ZARZĄDZENIE NR 0050.49.2016
WÓJTA GMINY DĄBROWA CHEŁMIŃSKA
z dnia 08 czerwca 2016 r.

w sprawie wprowadzenia Polityki bezpieczeństwa informacji oraz instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych

Na podstawie art. 36 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tj. Dz. U. z 2015 r., poz. 1235 z późn. zm.) oraz § 3, § 4 i § 5 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024) w związku z art. 33 ust. 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (tj. Dz. U. z 2016 r., poz. 446) zarządzam, co następuje:

§ 1. 1. Wprowadza się „Politykę Bezpieczeństwa Informacji w Urzędzie Gminy w Dąbrowie Chełmińskiej" zwaną dalej „Polityką", która stanowi załącznik 1 do niniejszego zarządzenia.

2. Wprowadza się „Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy w Dąbrowie Chełmińskiej", zwaną dalej „Instrukcją", która stanowi załącznik 2 do niniejszego zarządzenia.

§ 2. „Polityka" i „Instrukcja" mają zastosowanie na wszystkich stanowiskach pracy, gdzie przetwarzane są dane osobowe lub praca odbywa się w systemie informatycznym Urzędu Gminy w Dąbrowie Chełmińskiej.

§ 3. Nadzór nad wykonaniem zarządzenia powierza się Administratorowi Bezpieczeństwa Informacji w Urzędzie Gminy w Dąbrowie Chełmińskiej.

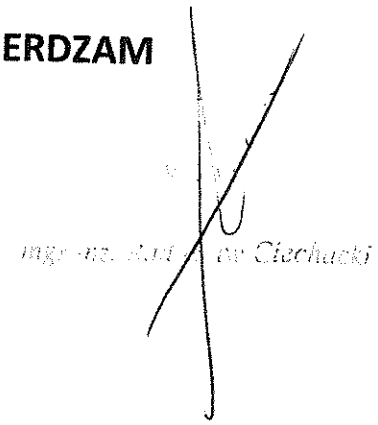
§ 4. Traci moc Zarządzenie Nr 0050.19.2013 Wójta Gminy Dąbrowa Chełmińska z dnia 28 czerwca 2013 r. w sprawie ustalenia Polityki Bezpieczeństwa i Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

§ 5. Zarządzenie wchodzi w życie z dniem podpisania.

mgr inż. Ludwik [illegible]

Załącznik nr 1 do Zarządzenia nr ..... Wójta Gminy Dąbrowa Chełmińska
z dnia .....

ZATWIERDZAM



POLITYKA BEZPIECZEŃSTWA INFORMACJI W URZĘDZIE GMINY W DĄBROWIE CHEŁMIŃSKIEJ

ADMINISTRATOR Bezpieczeństwa Informacji

Robert Bagiński

.....

Rozdział I
Postanowienia ogólne, definicje

§ 1

1. Wójt Gminy Dąbrowa Chełmińska świadomy wagi problemów związanych z ochroną prawa do prywatności, w tym w szczególności prawa osób fizycznych powierzających Urzędowi Gminy swoje dane osobowe do właściwej i skutecznej ochrony tych danych deklaruje zamiar:
    a) Podejmowania wszystkich działań niezbędnych dla ochrony praw i usprawiedliwionych interesów jednostki związanych z bezpieczeństwem danych osobowych,
    b) Stałego podnoszenia świadomości oraz kwalifikacji osób przetwarzających dane osobowe w Urzędzie Gminy w zakresie problematyki bezpieczeństwa tych danych, w tym propagowania świadomości wartości powierzonych danych osobowych jako czynnika wpływającego na jakość i ciągłość działalności oraz wiarygodność Urzędu Gminy w Dąbrowie Chełmińskiej,
    c) Traktowania obowiązków osób zatrudnionych przy przetwarzaniu danych osobowych jako należących do kategorii podstawowych obowiązków pracowniczych oraz stanowczego egzekwowania ich wykonania przez zatrudnione osoby,
    d) Doskonalenia i rozwijania nowoczesnych metod zabezpieczenia danych przed zagrożeniami związanymi z ich przetwarzaniem, szczególnie w zakresie dotyczącym dynamicznego rozwoju metod i technik przetwarzania tych danych w systemach informatycznych oraz sieciach telekomunikacyjnych.
    e) Zapobiegania naruszeniom zasad i procedur określonych w dokumentacji z zakresu ochrony danych osobowych przez osoby upoważnione do przetwarzania danych osobowych, związane z nieprzestrzeganiem procedur ochrony danych, w tym zwłaszcza:
    - niezgodne z procedurami zakończenie pracy lub opuszczenie stanowiska pracy (nieprawidłowe wyłączenie komputera, niezablokowanie wyświetlenia treści pracy na ekranie komputera przed tymczasowym opuszczeniem stanowiska pracy, pozostawienie po zakończeniu pracy nieschowanych do zamykanych na klucz szaf dokumentów zawierających dane osobowe, niezamknięcie na klucz pokoju po jego opuszczeniu),
    - naruszenie bezpieczeństwa danych przez nieautoryzowane ich przetwarzanie,
    - ujawnienie osobom nieupoważnionym procedur ochrony danych stosowanych u administratora danych,
    - ujawnienie osobom nieupoważnionym danych przetwarzanych przez administratora danych, w tym również nieumyślne ujawnienie danych osobom postronnym, przebywającym bez nadzoru lub niedostatecznie nadzorowanym w pomieszczeniach administratora danych,
    - niewykonywanie stosownych kopii zapasowych,
    - przetwarzanie danych osobowych w celach prywatnych,
    - wprowadzanie zmian do systemu informatycznego administratora danych i instalowanie programów bez zgody administratora systemu.

