Załącznik Nr 2 do Zarządzenia Nr 6/2015
z dnia 3 kwietnia 2015r.

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH

W STAROSTWIE POWIATOWYM
W NOWYM TOMYŚLU

OPRACOWAŁ

Administrator Bezpieczeństwa Informacji

§ 1.
POSTANOWIENIA OGÓLNE

1. Instrukcja określa zasady zarządzania systemem informatycznym służącym do przetwarzania danych osobowych zgodnie ze strategią określoną w „Polityce bezpieczeństwa w Starostwie Powiatowym w Nowym Tomyślu" wprowadzoną w życie zarządzeniem nr OG.120.6.2015 Starosty Nowotomyskiego z dnia 3 kwietnia 2015r. oraz postanowień rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024).
2. Instrukcja zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych w Starostwie Powiatowym w Nowym Tomyślu, określa:
   1) zasady, tryb postępowania i zalecenia Administratora Danych Osobowych, które należy stosować w trakcie przetwarzania danych osobowych w systemach informatycznych;
   2) sposób przydziału haseł dla użytkowników i częstotliwość ich zmiany oraz osoby odpowiedzialne za te czynności;
   3) sposób rejestrowania i wyrejestrowywania użytkowników oraz osoby odpowiedzialne za te czynności;
   4) zasady i procedury rozpoczynania i kończenia pracy;
   5) zasady i częstotliwość tworzenia kopii bezpieczeństwa;
   6) zasady i częstotliwość kontroli obecności wirusów komputerowych oraz metodę ich usuwania;
   7) zasady i czas przechowywania nośników informacji, w tym kopii informatycznych;
   8) zasady dokonywania przeglądów i konserwacji systemu i zbioru danych osobowych;
   9) zasady postępowania w zakresie komunikacji w sieci komputerowej.

3. Instrukcja opracowana została zgodnie z wymogami § 5 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych w systemach informatycznych.

§ 2.
DEFINICJE ZAWARTE W INSTRUKCJI

1. Słownik pojęć:
   1) **ustawa,** zwana dalej **ustawą** - rozumie się przez to ustawę z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U. z 2014r., poz. 1182);
   2) **jednostka** – rozumie się przez to Starostwo Powiatowe w Nowym Tomyślu;
   3) **system informatyczny**, zwany dalej **systemem** - to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych wraz z pracownikami upoważnionymi do obsługi systemu, który dostarcza i rozprowadza informacje;
   4) **użytkownik systemu** - rozumie się przez to upoważnioną przez Starostę Nowotomyskiego - kierownika jednostki, pracownika do przetwarzania danych osobowych w systemie informatycznym, który odbył stosowne szkolenie w zakresie ochrony danych;
   5) **identyfikator użytkownika** - rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
   6) **hasło** - rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;
   7) **sieć lokalna, LAN** – należy przez to rozumieć połączenie systemów informatycznych Starostwa wyłącznie dla własnych jej potrzeb przy wykorzystaniu urządzeń i sieci telekomunikacyjnych;
   8) **sieć telekomunikacyjna** - rozumie się przez to sieć telekomunikacyjną w rozumieniu art. 2 pkt 35 ustawy z dnia 16 lipca 2004r. - Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800, z późn. zm.);
   9) **sieć publiczna** - rozumie się przez to sieć publiczną w rozumieniu art. 2 pkt 29 ustawy z dnia 16 lipca 2004r. - Prawo telekomunikacyjne;
   10) **system informatyczny** to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i urządzeń programowych zastosowanych w celu przetwarzania danych;
   11) **teletransmisja, transmisja danych** - rozumie się przez to przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej lub lokalnej;

12) **integralność danych** - rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
13) **poufność danych** - rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom;
14) **uwierzytelnianie** - rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości użytkownika systemu;
15) **Administrator Danych (AD)** - w świetle przepisów ustawy o ochronie danych osobowych, art. 3 i 7 pkt 4 rozumie się przez to kierownika jednostki - Starostę Nowotomyskiego, który decyduje o celach i środkach przetwarzania danych osobowych;
16) **Administrator Bezpieczeństwa Informacji (ABI)** - rozumie się przez to osobę wyznaczoną przez Administratora Danych (kierownika jednostki), nadzorującą przestrzeganie zasad ochrony danych osobowych, w szczególności zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem;
17) **Administrator Systemu Informatycznego (ASI),** zwany też **Administratorem Systemu** - rozumie się przez to osobę zatrudnioną przez Starostę Nowotomyskiego - kierownika jednostki, upoważnioną do realizacji zadań związanych z zarządzaniem systemem informatycznym.

