Załącznik Nr 1 do Zarządzenia Wójta Gminy Białogard Nr 45/2015 z dnia 30 czerwca 2015 r.

POLITYKA BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH W URZĘDZIE GMINY BIAŁOGARD

OPRACOWAŁ:

EWA SZCZYBELSKA

Administrator Bezpieczeństwa Informacji

w URZĘDZIE GMINY BIAŁOGARD

Zatwierdzam:

WÓJT

.....

Jacek Smoliński

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 ze zm.) oraz rozporządzeniu Ministra Spraw Wewnętrznychi 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).

§ 2

Polityka określa tryb i zasady ochrony danych osobowych przetwarzanych w Urzędzie Gminy Białogard.

§ 3

Ilekroć w Polityce jest mowa o :

1) **Jednostka organizacyjna** – rozumie się przez to Urząd Gminy Białogard;
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 i 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** zwanym też **Administratorem Danych (ADO)** - w świetle art. 3 i 7 pkt 4 ustawy o ochronie danych osobowych rozumie się przez to kierownika jednostki który decyduje o celach i środkach przetwarzania danych osobowych;
10) **Administratorze Bezpieczeństwa Informacji** zwanym też **Administratorem Bezpieczeństwa (ABI)**- rozumie się przez to osobę powołaną przez Wójta Gminy Białogard, nadzorującą przestrzeganie zasad ochrony danych osobowych, w szczególności zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniemz naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem;
11) **Administratorze Systemu Informatycznego** zwanym też **Administratorem Systemu (ASI)** - rozumie się przez to osobę zatrudnioną przez kierownika jednostki upoważnioną do realizacji zadań związanych z zarządzaniem systemem informatycznym;
12) **kierownik komórki organizacyjnej –** rozumie się również samodzielne stanowisko pracy,
13) **użytkowniku systemu** zwanym też **użytkownikiem systemu informatycznego** - rozumie się przez to upoważnionego przez Wójta Gminy Białogard, 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

§ 4

Dane osobowe w Urzędzie Gminy Białogard są gromadzone, przechowywane, edytowane, archiwizowane w kartotekach, skorowidzach, księgach, wykazach ,zestawieniach oraz w innych zestawach i zbiorach ewidencyjnych poszczególnych komórek organizacyjnych Urzędu Gminy

Białogard na dokumentach papierowych, jak również w systemach informatycznych na elektronicznych nośnikach informacji.

§ 5

Polityka bezpieczeństwa wprowadza regulacje w zakresie zasad organizacji procesu przetwarzania danych osobowych i odnosi się swoją treścią do informacji:

1) w formie papierowej - przetwarzanej w ramach systemu tradycyjnego;
2) w formie elektronicznej - przetwarzanej w ramach systemu informatycznego.

§ 6

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

§ 7

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

§ 8

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 .

§ 9

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.

§ 10

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.

§ 11

Bezpośredni nadzór nad przetwarzaniem danych osobowych sprawują Kierownicy komórek organizacyjnych lub bezpośredni przełożeni.

§ 12

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 aktach osobowych pracownika, a drugi egzemplarz w dokumentacji ABI.

§ 13

1. Do informacji przechowywanych w systemach tradycyjnych jak i informatycznych mają dostęp jedynie upoważnieni pracownicy Urzędu Gminy Białogard oraz osoby mające imienne zarejestrowane upoważnienie, którego wzór stanowi załącznik Nr 2 do niniejszej Polityki. 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 Urzędu Gminy Białogard;

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. 3 stanowi załącznik Nr 3 do Polityki.

§ 14

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 II

ADMINISTRACJA I ORGANIZACJA BEZPIECZEŃSTWA

§ 15

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

2. Kierownicy komórek organizacyjnych oraz bezpośredni przełożeni 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.

§ 16

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

§ 17

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,

/administrator danych jest zobowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednia do zagrożeń oraz kategorii danych objętych ochroną ,a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom

nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem/.

c) zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych (szkolenia);

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;

8) prowadzi kontrolę w zakresie bezpieczeństwa;

9) prowadzi postępowanie wyjaśniające w przypadku naruszenia ochrony danych osobowych,

10) przygotowuje wnioski pokontrolne dla Administratora Danych Osobowych,

11) prowadzi rejestr zbiorów danych osobowych przetwarzanych przez administratora danych.

§ 18

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) zapewnia aktualizację dokumentacji technicznej systemu w tym opis struktur zbiorów i ich zależności;
6) prowadzi nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisywane są dane osobowe;
7) wykonuje kopie awaryjne/archiwalne /oraz nadzoruje ich przechowywanie;
8) wprowadza i nadzoruje mechanizmy autoryzacji.