2. Polityka Bezpieczeństwa w Urzędzie Gminy w Dąbrowie Chełmińskiej jest zbiorem zasad i procedur obowiązujących przy przetwarzaniu i wykorzystywaniu danych osobowych we wszystkich zbiorach danych osobowych administrowanych przez Wójta Gminy Dąbrowa Chełmińska.
3. Podstawą do opracowania i wdrożenia dokumentu są:
    a) Ustawa o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (tekst jednolity: Dz. U. 2015.poz 2135);
    b) Ustawa z dnia 8 marca 1990r. o samorządzie gminny (t.j. Dz. U. z 2015 r. poz. 1515,1890),
    c) Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 22 kwietnia 2004 r. w sprawie wzorów imiennego upoważnienia i legitymacji służbowej inspektora Biura Generalnego Inspektora Ochrony Danych Osobowych (Dz. U. z 2004 r. Nr 94, poz. 923) – art. 22a ustawy;
    d) Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 11 maja 2011 r. zmieniające rozporządzenie w sprawie wzorów imiennego upoważnienia i legitymacji służbowej inspektora Biura Generalnego Inspektora Ochrony Danych Osobowych (Dz. U. z 2011 r. Nr 103, poz. 601);
    e) 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. z 2004 r. Nr 100, poz. 1024) – art. 39a ustawy;
    f) Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 11 grudnia 2008 r. w sprawie wzoru zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (Dz. U. nr 229, poz. 1536) – art. 46a ustawy;
    g) Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 10 grudnia 2014 r. w sprawie wzorów zgłoszeń powołania i odwołania administratora bezpieczeństwa informacji (Dz. U. 2014, poz. 1934);
    h) Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015r. w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbiorów danych (Dz.U. 2015 poz. 719);
    i) Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015r. w sprawie trybu i sposobu realizacji zadań w celu zapewnienia przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji (Dz.U. 2015 poz. 745);
4. Przetwarzanie danych osobowych w Urzędzie Gminy w Dąbrowie Chełmińskiej jest dopuszczalne wyłącznie pod warunkiem przestrzegania ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych i wydanych na jej podstawie przepisów wykonawczych w tym niniejszej polityki i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, które powinny być spójne z polityką bezpieczeństwa informacji wymaganą przez ustawę o informatyzacji działalności podmiotów realizujących zadania publiczne.
5. Polityka Bezpieczeństwa ma zastosowanie do ochrony zbiorów danych osobowych przetwarzanych w Urzędzie Gminy w Dąbrowie Chełmińskiej, w celu ich bezpiecznego wykorzystania oraz określa zasady korzystania z systemów informatycznych.