§ 3.
ZASADY DOSTĘPU UŻYTKOWNIKA DO SYSTEMU

1. Dostęp do systemu informatycznego służącego do przetwarzania danych osobowych, może uzyskać wyłącznie osoba (użytkownik) zarejestrowana w tym systemie przez Administratora Systemu na wniosek kierownika komórki organizacyjnej i po akceptacji Administratora Bezpieczeństwa Informacji,
2. Rejestracja, o której mowa w ust. l, polega na nadaniu identyfikatora i przydziale hasła oraz wprowadzeniu tych danych do bazy użytkowników systemu,
3. Każdy użytkownik systemu przed przystąpieniem do przetwarzania danych osobowych musi zapoznać się z:

1) Ustawą o ochronie danych osobowych z dnia 29 sierpnia 1997r. (Dz. U. z 2014r., poz. 1182),
2) Zarządzeniem nr OG.120.6.2015 Starosty Nowotomyskiego z dnia 3 kwietnia 2015r. w sprawie ustalenia Polityki bezpieczeństwa w Starostwie Powiatowym w Nowym Tomyślu,
3) Niniejszą instrukcją.

§ 4.
PROCEDURA NADAWANIA UPRAWNIEŃ DO PRZETWARZANIA DANYCH OSOBOWYCH

1. Administrator Danych:
   1) przyznaje uprawnienia na wniosek kierownika komórki organizacyjnej, a Administrator Systemu Informatycznego przyznaje uprawnienia w zakresie dostępu do systemu informatycznego na podstawie pisemnego upoważnienia (wniosku) określającego zakres uprawnień pracownika, którego wzór stanowi **załącznik nr 1**, z wyłączeniem osób kierujących Starostwem,
   2) podpisuje dokument uprawnień dla osoby upoważnionej do przetwarzania danych osobowych w systemie informatycznym Starostwa.
2. ASI zgodnie z przekazanym dokumentem:
   1) rejestruje użytkownika w systemie i nadaje mu określone uprawnienia,
   2) opatruje otrzymany od ABI dokument uprawnień swoim podpisem i datą.
3. ABI aktualizuje ewidencję, i przekazuje informację o zarejestrowaniu użytkownika w systemie kierownikowi komórki organizacyjnej.
4. Użytkownik systemu w obecności ASI uwierzytelnia się w systemie.
5. Użytkownik zmienia nadane mu przez ASI hasło i rozpoczyna pracę w aplikacji.
6. Użytkownik systemu loguje się i po ustaleniu znanego tylko jemu hasła, przekazuje je w zamkniętej kopercie ASI.
7. Wszelkie zmiany uprawnień do systemu zawierającego dane osobowe są ustanawiane na wniosek kierownika komórki organizacyjnej i kierowane do ABI.