§ 19

Kierownik komórki organizacyjnej oraz bezpośredni przełożony 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,
5) zgłasza potrzeby w zakresie zabezpieczenia danych osobowych w Urzędzie Gminy Białogard.

§ 20

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.

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

§ 21

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. Zestawienie zbiorów danych osobowych oraz programów do przetwarzania tych danych prowadzi ABI. Wzór wykazu zbiorów stanowi załącznik Nr 4 do Polityki bezpieczeństwa.

§ 22

Ze względu na rodzaj i charakter danych osobowych zawartych w zbiorach, w Urzędzie Gminy Białogard wyróżnia się dwie kategorie danych:

1) **dane osobowe zwykłe** - wszelkie dane (informacje) dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, zgromadzone w zbiorach danych osobowych.
2) **dane osobowe szczególnie chronione** – zgodnie z art. 27 ust.1 ustawy o ochronie danych osobowych, wszelkie dane (informacje) ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne, przynależność partyjną lub związkową, jak również informacje o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz dane dotyczące skazania osoby, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.

§ 23

1.Zgodnie z postanowieniami art. 40 ustawy o ochronie danych osobowych, z uwagi na gromadzone kategorie zbiorów danych osobowych istnieje obowiązek zgłoszenia do rejestracji tych zbiorów Generalnemu Inspektorowi Ochrony Danych Osobowych z wyjątkiem przypadków, o których mowa w art. 43 ust. 1 i 1a tejże ustawy.

2. Użytkownicy danych osobowych są zobowiązani do przekazywania ABI informacji o zamiarze utworzenia nowego zbioru danych osobowych oraz o zmianach w zbiorach juz istniejących. Wzór informacji o zamiarze utworzenia nowego zbioru stanowi załącznik Nr 5 do Polityki bezpieczeństwa. Natomiast wzór wykazu zmian w zbiorze stanowi załącznik Nr 6 do Polityki bezpieczeństwa

3. Na podstawie posiadanych zbiorów danych osobowych tworzy sie ewidencję struktur zbiorów, którą prowadzi ABI. Wzór stanowi załącznik Nr 7 do Polityki bezpieczeństwa

Rozdział IV

SPOSÓB PRZEPŁYWU DANYCH POMIĘDZY POSZCZEGÓLNYMI SYSTEMAMI

§ 24

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. Przekazywanie informacji (danych) w systemie informatycznym poza sieć lokalną jednostki odbywa się w relacji jednostka organizacyjna - mieszkańcy, przedsiębiorcy, kontrahenci, zakład ubezpieczeń społecznych, urząd skarbowy, banki, Narodowy Fundusz Ochrony Zdrowia, urząd wojewódzki, urząd marszałkowski inne jednostki administracji samorządowej i rządowej.

3. Zabronione jest jednoczesne podłączanie komputerów do sieci wewnętrznej Urzędu Gminy Białogard i sieci zewnętrznych (Plus , Era , Orange , Play, pozostałe sieci komórkowe, WiFi , WiMAX itp.).

4. ASI prowadzi wykaz sposobu przepływu danych pomiędzy poszczególnymi systemami, wzór stanowi załącznik Nr 8 do Polityki bezpieczeństwa.

Rozdział V

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

§ 25

1. Dostęp do danych wprowadzonych przez użytkowników systemów informatycznych mają jedynie upoważnione osoby oraz Administrator Systemu Informatycznego zapewniający jego prawidłową eksploatację.

2. Pomieszczenia, w których przetwarza się dane osobowe powinny być fizycznie zabezpieczone przed dostępem osób nieuprawnionych, to znaczy posiadać odpowiednie zamki do

drzwi, zabezpieczenia w oknach (w szczególności na parterze) oraz być wyposażone w środki ochrony ppoż.

Wykaz pomieszczeń stanowiących obszar przetwarzania danych osobowych w Urzędzie Gminy Białogard prowadzi ABI. Wzór wykazu pomieszczeń stanowiących obszar przetwarzania danych osobowych stanowi załącznik Nr 9 do Polityki bezpieczeństwa.

3. W pomieszczeniach gdzie przebywają osoby postronne, monitory stanowisk dostępu do danych osobowych powinny być ustawione w taki sposób by uniemożliwić tym osobom wgląd w dane osobowe.