§ 2

Określenia i skróty użyte w Polityce Bezpieczeństwa Informacji oznaczają:

1) **OchrDanychU** – ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz.U. z 2015 poz. 2135 ze zm.);
2) **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);
3) **Urząd** – Urząd Gminy w Dąbrowie Chełmińskiej;
4) **Administrator Danych Osobowych** – Wójta Gminy Dąbrowa Chełmińska, zwanego dalej „ADO";
5) **Administrator Bezpieczeństwa Informacji** – osobę powołaną przez Wójta Gminy Dąbrowa Chełmińska, wpisaną do prowadzonego przez Generalnego Inspektora Ochrony Danych Osobowych rejestru administratorów bezpieczeństwa informacji, , zwaną dalej „ABI";
6) **Administrator Systemów Informatycznych/Informatyk** – osobę wyznaczoną przez Wójta Gminy Dąbrowa Chełmińska, zwaną dalej „ASI/Informatyk";
7) **osoba upoważniona lub użytkownik systemu** – osobę posiadającą upoważnienie wydane przez ADO dopuszczoną jako użytkownik do przetwarzania danych osobowych w systemie informatycznym danej komórki organizacyjnej w zakresie wskazanym w upoważnieniu, zwaną dalej „użytkownikiem";
8) **osoby zatrudnione przy przetwarzaniu danych osobowych** – wszystkie osoby, w tym użytkowników systemu informatycznego, mające dostęp do danych osobowych.
9) **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;
10) **dane osobowe** - wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
11) **przetwarzanie danych** – 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;
12) **system informatyczny** - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych;
13) **system tradycyjny** - zespół procedur organizacyjnych, związanych z mechanicznym przetwarzaniem informacji i wyposażenia i środków trwałych w celu przetwarzania danych osobowych na papierze;
14) **siec telekomunikacyjna** – rozumie się przez to sieć telekomunikacyjną w rozumieniu art. 2 pkt. 23 ustawy z dnia 21 lipca 2000 r. – Prawo telekomunikacyjne (t.j. Dz. U. z 2014 r. poz. 243 z późn. zm.),
15) **teletransmisja** – rozumie się przez to przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej,
16) **usuwanie danych** - rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;
17) **identyfikator** - rozumie się przez to ciąg znaków literowych, cyfrowych lub innych,

jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym,

18) **hasło** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie użytkownikowi,
19) **integralność danych** – rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
20) **poufności danych** – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom,
21) **przetwarzającym** – rozumie się przez to podmiot, któremu zostało powierzone przetwarzanie danych osobowych na podstawie umowy zawieranej zgodnie z art. 31 OchrDanychU.

Rozdział II
Obszary przetwarzania danych osobowych

§ 3

1. Obszar przetwarzania danych osobowych w Urzędzie obejmuje budynek, pomieszczenia i części pomieszczeń, w których przetwarzane są dane osobowe (miejsca, w których wykonuje się operacje na danych osobowych, tj. wpisuje, zmienia, kopiuje) oraz miejsca, gdzie przechowuje się nośniki informacji zawierające dane osobowe (szafy z dokumentacją papierową, szafy zawierające elektroniczne nośniki informacji, pomieszczenia, w których składowane są uszkodzone nośniki danych).
2. Obszar przetwarzania danych osobowych określony jest w „Wykazie pomieszczeń, w których przetwarzane są dane osobowe", stanowiącym załącznik nr 1 do Polityki Bezpieczeństwa Informacji. Wykaz ten zawiera następujące informacje:
   1) lokalizację budynku,
   2) numer pomieszczenia i jego przeznaczenie,
   3) wskazanie piętra budynku,
   4) określenie referatu użytkującego dane pomieszczenie,
   5) wskazanie liczby osób pracujących w pomieszczeniu: wskazanie stanowisk i liczby osób,
   6) określenie zabezpieczenia pomieszczenia.
3. Obszar przetwarzania danych oraz warunki ochrony tego obszaru określone zostały w załączniku nr 2 do Polityki Bezpieczeństwa Informacji „Zasady ochrony pomieszczeń, w których przetwarzane są dane osobowe".

§ 4

1. Wykaz zbiorów danych przetwarzanych w Urzędzie Gminy określony został w załączniku nr 3 do Polityki Bezpieczeństwa Informacji – „Wykaz zbiorów danych osobowych i systemów do ich przetwarzania".
2. Szczegółowe informacje dotyczące stosowanego sprzętu oraz oprogramowania służącego do przetwarzania a danych osobowych zawiera załącznik nr 3 do Polityki Bezpieczeństwa Informacji..

§ 5

1. Strukturę oraz zakres zbiorów danych osobowych przetwarzanych w Urzędzie Gminy w Dąbrowie Chełmińskiej zawiera załącznik nr 5 do Polityki Bezpieczeństwa Informacji.
2. Przetwarzanie danych osobowych w Urzędzie Gminy odbywa się w sposób tradycyjny oraz na serwerze i na stacjach roboczych użytkowników.