§ 5.
METODY I ŚRODKI UWIERZYTALNIANIA

1. W systemie informatycznym Starostwa Powiatowego w Nowym Tomyślu stosuje się metody uwierzytelniania dostępu:
   1) stacji komputerowej z poziomu BIOS,
   2) do sieci lokalnej,
   3) do aplikacji.
2. Do uwierzytelniania użytkownika w systemie we wszystkich poziomach stosuje się hasła.
3. Identyfikator użytkownika nadawany jest na poziomie autoryzacji w sieci oraz aplikacji.
4. Bezpośredni dostęp do danych osobowych uzyskuje się wyłącznie po podaniu właściwego identyfikatora i hasła.
5. Identyfikator powinien składać się z min. 5znaków, a przypadku jego zbieżności z identyfikatorem wcześniej zarejestrowanego użytkownika Administrator Systemu po uzgodnieniu z ABI nadaje inny identyfikator.
6. W identyfikatorze pomija się polskie znaki diakrytyczne i znaki specjalne.
7. Hasło użytkownika do zasobów sieciowych (jeśli system posiada odpowiedni mechanizm) zmienia się raz na miesiąc.
8. Hasło na poziomie dostępu do aplikacji i sieci składa się co najmniej z 8 znaków, zawiera małe i wielkie litery oraz cyfry lub znaki specjalne.
9. Hasła nie mogą być powszechnie używanymi słowami. W szczególności nie należy jako haseł wykorzystywać: identyfikatorów, dat, imion, nazwisk, inicjałów, numerów rejestracyjnych samochodów, numerów telefonów.
10. Hasło użytkownika systemu przy wpisywaniu nie może być wyświetlone na ekranie i musi być utrzymywane w tajemnicy zarówno w trakcie jego użytkowania jak również po upływie jego ważności.
11. Zmiana hasła do systemu następuje również w przypadku podejrzenia, że hasło mogło zostać ujawnione lub w sytuacji gdy użytkownik zapomniał swojego hasła.
12. Identyfikator użytkownika systemu nie powinien być zmieniany, a po jego wyrejestrowaniu z systemu informatycznego nie jest przydzielany innej osobie.

13. Czas pracy i ewentualne przerwy w pracy w systemie informatycznym dla poszczególnych użytkowników systemu ustalają kierownicy komórek organizacyjnych. Natomiast na pracę w systemie informatycznym poza godzinami funkcjonowania Starostwa musi wyrazić zgodę Administrator Danych.
14. Użytkownik systemu przed opuszczeniem stanowiska pracy zobowiązany jest do zakończenia pracy w tym systemie, polega to na wyjściu/wylogowaniu się z wszystkich otwartych aplikacji i zasobów sieciowych.
15. W przypadku czasowego opuszczenia stanowiska komputerowego pracownik powinien uruchomić wygaszacz ekranu zabezpieczony hasłem lub system sam wymusi jego start po 15 minutach.
16. Użytkownicy posiadający systemy, które mają dostęp do danych osobowych ustawiają monitory/ekrany w ten sposób, żeby uniemożliwić osobom postronnym wgląd w te dane.

§ 6.
WYREJESTROWANIE UŻYTKOWNIKA

1. Wyrejestrowania użytkownika z systemu informatycznego dokonuje Administrator Systemu Informatycznego na wniosek Administratora Bezpieczeństwa Informacji.
2. Wyrejestrowanie, o którym mowa w ust. 1, może mieć charakter czasowy lub trwały.
3. Wyrejestrowanie następuje poprzez:
   1) zablokowanie konta użytkownika do czasu ustania przyczyny uzasadniającej blokadę (wyrejestrowanie czasowe - zawieszenie),
   2) zawieszenie trwałe konta użytkownika (konto i jego historia zostaje w systemie lecz następuje jego dezaktywacja).
4. Przyczyną czasowego wyrejestrowania użytkownika z systemu informatycznego jest:
   1) nieobecność w pracy trwająca dłużej niż 31 dni kalendarzowych,
   2) zawieszenie w pełnieniu obowiązków służbowych,
   3) zwolnienie z pełnienia obowiązków służbowych.
5. Przyczyną trwałego wyrejestrowania użytkownika z systemu informatycznego jest rozwiązanie lub wygaśnięcie stosunku pracy użytkownika.
6. Wyrejestrowanie użytkownika z systemu informatycznego dokonuje Administrator Systemu na wniosek ABI, **załącznik nr 1**, z podaniem daty oraz przyczyny odebrania uprawnień.

7. Administrator Bezpieczeństwa Informacji zobowiązany jest do prowadzenia i ochrony rejestru użytkowników wraz z ich uprawnieniami, rejestr stanowi **załącznik nr 2**.