4. Dokumenty i nośniki informacji, zawierające dane osobowe powinny być zabezpieczone przed dostępem osób nieupoważnionych do przetwarzania danych. Jeśli nie są aktualnie używane powinny być przechowywane w szafach lub w innych przeznaczonych do tego celu urządzeniach biurowych, posiadających odpowiednie zabezpieczenia.

Rozdział VI

UDOSTĘPNIANIE POSIADANYCH W ZBIORZE DANYCH OSOBOWYCH

§ 26

1. Na wniosek osoby, której dane dotyczą, ADO jest obowiązany, w terminie 30 dni, poinformować o przysługujących jej prawach, a zwłaszcza wskazać w formie zrozumiałej odnośnie danych osobowych jej dotyczących:

1) jakie dane osobowe zawiera zbiór,
2) w jaki sposób zebrano dane,
3) w jakim celu i zakresie dane są przetwarzane,
4) w jakim zakresie oraz komu dane zostały udostępnione.

2. Na wniosek osoby, której dane dotyczą, informacji, o których mowa w ust. 1, udziela się na piśmie.

§ 27

1. Każdej osobie przysługuje prawo do kontroli przetwarzania danych, które jej dotyczą, zawartych w zbiorach danych, a zwłaszcza prawo do:

1) uzyskania wyczerpującej informacji, czy taki zbiór istnieje, oraz do ustalenia administratora danych, adresu jego siedziby i pełnej nazwy,

2) uzyskania informacji o celu, zakresie i sposobie przetwarzania danych zawartych w takim zbiorze,
3) uzyskania informacji, od kiedy przetwarza się w zbiorze dane jej dotyczące, oraz podania w powszechnie zrozumiałej formie treści tych danych,
4) uzyskania informacji o źródle, z którego pochodzą dane jej dotyczące,
5) uzyskania informacji o sposobie udostępniania danych, a w szczególności informacji o odbiorcach lub kategoriach odbiorców, którym dane te są udostępniane,
6) żądania uzupełnienia, uaktualnienia, sprostowania danych osobowych, czasowego lub stałego wstrzymania ich przetwarzania lub ich usunięcia, jeżeli są one niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy albo są już zbędne do realizacji celu, dla którego zostały zebrane,
7) 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,
8) 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,
9) wniesienia do administratora danych żądania ponownego, indywidualnego rozpatrzenia sprawy rozstrzygniętej z naruszeniem zakazu ostatecznego rozstrzygnięcia indywidualnej sprawy, gdy treść była wyłącznie wynikiem operacji na danych osobowych prowadzonych w systemie informatycznym.

2. Osoba zainteresowana może skorzystać z prawa do informacji, o których mowa w ust. 1 pkt 1 - 5, nie częściej niż raz na 6 miesięcy.

§ 28

1. W razie wykazania przez osobę, której dane osobowe dotyczą, że są one niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy albo są zbędne do realizacji celu, dla którego zostały zebrane, administrator danych jest obowiązany, bez zbędnej zwłoki, do uzupełnienia, uaktualnienia, sprostowania danych, czasowego lub stałego wstrzymania przetwarzania

kwestionowanych danych lub ich usunięcia ze zbioru, chyba że dotyczy to danych osobowych, w odniesieniu do których tryb ich uzupełnienia, uaktualnienia lub sprostowania określają odrębne ustawy.

2. Każda z osób zatrudnionych przy przetwarzaniu danych w razie powzięcia takiej wiadomości ma obowiązek o wystąpieniu osoby, której dane dotyczą, poinformować ABI.

§ 29

1. Do udostępniania posiadanych w zbiorze danych osobowych upoważniony jest kierownik jednostki lub pracownik posiadający wymagane prawem upoważnienie.

2. W przypadku udostępniania danych osobowych w celach innych niż wyłączenie do zbioru, administrator danych udostępnia posiadane w zbiorze dane osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa.

3. Pracownik udostępniający dane osobowe zobowiązany jest zaznaczenia w formie pisemnej, iż można je wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.

4. Na pisemny wniosek pochodzący od osoby, której dane dotyczą, informacje o osobie powinny być udzielone w terminie 30 dni od daty złożenia wniosku.

5. Za przygotowanie danych osobowych do udostępnienia w zakresie wskazanym we wniosku odpowiada użytkownik danych osobowych.

6. Odpowiedź na wniosek o udostępnienie danych osobowych przed wysłaniem jest akceptowany i parafowany przez użytkownika danych osobowych i **podpisywany przez ADO lub osobę upoważnioną.**

7. Informacje zawierające dane osobowe są przekazywane uprawnionym podmiotom lub osobom za potwierdzeniem odbioru:

1) listem poleconym za pokwitowaniem odbioru;

3) w inny bezpieczny, prawem określony sposób.