§ 6

1. W ramach procesów przetwarzania danych ma miejsce przepływ danych pomiędzy różnymi systemami informatycznymi. Informacje na temat przepływu danych pomiędzy różnymi systemami informatycznymi znajdują się w „Wykazie zbiorów danych osobowych i systemów ich przetwarzania, o którym mowa w § 4 ust. 1".
2. Szczegółowe informacje dotyczące przepływu danych osobowych pomiędzy danymi systemami informatycznymi znajdują się w instrukcjach zarządzania danym systemem.

§ 7

W systemie informatycznym obowiązują zabezpieczenia na poziomie wysokim. Szczegółowe omówienie środków zabezpieczenia technicznego i organizacyjnego znajduje się w „Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie Gminy w Dąbrowie Chełmińskiej.", stanowiącej załącznik nr 2 do Zarządzenia nr ..... Wójta Gminy Dąbrowa Chełmińska z dnia .....

Rozdział III
Zarządzanie przetwarzaniem danych osobowych oraz czuwanie nad ich bezpieczeństwem

§ 8

1. Administrator danych osobowych:
   realizuje zadania w zakresie ochrony danych osobowych, w tym zwłaszcza:
   1) podejmuje decyzje o celach i środkach przetwarzania danych osobowych z uwzględnieniem przede wszystkim zmian w obowiązującym prawie, organizacji administratora danych oraz technik zabezpieczenia danych osobowych;
   2) upoważnia poszczególne osoby do przetwarzania danych osobowych w określonym indywidualnie zakresie, odpowiadającym zakresowi jej obowiązków;
   3) wyznacza administratora bezpieczeństwa informacji oraz określa zakres jego zadań i czynności;
   4) zapewnia użytkownikom odpowiednie stanowiska pracy umożliwiające bezpieczne przetwarzanie danych;
   5) podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia procedur bezpiecznego przetwarzania danych osobowych.

2. Administrator bezpieczeństwa informacji:
   realizuje zadania w zakresie nadzoru nad przestrzeganiem zasad ochrony danych osobowych, w tym zwłaszcza:
   1) sprawuje nadzór nad wdrożeniem stosownych środków fizycznych, a także organizacyjnych i technicznych – w celu zapewnienia bezpieczeństwa danych,
   2) sprawuje nadzór nad funkcjonowaniem systemu zabezpieczeń, w tym także nad prowadzeniem ewidencji z zakresu ochrony danych osobowych,
   3) prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych oraz pozostałej dokumentacji z zakresu ochrony danych,
   4) nadzoruje udostępnianie danych osobowych odbiorcom danych i innym podmiotom,
   5) przygotowuje wnioski zgłoszeń rejestracyjnych i aktualizacyjnych zbiorów danych oraz prowadzi inną korespondencję z Generalnym Inspektorem Ochrony Danych Osobowych,
   6) prowadzi oraz aktualizuje dokumentację opisującą sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych,
   7) podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia systemu informatycznego,

   W przypadku niewyznaczenia Administratora Bezpieczeństwa Informacji wymienione powyżej obowiązki pełni Administrator Danych Osobowych.
3. ADO powołuje zarządzającego oprogramowaniem, który przeprowadza okresową inwentaryzację oprogramowania oraz ustanawia zasady i procedury ciągłego utrzymania oprogramowania.
4. ADO powołuje Administratora Systemów Informatycznych (ASI) w przypadku niepowołania ASI, funkcję i jego zadnia wykonuje informatyk Urzędu Gminy zgodnie z zakresem obowiązków.
5. Osoba upoważniona do przetwarzania danych osobowych jest zobowiązana przestrzegać następujących
   zasad:
   1) może przetwarzać dane osobowe wyłącznie w zakresie ustalonym indywidualnie przez administratora danych w upoważnieniu i tylko w celu wykonywania nałożonych na nią obowiązków. Rozwiązanie stosunku pracy, odwołanie z pełnionej funkcji powoduje wygaśnięcie upoważnienia do przetwarzania danych osobowych;
   2) musi zachować w tajemnicy dane osobowe oraz przestrzegać procedur ich bezpiecznego przetwarzania. Przestrzeganie tajemnicy danych osobowych obowiązuje przez cały okres zatrudnienia u administratora danych, a także po ustaniu stosunku pracy lub odwołaniu z pełnionej funkcji;
   3) zapoznaje się z przepisami prawa w zakresie ochrony danych osobowych oraz postanowieniami niniejszej polityki i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych;
   4) stosuje określone przez administratora danych oraz administratora bezpieczeństwa informacji procedury oraz wytyczne mające na celu zgodne z prawem, w tym zwłaszcza adekwatne, przetwarzanie danych;
   5) zabezpiecza dane przed ich udostępnianiem osobom nieupoważnionym.