§ 7.
ROZPOCZĘCIE PRACY W SYSTEMIE SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH

1. Rozpoczęcie pracy w systemie przetwarzającym dane osobowe odbywa się poprzez:
   1) przygotowanie stanowiska pracy,
   2) włączenie stacji roboczej,
   3) wprowadzenie swoich identyfikatorów i haseł w zależności od ustalonych poziomów dostępu i charakteru wykonywanej pracy.

§ 8.
ZAWIESZENIE PRACY W SYSTEMIE SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH

1. W trakcie pracy, przy każdorazowym opuszczeniu stanowiska komputerowego, użytkownik zobowiązany jest dopilnować, aby na ekranie nie były wyświetlane dane osobowe.
2. Przy opuszczaniu pomieszczenia użytkownik powinien uruchomić wygaszacz ekranu.

§ 9.
ZAKOŃCZENIE PRACY W SYSTEMIE SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH

1. Zakończenie pracy w systemie odbywa się poprzez:
   1) zamknięcie aplikacji,
   2) wylogowanie się z zasobów sieciowych,
   3) zamknięcie systemu operacyjnego,
   4) wyłączenie stacji roboczej, monitora, UPS'a i innych urządzeń peryferyjnych.

§ 10.

ZASADY PRACY W SYSTEMIE SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH

1. Zabrania się użytkownikom pracującym w systemie:
   1) udostępniania stacji roboczej osobom niezarejestrowanym z zastrzeżeniem pkt 2,
   2) udostępniania stacji roboczej do konserwacji lub naprawy bez porozumienia z Administratorem Systemu Informatycznego,
   3) instalowania i używania nielicencjonowanego oprogramowania.

§ 11.

NARUSZENIE BEZPIECZEŃSTWA W SYSTEMIE SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH

1. Każdy przypadek naruszenia ochrony danych osobowych lub przesłanki, które mogą wskazywać na naruszenie bezpieczeństwa podlegają zgłoszeniu do Administratora Bezpieczeństwa Informacji, a w szczególności:
   1) naruszenia bezpieczeństwa systemu informatycznego,
   2) stwierdzenia objawów (stanu urządzeń, sposobu działania programu lub jakości komunikacji w sieci).
2. Administratorowi Bezpieczeństwa Informacji zgłasza się w szczególności przypadki:
   1) użytkowania stacji roboczej przez osobę nie będącą użytkownikiem systemu,
   2) usiłowania logowania się do systemu (sieci) przez osobę nieuprawnioną,
   3) usuwania, dodawania lub modyfikowania bez wiedzy i zgody użytkownika jego dokumentów, plików i baz danych,
   4) przebywania osób nieuprawnionych w obszarze, w którym przetwarzane są dane osobowe, w trakcie nieobecności osoby zatrudnionej przy przetwarzaniu tych danych i bez zgody Administratora Danych (pozostawiania bez nadzoru otwartych pomieszczeń, w których przetwarzane są dane osobowe),
   5) udostępniania osobom nieuprawnionym stacji roboczej lub komputera przenośnego, służących do przetwarzania danych osobowych,

6) niezabezpieczenia hasłem dostępu do komputera służącego do przetwarzania danych osobowych,
7) przechowywania kopii awaryjnych w tych samych pomieszczeniach, w których przechowywane są zbiory danych osobowych eksploatowane na bieżąco,
8) przechowywania nośników informacji oraz wydruków z danymi osobowymi, w warunkach umożliwiających do nich dostęp osobom nieuprawnionym.

3. Obowiązek dokonania zgłoszenia, o którym mowa w ust 1, spoczywa na każdym użytkowniku, który powziął wiadomość o naruszeniu ochrony danych osobowych.
4. W przypadku naruszenia integralności bezpieczeństwa sieciowego, obowiązkiem Administratora Systemu jest natychmiastowe wstrzymanie udostępniania zasobów dla użytkowników i odłączenie serwerów od sieci.
5. Użytkownik sieci i Administrator Systemu w porozumieniu z Administratorem Bezpieczeństwa Informacji ustalają przyczyny naruszenia integralności bezpieczeństwa sieciowego.
6. Przywrócenie udostępniania zasobów użytkownikom może nastąpić dopiero po ustaleniu i usunięciu przyczyny naruszenia integralności bezpieczeństwa sieciowego.