8. W przypadku udostępniania danych osobowych ze zbioru danych osobowych informację o udostępnieniu danych osobowych odnotowuje się **lub sporządza kserokopię** dokumentu zawierającego udostępniane dane. Nie dotyczy to sytuacji, gdy przepisy prawa zezwalają na zbieranie danych osobowych bez konieczności ujawniania adresata danych.

§ 30

1. Powierzenie przetwarzania danych osobowych innemu podmiotowi może nastąpić wyłącznie w drodze umowy zawartej w formie pisemnej przez ADO z uwzględnieniem wymagań określonych w art. 31 ust. 1 tejże ustawy.

Rozdział VII
ZACHOWANIE BEZPIECZEŃSTWA PRZEZ UŻYTKOWNIKÓW SYSTEMU

§ 31

Użytkownicy systemu zobowiązani są stosować odpowiednie środki bezpieczeństwa w pomieszczeniach, w których zainstalowano sprzęt systemu informatycznego by nie spowodować jego uszkodzenia.

§ 32

1. Wszyscy użytkownicy systemu muszą stosować się do obowiązujących procedur bezpieczeństwa.

2. Hasło podlega szczególnej ochronie. Użytkownik ma obowiązek tworzenia haseł. W przypadku, gdy użytkownik zapomni swoje hasło, może on odnowić hasło w porozumieniu z Administratorem Systemu Informatycznego.

Rozdział VIII
BEZPIECZEŃSTWO FIZYCZNE

§ 33

1 Dane osobowe, które są przedmiotem przetwarzania zgodnie z przepisami ustawy o ochronie danych osobowych, gromadzone i przechowywane są w serwerach i w postaci tradycyjnej.

2. Środki bezpieczeństwa fizycznego są konieczne dla zapobiegania niepowołanemu dostępowi do informacji, nieautoryzowanym operacjom w systemie, kontroli dostępu do zasobów oraz w celu zabezpieczenia sprzętu teleinformatycznego.

§ 34

1. Obszar systemów informatycznych w Urzędzie Gminy Białogard obejmuje wszystkie pomieszczenia w budynku przy ul. Wileńskiej 8.

§ 35

1. Pomieszczenia, w których znajdują się systemy informacji winny być:

1) wyposażone w szafy ,meble biurowe zamykane na klucz umożliwiające przechowywanie dokumentów,
2) zamknięte, jeśli nikt w nich nie przebywa.

2. Przed przystąpieniem do pracy użytkownicy danych zobowiązani są do dokonania sprawdzenia stanu urządzeń informatycznych i oględzin stanowiska pracy, w tym do zwrócenia szczególnej uwagi, czy nie zaszły okoliczności wskazujące na naruszenie lub na próbę naruszenia ochrony danych osobowych przetwarzanych w systemach informatycznych i w zbiorach nieinformatycznych.

3. Do okoliczności, uznawanych za naruszenie, próbę naruszenia ochrony systemu przetwarzającego dane osobowe, uważa się w szczególności:

1) nieuprawniony dostęp lub próbę dostępu do danych osobowych lub pomieszczeń, w których się one znajdują;
2) nieuprawnione naruszenie lub próby naruszenia poufności, integralności i rozliczalności danych i systemu;
3) niezamierzoną zmianę lub utratę danych zapisanych na kopiach zapasowych;
4) nieuprawniony dostęp do danych osobowych (sygnał o nielegalnym logowaniu lub inny objaw wskazujący na próbę lub działanie związane z nielegalnym dostępem do systemu);
5) udostępnienie danych osobowych lub ich części osobom nieupoważnionym;
6) inny stan systemu informatycznego lub pomieszczeń niż pozostawiony przez użytkownika po zakończeniu pracy;
7) wydarzenia losowe, obniżające poziom ochrony systemu (np. brak zasilania, pożar);
8) kradzież sprzętu informatycznego lub nośników zewnętrznych zawierających dane osobowe (np. wydruków komputerowych, dyskietek, płyt CD-ROM, dysków twardych, pamięci zewnętrznych, itp.).

4. W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenie ochrony danych osobowych pracownicy zobowiązani są do bezzwłocznego powiadomienia o tym fakcie ABI i ASI.