§ 9

1. W celu realizacji powierzonych zadań ABI w Urzędzie ma prawo:
   1) kontrolować komórki organizacyjne Urzędu w zakresie właściwego zabezpieczenia systemów informatycznych oraz pomieszczeń, w których przetwarzane są dane osobowe;
   2) wydawać polecenia kierownikom komórek organizacyjnych Urzędu w zakresie bezpieczeństwa danych osobowych;
   3) informować ADO o przypadkach naruszenia bezpieczeństwa danych osobowych;
   4) żądać od wszystkich pracowników Urzędu wyjaśnień w sytuacjach naruszenia bezpieczeństwa danych osobowych.
2. ABI w przeprowadza nie częściej niż raz w kwartale i nie rzadziej niż raz w roku sprawdzenie w zakresie przestrzegania przez użytkowników zasad określonych w polityce Bezpieczeństwa Informacji Urzędu Gminy w Dąbrowie Chełmińskiej oraz innych przepisów prawa w zakresie ochrony danych osobowych, z czego sporządza sprawozdanie.

§ 10

1. Wójt Gminy w Dąbrowie Chełmińskiej wyznacza jako osoby odpowiedzialne za zasoby zbiorów danych osobowych kierowników komórek organizacyjnych oraz osoby pracujące na samodzielnych stanowiskach w Urzędzie Gminy.
2. Wójt Gminy Dąbrowa Chełmińska zobowiązuje kierowników komórek w organizacyjnych oraz osób pracujące na samodzielnych stanowiskach do:
   1) zarządzania zbiorem danych osobowych w ramach zadań realizowanych przez siebie zadań zgodnie z zakresem obowiązków;
   2) występowania z wnioskiem wobec podległych pracowników, do ADO poprzez ABI o nadanie lub cofnięcie upoważnień dotyczących dostępu do zbiorów danych osobowych - wzór załącznik nr 6 do Polityki Bezpieczeństwa Informacji; wniosek przedkładany jest do ABI, który po zaakceptowaniu go, przygotowuje upoważnienie lub cofnięcie upoważnienia do przetwarzania danych osobowych;
   3) ASI/Informatyk po wydaniu upoważnienia przez ADO nadaje osobie upoważnionej indywidualny identyfikator użytkownika systemu informatycznego oraz nadaje pierwsze hasło dostępowe przekazywane wyłącznie użytkownikowi;
   4) zgłaszania do ABI zamiaru utworzenia zbioru danych osobowych oraz informacji dotyczących zmian w zakresie i sposobach przetwarzania tego zbioru;
   5) nadzoru nad udostępnianiem danych osobowych;
   6) przestrzeganie obowiązków dotyczących obszaru przetwarzania, wykazu osób upoważnionych do przetwarzania danych osobowych, zastosowania zabezpieczeń zbiorów;
   7) prowadzenia aktywnego i bieżącego nadzór nad osobami zatrudnionymi przy przetwarzaniu danych osobowych w kierowanym referacie, z uwzględnieniem zakresu odpowiedzialności za ochronę tych danych w stopniu odpowiednim do zadań wykonywanych przez te osoby przy przetwarzaniu danych osobowych,
   8) zapoznawanie pracowników mających dostęp do danych osobowych z przepisami dotyczącymi ochrony danych osobowych.

§ 11

1. ASI/informatyk odpowiada za bezpieczeństwo systemów informatycznych Urzędu.
2. Do obowiązków ASI/informatyka w zakresie ochrony danych osobowych należy w szczególności:
   1) zapewnienie bezpieczeństwo zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych osobowych w Urzędzie;
   2) nadzór nad naprawami, konserwacją i likwidacją urządzeń komputerowych, na których zapisane są dane osobowe;
   3) konserwacja, uaktualnianiem systemów służących do przetwarzania danych osobowych;
   4) podejmowanie działań zabezpieczających stan systemu informatycznego w Urzędzie w przypadku otrzymania informacji o naruszeniu zabezpieczeń informatycznych;
   5) wsparcie pracowników merytorycznych w zakresie przestrzegania zasad bezpieczeństwa udostępniania danych osobowych innym podmiotom drogą teletransmisji danych;
   6) podejmowanie działań w przypadku naruszeń w systemie zabezpieczeń;
   7) nadzór nad funkcjonowaniem mechanizmów uwierzytelniania użytkowników.