§ 12.
KOPIE ZAPASOWE

1. Obowiązek tworzenia kopii awaryjnych danych (plików, aplikacji i baz danych) przechowywanych na dyskach lokalnych stacji roboczych, mają użytkownicy pracujący na przypisanych do nich komputerach.
2. Kopie o których mowa w ust.1 są tworzone przez użytkowników na płytach CD lub innych zarejestrowanych przez ABI nośnikach danych i przechowywane w odpowiednio do tego przeznaczonych zamkniętych szafach.
3. Obowiązek tworzenia kopii awaryjnych danych (plików, aplikacji i baz danych) znajdujących się na zasobach sieciowych Starostwa Powiatowego w Nowym Tomyślu ma ASI.
4. Kopie awaryjne, przyrostowe całego sieciowego systemu operacyjnego każdego z serwerów znajdujących się w pok. 3a w budynku „C" przeprowadzane są automatycznie raz w tygodniu na zewnętrznej macierzy danych znajdującej się w tym samym pomieszczeniu.

5. ASI wykonuje ręcznie dodatkowe kopie zapasowe w odstępach 2-3 dniowych samych baz danych z serwerów znajdujących się w pok. 3a w budynku „C" i umieszcza je na zewnętrznych dyskach sieciowych znajdujących się w szafach krosowniczych w budynkach „E" pok. 27 i „D" w pokoju nr 10.
6. Sporządzone kopie awaryjne (jeśli umożliwia to dostawca aplikacji i oprogramowania) są okresowo sprawdzane pod kątem dalszej ich przydatności do odtworzenia danych w przypadku awarii systemu.
7. Kopie awaryjne, po utracie przydatności są bezzwłocznie usuwane.
8. W przypadku uszkodzenia lub zużycia nośnika zawierającego dane osobowe należy fizycznie zniszczyć nośnik.
9. Sporządzanie kopii zapasowych obejmujących systemy informatyczne znajdujące się w budynku „F" przy ul. Poznańskiej 42, a realizujących zadania Powiatowego Ośrodka Dokumentacji Geodezyjnej i Kartograficznej wykonywane są w sposób następujący:
   1) pełne kopie zapasowe baz danych sql systemów do prowadzenia zasobu geodezyjnego i kartograficznego – automatycznie przez kontroler domenowy przeprowadzane codziennie w godzinach 16:00 - 17:00 – zasoby znajdują się na serwerze znajdującym się w tym samym pomieszczeniu tj. pokoju 2,
   2) kopie danych z ust. 9 pkt. 1 kopiowane są w sposób automatyczny na zewnętrzną macierz dyskową, zlokalizowaną w szafie krosowniczej w budynku „E" pok. 27 w godzinach 18:00 - 19:00.

§ 13.
OCHRONA ANTYWIRUSOWA

1. Sprawdzanie obecności wirusów komputerowych w systemie oraz ich usuwanie odbywa się przy wykorzystaniu licencjonowanego oprogramowania w oparciu o serwer dystrybucji aktualnych sygnatur i wersji oprogramowania.
2. Oprogramowanie antywirusowe zainstalowane jest na wszystkich stacjach roboczych w sieci lokalnej oraz w zaporze sieciowej firewall.
3. Oprogramowanie, o którym mowa w ust. 1 i 2, sprawuje ciągły nadzór (ciągła praca w tle) nad pracą systemu i jego zasobami oraz serwerami i stacjami roboczymi.
4. Do obowiązków Administratora Systemu należy aktualizacja oprogramowania służącego do sprawdzania w systemie obecności wirusów komputerowych.

§ 14.
ZASILANIE AWARYJNE

1. System i urządzenia informatyczne służące do przetwarzania danych osobowych, zasilane energią elektryczną, zabezpiecza się przed utratą danych osobowych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.
2. Minimalne zabezpieczenie systemu i urządzeń informatycznych, o których mowa w ust. 1, polega na wyposażeniu serwera (serwerów) oraz wybranych stacji roboczych w zasilacze awaryjne (UPS).