5. ABI i ASI sporządzają raport z przebiegu zdarzenia, zawierający w szczególności informacje o:

1) dacie i godzinie powiadomienia o zdarzeniu;

2) godzinie przybycia do pomieszczeń, w których zdarzenie nastąpiło;

3) istniejącej w chwili przybycia sytuacji;

4) podjętych działaniach i ich zasadności,

5) stanie systemu po podjęciu działań naprawczych;

6) wnioskach w sprawie ograniczenia możliwości ponownego wystąpienia naruszenia ochrony danych osobowych, wzór stanowi załącznik Nr 10 do Polityki bezpieczeństwa. Raport, ABI przekazuje niezwłocznie ADO, a przypadku jego nieobecności osobie upoważnionej.

§ 36

Instalacja urządzeń systemu i sieci teleinformatycznej odbywa się za wiedzą i pod kontrolą kierownika komórki organizacyjnej, który jest również odpowiedzialny za warunki wprowadzania do użycia, przechowywania, eksploatacji oraz wycofywania z użycia każdego urządzenia.

Dział IX
BEZPIECZEŃSTWO SPRZĘTU I OPROGRAMOWANIA

§ 37

Sprzęt i oprogramowanie, indywidualnie lub łącznie mają ścisły związek z bezpieczeństwem systemu i sieci teleinformatycznej. Dlatego, powinny być ściśle przestrzegane procedury bezpieczeństwa odnoszące się do tych elementów.

§ 38

Sieć teleinformatyczna jest organizacyjnym i technicznym połączeniem systemów teleinformatycznych wraz z łączącymi je urządzeniami i liniami telekomunikacyjnymi. Niedopuszczalne jest samowolne przemieszczanie lub zmiana konfiguracji stacji roboczej bez wiedzy kierownika komórki organizacyjnej.

§ 39

Zabrania się korzystania z jakiegokolwiek nowego oprogramowania bez zgody Administratora Systemu Informatycznego.

§ 40

1. Dostęp do zbiorów danych osobowych znajdujących się na serwerach następuje po wprowadzeniu hasła, które znane jest tylko osobie przetwarzającej dane.

2. Każdorazowo po dokonaniu przetworzenia aplikacja powinna być zamknięta.

3. W przypadku podejrzenia, iż wiadomości o sposobie dostępu do elektronicznej bazy danych uzyskała osoba do tego niepowołana, osoba przetwarzająca dane w porozumieniu z ASI powinna dokonać zmiany hasła.

§ 41

1. Elektroniczne bazy danych osobowych są archiwizowane.

2. Kopie są wykonywane na nośnikach magnetycznych.

§ 42

Używanie oprogramowania prywatnego w sieci jest zabronione. Na stacjach roboczych powinno być zainstalowane niezbędne oprogramowanie przypisane do danego stanowiska.

Rozdział X

KONSERWACJE I NAPRAWY

§ 43

Każde urządzenie użytkowane w systemie informatycznym, powinno podlegać rutynowym czynnościom konserwacyjnym oraz przeglądom wykonywanym przez uprawnione osoby.

§ 44

1. Za konserwację oprogramowania systemowego oraz aplikacyjnego serwera systemu informatycznego odpowiedzialny jest Administrator Systemu Informatycznego. Konserwacja oprogramowania obejmuje także jego aktualizację.

2. Za konserwację oprogramowania stanowisk roboczych odpowiedzialny jest kierownik komórki organizacyjnej. Wszelkie aktualizacje oprogramowania powinny być uzgadniane z Administratorem Systemu Informatycznego.

§ 45

Administrator Systemu Informatycznego przed rozpoczęciem naprawy urządzenia przez zewnętrzne firmy sprawdza, czy spełnione są następujące wymagania:

1) w przypadku awarii serwera i konieczności oddania sprzętu do serwisu, nośniki magnetyczne zawierające dane osobowe powinny być wymontowane i do czasu naprawy serwera przechowywane w pomieszczeniu biurowym znajdującym się w strefie o ograniczonym dostępie;
2) w przypadku uszkodzenia nośnika magnetycznego zawierającego dane osobowe należy komisyjnie dokonać jego zniszczenia.
3)

§ 46

Serwer systemu oraz poszczególne stacje robocze (opcjonalnie) powinny być zabezpieczone urządzeniami podtrzymującymi zasilanie (UPS), co umożliwi funkcjonowanie systemu w przypadku awarii zasilania.

