o pracę i świadectwa pracy**

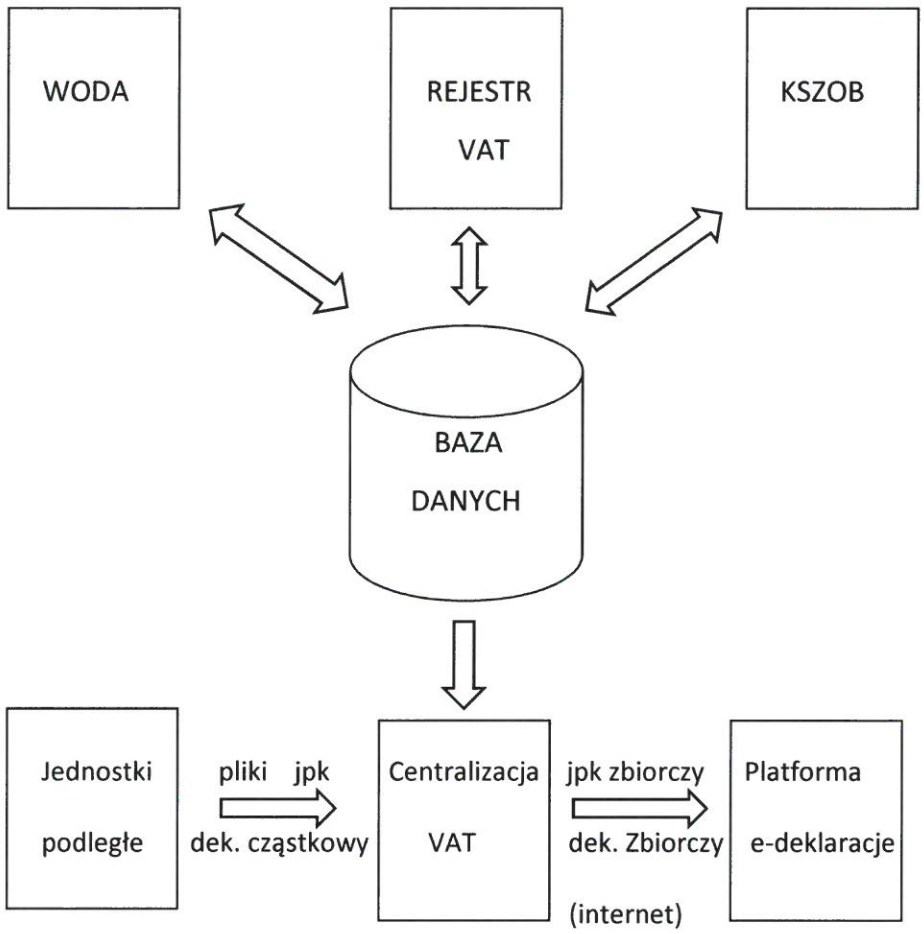


5. **GOMIG – KSZOB**



6. **WODA-REJESTR VAT – KSZOB - Centralizacja VAT**

Wymiana plików odbywa się w sieci lokalnej poprzez dysk sieciowy



Załącznik Nr 5
do Polityki Bezpieczeństwa

Oświadczenie
osoby upoważnionej do przetwarzania danych osobowych

Ja niżej podpisany/na oświadczam, że:

1) przed uzyskaniem dostępu do danych osobowych zapoznałem się z przepisami dotyczącymi ochrony danych osobowych, w szczególności:
   a) z ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U.2016.922 t.j. z pózn. zm.),
   b) rozporządzeniem 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);
   c) Zarządzeniem ..... roku w sprawie wprowadzenia Polityki Bezpieczeństwa przetwarzania danych osobowych oraz Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Turośl,
2) znana jest mi treść art. 6 ustawy o ochronie danych osobowych, zgodnie z którym za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
3) potwierdzam fakt odbycia szkolenia z ochrony danych osobowych;
4) zobowiązuję się do przestrzegania przepisów o ochronie danych osobowych, w tym w szczególności do niedokonywania bez upoważnienia: odczytu, modyfikacji, powielania, usuwania, zapisywania na nośnikach oraz przekazywania danych w dowolnej formie;
5) mam świadomość ciążącego na mnie obowiązku zachowania w tajemnicy, w okresie zatrudnienia oraz po ustaniu zatrudnienia, danych osobowych, do których uzyskam dostęp oraz sposobów ich zabezpieczenia;
6) przyjmuję do wiadomości, że niedotrzymanie powyższych zobowiązań będzie stanowiło naruszenie przepisów karnych ustawy o ochronie danych osobowych oraz podstawowych obowiązków pracowniczych i dlatego spowoduje skierowanie zawiadomienia o podejrzeniu popełnienia przestępstwa oraz/lub rozwiązanie umowy o pracę lub innej umowy cywilnoprawnej.

.....

(podpis osoby upoważnionej do przetwarzania danych)

WÓJT
mgr Piotr Niedbal

Załącznik Nr 6
do Polityki Bezpieczeństwa

EWIDENCJA NARUSZEŃ BEZPIECZEŃSTWA

Naruszenie bezpieczeństwa/ incydent	Źródło zgłoszenia	Data rozpoczęcia	Data zakończenia	Osoba odpowiedzialna	Przyczyna	Podjęte działania	Uwagi/ocena skuteczności

WÓJT
mgr Piotr Niedbała