§ 15.
NAPRAWA, SERWIS URZĄDZEŃ

1. Urządzenia informatyczne służące do przetwarzania danych osobowych można przekazać do naprawy, konserwacji lub likwidacji dopiero po uprzednim uzyskaniu zgody Administratora Bezpieczeństwa Informacji.
2. Urządzenia, o których mowa w ust. l przed ich przekazaniem pozbawia się zapisu danych osobowych poprzez wymontowanie dysku twardego z zastrzeżeniem ust. 3.
3. Jeżeli nie jest to możliwe, urządzenie to może być naprawiane wyłącznie pod nadzorem Administratora Systemu.
4. Jeżeli nie jest możliwe pozbawienie urządzenia przekazywanego do likwidacji zapisu danych osobowych, należy je przed przekazaniem uszkodzić w sposób uniemożliwiający odczytanie z niego danych.

§ 16.
PRZEGLĄD I KONSERWACJE

1. Przeglądu i konserwacji systemu dokonuje doraźnie Administrator Systemu.
2. Przeglądu i sprawdzenia poprawności zbiorów danych zawierających dane osobowe dokonuje użytkownik przy współudziale Administratora Systemu w sytuacji wątpliwości co do ich poprawnego działania oraz po aktualizacjach aplikacji.

3. Ewentualne błędy baz danych są niezwłocznie usuwane przez ASI lub opiekunów technicznych danej aplikacji.
4. W przypadku działań konserwacyjnych, awarii oraz napraw ASI prowadzi „Dziennik systemu informatycznego Starostwa Powiatowego w Nowym Tomyślu **załącznik nr 3.**

§ 17.
BEZPIECZEŃSTWO KOMUNIKACJI

1. Bezpieczeństwo komunikacji w obrębie systemów przetwarzających dane osobowe Administrator Systemu zapewnia przy użyciu narzędzi w obrębie systemu.
2. W systemach działających sieciowo, na zasadzie udostępnienia zasobów na serwerze, Administrator Systemu powinien uwzględniać dedykowane przyzwolenia dostępu.

§ 18
KOMUNIKACJA WEWNĘTRZNA

1. Przesyłanie danych osobowych w komunikacji wewnętrznej (sieci lokalnej) musi być oznaczone w sposób dostępny jedynie dla uprawnionych użytkowników przy użyciu narzędzi zabezpieczeń w obrębie systemu informatycznego.
2. W sytuacji, gdy dostępne narzędzia informatyczne nie będą wystarczające do działania w komunikacji wewnętrznej, użytkownik systemu wyznacza sposób postępowania, mając w szczególności na uwadze ochronę danych osobowych.

§ 19
KOMUNIKACJA ZEWNĘTRZNA

1. Do przesyłania danych przy połączeniach w sieci publicznej (Internet), z uwagi na przekazywane dane osobowe, powinny być wykorzystywane tylko kanały transmisji wykorzystywane przez autoryzowane programy wykorzystywane również w innych urzędach oraz instytucjach państwowych i w oparciu o przepisy prawne regulujące sposób wysyłania tych danych.

2. Odpowiednią dokumentację, rejestry i procedury prowadzi ABI.
3. Procedura korzystania z internetu:
   1) Użytkownik zobowiązany jest do korzystania z internetu wyłącznie w celach służbowych,
   2) Zabrania się zgrywania na dysk twardy komputera oraz uruchamiania jakichkolwiek programów nielegalnych oraz plików pobranych z niewiadomego źródła. Pliki takie powinny być ściągane tylko za każdorazową zgodą ASI i ABI,
   3) Użytkownik ponosi odpowiedzialność za szkody spowodowane przez oprogramowanie ściągnięte z internetu i przez niego zainstalowane,
   4) Nie należy w opcjach przeglądarki internetowej włączać opcji zapamiętywania haseł.
4. Procedura korzystania z poczty elektronicznej:
   1) Przesyłanie informacji zawierających dane osobowe poza Starostwo Powiatowe w uzasadnionych przypadkach może odbywać się tylko przez osoby upoważnione i wyłącznie za zgodą ABI oraz pod nadzorem ASI (odpowiednie szyfrowanie i kryptografia),
   2) Przesyłanie pozostałych informacji nie zawierających danych osobowych poza Starostwo Powiatowe może odbywać się tylko przez osoby upoważnione,
   3) Użytkownicy powinni zwracać szczególną uwagę na poprawność adresu odbiorcy dokumentu,
   4) Zaleca się, aby użytkownik podczas przesyłania danych osobowych mailem zawarł w treści prośbę o potwierdzenie otrzymania i zapoznania się z informacją przez adresata,
   5) Nie należy otwierać załączników (plików) w korespondencji elektronicznej nadesłanej przez nieznanego nadawcę,
   6) Użytkownicy powinni okresowo kasować niepotrzebne wiadomości pocztowe.