§ 47

W celu zabezpieczenia ciągłości pracy, informacja przechowywana i przetwarzana w systemie podlega codziennej, przyrostowej archiwizacji (opcjonalnie) oraz pełnej archiwizacji przeprowadzanej nie rzadziej niż na miesiąc. Kopie bezpieczeństwa danych są wykonywane na nośnikach magnetooptycznych, i przechowywane są przez Administratora Systemu Informatycznego. Użycie kopii bezpieczeństwa następuje na polecenie Administratora Systemu Informatycznego w przypadku odtwarzania systemu po awarii.

Rozdział XI

POLITYKA ANTYWIRUSOWA

§ 48

1. Wszystkie serwery i komputery są sprawdzane przy użyciu oprogramowania do wykrywania i usuwania wirusów komputerowych.

2. W zakresie ochrony antywirusowej wprowadza się następujące zalecenia:

1) nie należy używać oprogramowania na stacji roboczej innego niż zaleca Administrator Systemu Informatycznego;
2) przed użyciem nośnika danych sprawdzić czy nie jest zainfekowany wirusem komputerowym.

2. W przypadku jakichkolwiek wątpliwości odnośnie zagrożenia wirusowego należy sprawdzić zawartość całego dysku twardego programem antywirusowym. W przypadku dalszych niejasności należy kontaktować się z administratorem sieci lokalnej.

Rozdział XII
PRZEPISY KOŃCOWE

§ 49

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.

- ***Art.49.1.*** *Kto przetwarza dane osobowe, choć ich przetwarzanie nie jest dopuszczalne albo do których nie jest uprawniony , podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2;*

  2. Jeżeli czyn określony w ust. 1 dotyczy danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym, sprawca podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 3.
- ***Art. 51. 1.*** *Kto administrując zbiorem danych lub będąc obowiązany do ochrony danych osobowych udostępnia je lub umożliwia dostęp do nich osobom nieupoważnionym, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.*

  2. Jeżeli sprawca działa nieumyślnie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.
- ***Art. 52.*** *Kto administrując danymi narusza choćby nieumyślnie obowiązek zabezpieczenia ich przed zabraniem przez osobę nieuprawnioną, uszkodzeniem lub*

zniszczeniem, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

- ***Art. 53.*** *Kto będąc do tego obowiązany nie zgłasza do rejestracji zbioru danych, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.*
- ***Art. 54.*** *Kto administrując zbiorem danych nie dopełnia obowiązku poinformowania osoby, której dane dotyczą, o jej prawach lub przekazania tej osobie informacji umożliwiających korzystanie z praw przyznanych jej w niniejszej ustawie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.*
- ***Art. 52.*** *Kto administrując danymi narusza choćby nieumyślnie obowiązek zabezpieczenia ich przed zabraniem przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.*
- ***Art. 53.*** *Kto będąc do tego obowiązany nie zgłasza do rejestracji zbioru danych, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.*
- ***Art. 54.*** *Kto administrując zbiorem danych nie dopełnia obowiązku poinformowania osoby, której dane dotyczą, o jej prawach lub przekazania tej osobie informacji umożliwiających korzystanie z praw przyznanych jej w niniejszej ustawie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.*

§ 50

W sprawach nie uregulowanych w niniejszej Polityce bezpieczeństwa informacji mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r. poz. 1182, ze 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).

Wykaz osób, które zapoznały sie z „Polityką Bezpieczeństwa Przetwarzania Danych Osobowych w Urzędzie Gminy Białogard" i „Instrukcją Zarządzania Systemem Informatycznym Służącym Do Przetwarzania Danych Osobowych w Urzędzie Gminy Białogard", wprowadzonych zarządzeniem Nr 45/ 2015 Wójta Gminy Białogard z dnia 30 czerwca 2015 r.

Przyjęłam/łem do wiadomości i stosowania zapisy „Polityki Bezpieczeństwa Przetwarzania Danych Osobowych w Urzędzie Gminy Białogard" i „Instrukcji Zarządzania Systemem Informatycznym Służącym Do Przetwarzania Danych Osobowych w Urzędzie Gminy Białogard".

Lp.	Nazwisko i imię	Stanowisko	Data, podpis

Wykaz osób, które zapoznały sie z „Polityką Bezpieczeństwa Przetwarzania Danych Osobowych w Urzędzie Gminy Białogard" i „Instrukcją Zarządzania Systemem Informatycznym Służącym Do Przetwarzania Danych Osobowych w Urzędzie Gminy Białogard", wprowadzonych zarządzeniem Nr 45/ 2015 Wójta Gminy Białogard z dnia 30 czerwca 2015 r.