Rozdział IV
Gromadzenie danych osobowych

§ 12

Dane osobowe przetwarzane w Urzędzie mogą być uzyskiwane bezpośrednio od osób, których te dane dotyczą, lub z innych źródeł, w granicach dozwolonych przepisami prawa.

§ 13

1. Zebrane dane osobowe mogą być wykorzystane wyłącznie do celów, dla jakich zostały pozyskane. Po wykorzystaniu dane osobowe powinny być przechowywane w formie uniemożliwiającej identyfikację osób, których dotyczą.
2. W przypadku konieczności udostępnienia dokumentów i danych, wśród których znajdują się dane osobowe niemające bezpośredniego związku z celem udostępnienia, należy bezwzględnie dokonać ich anonimizacji.

§ 14

W przypadku gdy dane osobowe są niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem OchrDanychU albo są zbędne do realizacji celu, dla którego zostały zebrane, przetwarzający jest zobowiązany do ich uzupełnienia, uaktualnienia, sprostowania lub usunięcia.

Rozdział V
Przetwarzanie danych osobowych

§ 15

1. Kierownicy komórek organizacyjnych oraz osoby zatrudnione na samodzielnych stanowiskach obowiązane jest zgłaszać ABI zamiar utworzenia nowego zbioru danych osobowych zgodnie z wzorem wniosku stanowiącym załącznik nr 7 do Polityki Bezpieczeństwa Informacji.
2. ABI przygotowuje projekt zgłoszenia zbioru danych osobowych do rejestracji GIODO, jeżeli takie zgłoszenie jest ustawowo wymagane, na podstawie obowiązującego wzoru zgłoszenia.
3. ASI, w uzgodnieniu z ABI, określa warunki techniczne dotyczące zabezpieczeń w systemie informatycznym, o których mowa w części E i F zgłoszenia zbioru danych osobowych do rejestracji GIODO.
4. ABI sprawdza warunki techniczne dotyczące zabezpieczeń w systemie informatycznym opisane w części E i F zgłoszenia zbioru danych osobowych do rejestracji GIODO; w przypadku niewystarczającego poziomu zabezpieczeń występuje z wnioskiem do ASI o podniesienie poziomu zabezpieczeń.
5. Przygotowany przez ABI projekt zgłoszenia zbioru danych osobowych do rejestracji GIODO parafuje osoba sporządzająca wniosek o utworzenie nowego zbioru danych osobowych.
6. Parafowany wniosek ABI przedstawia do akceptacji ADO i zgłasza go do GIODO.
7. Kierownicy komórek organizacyjnych oraz osoby zatrudnione na samodzielnych stanowiskach zgłaszają do ABI w terminie 14 dni zmiany w przetwarzanych zbiorach danych - załącznik nr 7 do Polityki Bezpieczeństwa Informacji.
8. ASI zgłasza – w terminie 14 dni – zmiany dotyczące sposobu przetwarzania danych osobowych oraz ich zabezpieczeń w systemie informatycznym.
9. ABI przygotowuje aktualizację zbioru danych osobowych w terminie 30 dni od dnia dokonania zmiany w zbiorze, na podstawie obowiązującego wzoru. Przepisy ust. 2–7 stosuje się odpowiednio.

Rozdział VI
Obowiązek informacyjny

§ 16

1. Pracownicy przetwarzający danych osobowe, odpowiedzialni są za poinformowanie osób, których dane osobowe przetwarzają, o:
    1) adresie siedziby urzędu, pod którym dane są zbierane i przetwarzane;
    2) celu zbierania danych;
    3) dobrowolności lub obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej;
    4) prawie wglądu do treści swoich danych oraz możliwości ich poprawiania.
2. W przypadku zbierania danych osobowych nie bezpośrednio od osoby, której one dotyczą, osobę tę należy dodatkowo poinformować o źródle danych oraz o uprawnieniach wynikających z art. 32 ust. 1 pkt 7 i 8 OchrDanychU.
3. Wzór formularza stosowanego dla spełnienia obowiązków, o których mowa w ust. 1 i 2, stanowi

załącznik nr 8 do Polityki Bezpieczeństwa Informacji.