§ 20.
OZNACZANIE NOŚNIKÓW DANYCH

1. Nośniki informatyczne zawierające dane osobowe powinny być opisane w sposób czytelny i zrozumiały dla użytkownika, a zarazem nie powinny ułatwiać rozpoznania zawartości przez osoby nieupoważnione.

§ 21.
BEZPIECZEŃSTWO NOŚNIKÓW I URZĄDZEŃ

1. Nośniki informatyczne przechowywane są w miejscach, do których dostęp mają wyłącznie osoby upoważnione.
2. Nośniki o których mowa w ust. 1 są regularnie przeglądane i po stwierdzeniu utracenia waloru przydatności powinny zostać zniszczone.
3. Użytkownicy stacji roboczych wykonujących kopie zapasowe o których mowa w §12 pkt. 2 powinni prowadzić odpowiedni rejestr nośników przechowywanych i zniszczonych.

§ 22.
PRZENOŚNE NOŚNIKI INFORMATYCZNE

1. Zezwala się na używanie wyłącznie zarejestrowanych (ewidencjonowanych przez ABI) i zakupionych przez Jednostkę, zewnętrznych nośników danych typu: zewnętrzne dyski twarde, pamięci flash (pendrive) i inne przenośne nośniki.
2. Nośniki o których mowa w pkt. 1 będące własnością Jednostki mogą być używane tylko i wyłącznie w jej obrębie i zabrania się ich wynoszenia oraz eksploatowania na zewnątrz.
3. Osoby użytkujące przenośne nośniki informatyczne, służące do przetwarzania danych osobowych, obowiązane są niezwłocznie informować na piśmie Administratora Bezpieczeństwa Informacji o zakresie, rodzaju zbieranych danych osobowych oraz celu ich przetwarzania. Administrator Bezpieczeństwa Informacji może żądać usunięcia danych, co do których zachodzi uzasadnione podejrzenie, że nie są przetwarzane zgodnie z zasadami określonymi w przepisach o ochronie danych osobowych.

§ 23.
PRZENOŚNY KOMPUTER

1. Osoba użytkująca przenośny komputer (laptop, notebook, tablet itp.), służący do przetwarzania danych osobowych, obowiązana jest zachować szczególną ostrożność podczas transportu i przechowywania tego komputera poza obszarem ochrony danych w celu zapobieżenia dostępowi do tych danych osobie niepowołanej.
2. Urządzenia o których mowa w pkt. 1 nie mogą służyć do przetwarzania danych osobowych.

§ 24.
WYDRUKI

1. Użytkownik sporządzający wydruki, które zawierają dane osobowe jest odpowiedzialny za zachowanie szczególnej ostrożności przy korzystaniu z nich, a zwłaszcza za zabezpieczenie ich przed dostępem osób nieuprawnionych i nie posiadających imiennego upoważnienia do ich przetwarzania.
2. Wydruki zawierające dane osobowe, które są przeznaczone do usunięcia, należy zniszczyć w stopniu uniemożliwiającym ich odczytanie.