Przyjęłam/łem do wiadomości i stosowania zapisy „Polityki Bezpieczeństwa Przetwarzania Danych Osobowych w Urzędzie Gminy Białogard" i „Instrukcji Zarządzania Systemem Informatycznym Służącym Do Przetwarzania Danych Osobowych w Urzędzie Gminy Białogard".

Lp.	Nazwisko i imię	Stanowisko	Data, podpis

Załącznik Nr 1 do Polityki Bezpieczeństwa w Urzędzie Gminy Białogard.

WZÓR

O Ś W I A D C Z E N I E

Imię i nazwisko	
Stanowisko służbowe	
Nazwa komórki organizacyjnej	

Stwierdzam własnoręcznym podpisem, że zapoznałem/am/ się z „Polityką Bezpieczeństwa Przetwarzania Danych Osobowych w Urzędzie Gminy Białogard oraz Instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Białogard.

Jednocześnie, zgodnie z przepisami ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r. , poz. 1182 ze zm.) zobowiązuję się do ochrony przed niepowołanym dostępem, nieuzasadnioną modyfikacją lub zniszczeniem, nielegalnym ujawnieniem lub pozyskaniem, danych osobowych przetwarzanych w Urzędzie Gminy Białogard oraz do zachowania ich w tajemnicy w czasie trwania jak i po ustaniu zatrudnienia.

Równocześnie oświadczam, że zostałem(am) poinformowany(a) o odpowiedzialności służbowej i karnej w przypadku naruszenia przepisów.

....

(imię, nazwisko i podpis osoby przyjmującej oświadczenie)

(data i podpis składającego oświadczenie)

Załącznik Nr 2 do Polityki Bezpieczeństwa w Urzędzie Gminy Białogard.

Wzór

U P O W A Ż N I E N I E *Nr .....*

Zgodnie z art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r. , poz. 1182 ze zm.), zgodnie z zakresem czynności i złożonego oświadczenia w sprawie znajomości przepisów dotyczących ochrony danych osobowych

U p o w a ż n i a m

Pana/Panią:

.....
imie i nazwisko

do przetwarzania danych osobowych gromadzonych w systemie informatycznym/ nie informatycznym w ..... w zbiorach :
(nazwa komórki organizacyjnej)

Lp.	PEŁNA NAZWA ZBIORU

Powyższe upoważnienie wydaje się na okres do .....
(wpisać na jaki okres lub bezterminowo)

Administrator Danych Osobowych

.....

....
/miejscowość/ */data/*

Załącznik Nr 3 do Polityki Bezpieczeństwa w Urzędzie Gminy Białogard.

WZÓR

Ewidencja osób upoważnionych do przetwarzania danych osobowych

(podstawa prawna art. 39 ustawy o ochronie danych osobowych).

L.p.	Imię i nazwisko	Stanowisko	Komórka organizacyjna	Data przeszkolenia	Nr upoważnienia imiennego	Identyfikator	Data nadania upoważnienia	Data ustania upoważnienia	Zakres upoważnienia*

*Zakres upoważnienia:

wgląd	**D**
wprowadzanie	**W**
modyfikacja	**M**
usuwanie	**U**

Załącznik Nr 4 do Polityki Bezpieczeństwa w Urzędzie Gminy Białogard

WZÓR

Wykaz zbiorów danych przetwarzanych w Urzędzie Gminy Białogard

Lp	NAZWA ZBIORU	Zakres przetwarzanych w zbiorze danych o osobach	Inne dane osobowe	System danych T-tradyc. I-inform.	Nazwa Programu 1) forma danych 2) zabezpieczenie informatyczne, 3) bazę danych chroni UPS (TAK / NIE)	Lokalizacja	Zabezpieczenie fizyczne
1.	DZIENNIK KORESPONDENCJI	nazwiska i imiona adres zamieszkania lub pobytu	adres poczty elektronicznej,	T	Nie dotyczy	Podać: - *Adres,* - *Nr budynku* - *Nr pokoju*	Alarm, , zamki patentowe, wydruki przechowywane w szafach zamykanych na klucz, , zabezp. p.poż.
2.	REJESTR SKARG I WNIOSKÓW	nazwiska i imiona, adres zamieszkania lub pobytu, numer telefonu,		T	Nie dotyczy	Podać: - *Adres,* - *Nr budynku* - *Nr pokoju*	Alarm, , zamki patentowe, wydruki przechowywane w szafach zamykanych na klucz, , zabezp. p.poż.

Zał. Nr 5 do Polityki Bezpieczeństwa w Urzędzie Gminy Białogard

1. NAZWA ZBIORU DANYCH

.....