§ 17

1. Materiały dotyczące innej niż ustawowa działalności Urzędu mogą być wysyłane tylko do tych osób, które wcześniej wyraziły zgodę na piśmie na przetwarzanie ich danych osobowych w tym celu.
2. Kandydaci do pracy w Urzędzie w procesie rekrutacji są zobowiązani podpisać pisemną zgodę na przetwarzanie ich danych osobowych.
3. Dokumenty złożone w celu określonym w ust. 2 są przechowywane w komórce organizacyjnej, która przetwarza te dane, i są włączane do akt osobowych pracownika.
4. Dokumenty pozyskane w procesie rekrutacji po jej zakończeniu:
   1) w przypadku oryginałów są przesyłane osobom aplikującym;
   2) w przypadku uwierzytelnionych kopii są komisyjnie niszczone, nie wcześniej niż 14 i nie później niż 30 dni po zakończeniu rekrutacji.
5. Wzór formularza stosowanego dla spełnienia obowiązków wymienionych w ust. 2, stanowi załącznik 9 do Polityki Bezpieczeństwa Informacji.

Rozdział VII
Udostępnianie danych osobowych

§ 18

1. ADO udostępnia dane osobowe przetwarzane we własnych zbiorach tylko osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa.
2. Dane osobowe mogą być udostępniane w następujących przypadkach:
   1) na podstawie wniosku od podmiotu uprawnionego do otrzymywania danych osobowych na podstawie przepisów;
   2) na podstawie umowy z innym podmiotem, w ramach której istnieje konieczność udostępnienia danych;
   3) na podstawie wniosku osoby, której dane dotyczą.
3. Wniosek o udostępnienie danych osobowych musi być złożony wyłącznie w formie pisemnej. Powinien zawierać informacje umożliwiające wyszukanie żądanych danych osobowych w zbiorze oraz wskazywać ich zakres i przeznaczenie. Składający wniosek może złożyć go zgodnie ze wzorem określonym w załącznik nr 10 do Polityki Bezpieczeństwa Informacji lub pisemnie zawierając zakres zgodnie z załącznikiem nr 10 do Polityki Bezpieczeństwa Informacji .
4. Udostępniając dane osobowe należy zaznaczyć, że można je wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.
5. W przypadku żądania udzielenia informacji na temat przetwarzanych danych osobowych na pisemny wniosek pochodzący od osoby, której dane dotyczą, odpowiedź na wniosek następuje w terminie 30 dni od daty jego otrzymania.
6. Wniosek o udostępnienie przekazywany jest do pracownika merytorycznie odpowiedzialnego za załatwienie sprawy, który podejmuje decyzję o udostępnieniu danych po zasięgnięciu opinii bezpośredniego przełożonego.
7. W przypadkach skomplikowanych lub merytorycznie trudnych wniosek przekazywany jest ABI, który opiniuje decyzję o udostępnieniu danych osobowych i przekazuje ją kierownikowi

komórki organizacyjnej lub osobie pracującej na samodzielnym stanowisku.

8. Kierownik komórki organizacyjnej lub osoba pracująca na samodzielnym stanowisku odpowiedzialna za zbiór danych osobowych jest odpowiedzialny za przygotowanie danych osobowych do udostępnienia w zakresie wskazanym we wniosku.

§ 19

Odmowa udostępnienia danych osobowych następuje gdy bark jest podstawy prawnej do udostępnienia tych danych.

Rozdział VIII
Ochrona przetwarzania danych osobowych

§ 20

1. Do przetwarzania danych mogą być dopuszczeni pracownicy Urzędu posiadający upoważnienie nadane przez ADO. Wzór upoważnienia określa załącznik nr 11 do Polityki Bezpieczeństwa Informacji.
2. ABI prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych. Wzór ewidencji stanowi załącznik nr 12 do Polityki Bezpieczeństwa Informacji.

§ 21

1. ADO zobowiązany jest do zbierania, ewidencjonowania i przechowywania: oświadczeń osób przetwarzających dane osobowe o zachowaniu w tajemnicy danych, z którymi mają styczność, oraz środkach bezpieczeństwa stosowanych przy przetwarzaniu danych osobowych.
2. Wzór formularza oświadczenia stanowi załącznik nr 13 do Polityki Bezpieczeństwa Informacji.