§ 25.
DANE UŻYTKOWNIKA

1. System powinien umożliwić udostępnienie oraz możliwość wydruku, w zrozumiałej formie, treści danych o każdej osobie, której dane są przetwarzane, a w szczególności:
   1) daty pierwszego wprowadzenia danych tej osoby,
   2) źródła pochodzenia danych,
   3) nazwy użytkownika wprowadzającego dane,
   4) informacji - komu, kiedy i w jakim zakresie dane zostały udostępnione,
   5) sprzeciwu, o którym mowa w ustawie art. 32 ust. 1 pkt 7, po jego uwzględnieniu, oraz sprzeciwu określonego w ustawie art. 32 ust. 1 pkt 8.

§ 26.
ODPOWIEDZIALNOŚĆ

1. Naruszenie obowiązków wynikających z niniejszej Instrukcji Zarządzania Systemem Informatycznym 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.

§ 27.
OBOWIĄZKI ADMINISTRATORA SYSTEMÓW INFORMATYCZNYCH

1. Do obowiązków Administratora Systemów Informatycznych w zakresie ochrony danych osobowych przetwarzanych w systemach informatycznych należy w szczególności:
   1) realizacja zadań związanych z przeszkoleniem użytkowników w zakresie obsługi sprzętu informatycznego, oprogramowania systemowego oraz oprogramowania i obsługi aplikacji , którą będą wykorzystywali do pracy,
   2) operacyjne zarządzanie systemami informatycznymi w sposób zapewniający ochronę danych osobowych w nich przetwarzanych,
   3) przestrzeganie opracowanych dla systemu procedur operacyjnych i bezpieczeństwa,
   4) zarządzanie stosowanymi w systemach informatycznym środkami uwierzytelnienia, w tym rejestrowanie i wyrejestrowywanie użytkowników oraz dokonywanie zmiany uprawnień zgodnie z zaleceniami ABI,
   5) utrzymanie systemu w należytej sprawności technicznej,
   6) regularne tworzenie kopii zapasowych sieciowych zasobów danych osobowych oraz programów służących do ich przetwarzania oraz okresowe sprawdzanie poprawności wykonania kopii zapasowych,
   7) wykonywanie lub nadzór nad wykonywaniem okresowych przeglądów i konserwacji, zgodnie z odrębnymi procedurami, sprzętu IT, systemów informatycznych, aplikacji oraz elektronicznych nośników informacji, na których przetwarzane są dane osobowe.
   8) prowadzenie dokumentacji w formie dziennika zdarzeń wszystkich operacji mających wpływ na informatyczne zarządzanie danymi osobowymi.

PRZEPISY KOŃCOWE

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

Załącznik nr 2
do Instrukcji Zarządzania
Systemem Informatycznym

EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRACY W SYSTEMIE INFORMATYCZNYM ORAZ UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

L.p.	Nazwisko, Imię	System/aplikacja	Zakres upoważnienia do przetwarzania danych osobowych	Data nadania uprawnień	Data ustania uprawnień	Identyfikator użytkownika

Załącznik nr 3
do Instrukcji Zarządzania
Systemem Informatycznym

Dziennik zawiera opisy wszelkich zdarzeń istotnych dla działania systemu informatycznego w szczególności:

- w przypadku awarii – opis awarii, przyczyna awarii, szkody wynikłe na skutek awarii, sposób usunięcia awarii, opis systemu po awarii, wnioski,
- w przypadku konserwacji systemu – opis podjętych działań, wnioski.

DZIENNIK SYSTEMU INFORMATYCZNEGO
STAROSTWA POWIATOWEGO W NOWYM TOMYŚLU

L.p.	Data i godzina zdarzenia	Opis zdarzenia	Podjęte działania/wnioski	Podpis

Załącznik nr 1 do
Instrukcji Zarządzenia
Systemem Informatycznym

WNIOSEK
O NADANIE UPRAWNIEŃ W SYSTEMIE INFORMATYCZNYM

☐ Nowy użytkownik	☐ Modyfikacja uprawnień	☐ Odebranie uprawnień w systemie informatycznym

Imię i nazwisko użytkownika:	**Wydział/biuro/samodzielne stanowisko**
Opis i zakres uprawnień użytkownika w systemie informatycznym	
Data wystawienia:	Podpis bezpośredniego przełożonego użytkownika systemu:
Podpis Administratora Systemu:	Akceptacja ABI