2. ADMINISTRATOR DANYCH

Nazwa:.....

Miejscowość:.....

Ulica:.....

REGON:.....

3. Przedstawiciel administratora danych , o którym mowa w art.31a ustawy z dnia 29 sierpnia 1997r.o ochronie danych osobowych
   /w przypadku przetwarzania danych osobowych przez podmioty mające siedzibę albo miejsce zamieszkania w państwie trzecim, administrator danych jest obowiązany wyznaczyć swojego przedstawiciela w Rzeczypospolitej Polskiej/:

   Nazwa:.....

   Miejscowość:.....

   Ulica.....

4. Powierzenie przetwarzanie danych osobowych:

   Nazwa:.....

   Miejscowość:.....

   Ulica:.....

5. Podstawa prawna upoważniająca do prowadzenia zbioru danych */art.23.1,art.27.2/:*
   .....

6. Cel przetwarzania danych w zbiorze:
   .....

7. Opis kategorii osób, których dane są przetwarzane w zbiorze:
   .....

8. Zakres danych przetwarzanych w zbiorze:
   .....
   .....
   .....

9. Sposób zbierania danych do zbioru:
   .....

10. Sposób udostępniania danych ze zbioru:
    .....

11. Oznaczenie odbiorcy danych lub kategorii odbiorców , którym dane mogą być przekazywane:
    .....

12. Informacja dotycząca ewentualnego przekazywania danych do państwa trzeciego- rozumie się przez to państwo nienależące do Europejskiego Obszaru Gospodarczego :
    .....

    Uwaga :
    Administrator bezpieczeństwa informacji w ramach prowadzenia rejestru dokonuje:
    - wpisania zbioru danych w przypadku rozpoczęciu przetwarzania w nim danych osobowych- wpisu dokonuje się niezwłocznie po rozpoczęciu przetwarzania danych w zbiorze;
    - aktualizacji informacji dotyczących zbioru danych w przypadku zmiany informacji objętych wpisem;
    - wykreślenia zbioru danych w przypadku zaprzestania przetwarzania w nim danych osobowych.

Wszystkie zmiany związane z prowadzonym zbiorem są odnotowywane w wykazie zmian.

Załącznik Nr 6 do Polityki Bezpieczeństwa w Urzędzie Gminy Białogard

WYKAZ ZMIAN

WZÓR

w zbiorze .....

Lp.	RODZAJ ZMIANY • nowy wpis, • aktualizacja, • wykreślenie	DATA DOKONANIA ZMIANY	ZAKRES ZMIAN

Załącznik nr 8 do Polityki Bezpieczeństwa w Urzędzie Gminy Białogard

SPOSÓB PRZEPŁYWU DANYCH POMIĘDZY POSZCZEGÓLNYMI SYSTEMAMI

WZÓR

LP.	Rodzaj urządzenia	Rodzaj zbioru	Docelowy system informatyczny	Zakres przesyłanych danych osobowych	Sposób transmisji
1.	KOMPUTER STACJONARNY, WINDOWS, UWIERZYTELNIANIE: IDENTYFIKATOR + HASŁO	Dokumentacja związana z	Word / Excel	• imię i nazwisko • data i miejsce urodzenia, • PESEL, • adres zamieszkania /zameldowania/	manualny
2.	KOMPUTER STACJONARNY, WINDOWS, UWIERZYTELNIANIE: IDENTYFIKATOR + HASŁO	System Informacji Oświatowej	SIO, uwierzytelnianie: identyfikator + hasło	• imię i nazwisko • data i miejsce urodzenia, • PESEL, • adres zamieszkania /zameldowania	przesyłanie danych poprzez sieć telekomunikacyjną

Załącznik nr 10 do Polityki Bezpieczeństwa w Urzędzie Gminy Białogard

WYKAZ POMIESZCZEŃ STANOWIĄCYCH OBSZAR PRZETWARZANIA DANYCH OSOBOWYCH

Wzór

Budynek Urzędu ..... **Miejscowość** ..... **ul**.....		
L.P.	**Nazwa pomieszczenia**	**Miejsce ,położenie**
1.	Gabinet Wójta	pokój nr .....
2.	Gabinet Zastępcy Wójta	pokój nr.....
3.	Sekretariat	pokój nr.....
4.	Ewidencja ludności i dowodów osobistych	pokój nr.....
5.	Podatki	pokój nr.....
6.	Archiwum	pokój nr.....
7.	Ewidencja Działalności Gospodarczej	pokój nr.....
8.	Biuro Rady	pokój nr.....