§ 22

1. Powierzenie przetwarzania danych osobowych odbywa się zgodnie z art. 31 OchrDanychU na podstawie umowy zawartej na piśmie pomiędzy ADO a danym podmiotem, któremu zleca się czynności związane z przetwarzaniem danych osobowych.
2. Kierownik komórki organizacyjnej lub osoba zatrudniona na samodzielnym stanowisku informuje ABI o zamiarze powierzenia danych osobowych do przetwarzania innemu podmiotowi.
3. Pracownik merytoryczny odpowiedzialny za przetwarzanie zbioru przygotowuje projekt umowy powierzenia danych osobowych innemu podmiotowi.
4. W projekcie umowy należy określić zakres czynności związanych z przetwarzaniem powierzonych danych osobowych, zakres danych oraz wymagania dotyczące ochrony danych.
5. Każda osoba delegowana do wykonywania zadań na rzecz Urzędu Gminy w Dąbrowie Chełmińskiej, związanych z powierzeniem przetwarzania danych osobowych, obowiązana jest

podpisać oświadczenie o zachowaniu w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia.

6. Projekt umowy opiniują:
   a) ABI,
   b) ASI – jeżeli zlecenie czynności dotyczyć będzie przetwarzania danych w systemie informatycznym,
   c) radca prawny.
7. Zaparafowany projekt umowy jest przedkładany przez ABI do akceptacji i podpisu ADO. Wzór umowy powierzenia przetwarzania danych osobowych stanowi załącznik nr 14 do Polityki Bezpieczeństwa Informacji.

Rozdział IX
Postępowanie w przypadkach naruszenia bezpieczeństwa ochrony danych osobowych

§ 23

Przepisy niniejszego rozdziału stosuje się w przypadku:

1) stwierdzenia naruszenia zabezpieczenia systemu informatycznego (w obszarze danych osobowych;
2) podejrzenia naruszenia bezpieczeństwa danych osobowych

§ 24

Zasady postępowania przypadku naruszenia bezpieczeństwa danych osobowych obowiązują wszystkie osoby biorące udział w procesie przetwarzania danych osobowych.

§ 25

Naruszeniem zasad bezpieczeństwa danych osobowych jest każdy stwierdzony fakt nieuprawnionego ujawnienia danych osobowych, udostępnienia lub umożliwienia dostępu do nich osobom nieupoważnionym, zabrania danych przez osobę nieupoważnioną, uszkodzenia jakiegokolwiek elementu systemu informatycznego, a w szczególności:

1) nieautoryzowany dostęp do danych;
2) nieautoryzowane modyfikacje lub zniszczenie danych;
3) udostępnienie danych nieautoryzowanym podmiotom;
4) nielegalne ujawnienie danych;
5) pozyskiwanie danych z nielegalnych źródeł.

§ 26

1. W przypadku stwierdzenia naruszenia zabezpieczenia systemu informatycznego lub zaistnienia sytuacji, które mogą wskazywać na naruszenie bezpieczeństwa danych osobowych, każdy pracownik zatrudniony przy przetwarzaniu danych osobowych jest zobowiązany przerwać przetwarzanie danych osobowych i powiadomić o tym fakcie bezpośredniego przełożonego lub ABI, a następnie postępować stosownie do podjętej przez niego decyzji.

2. Zgłoszenie naruszenia ochrony danych osobowych powinno zawierać:
   1) opisanie działania wskazującego na naruszenie ochrony danych osobowych;
   2) określenie sytuacji i czasu, w jakim stwierdzono naruszenie ochrony danych osobowych;
   3) wskazanie istotnych informacji mogących wskazywać na przyczynę naruszenia;
   4) określenie znanych danej osobie sposobów zabezpieczenia systemu oraz wszelkich kroków podjętych po ujawnieniu zdarzenia.

§ 27

1. ABI podejmuje działania mające na celu:
   1) minimalizację negatywnych skutków zdarzenia;
   2) wyjaśnienie okoliczności zdarzenia;
   3) zabezpieczenie dowodów zdarzenia,
   4) umożliwienie dalszego bezpiecznego przetwarzania danych.
2. Dla realizacji celów określonych w ust. 1 ABI ma prawo do podejmowania wszelkich działań dopuszczonych przez prawo, w szczególności:
   1) żądania wyjaśnień od pracowników;
   2) korzystania z pomocy konsultantów;
   3) nakazania przerwania pracy, zwłaszcza w zakresie przetwarzania danych osobowych.

§ 28

Odmowa udzielenia wyjaśnień lub współpracy z ABI traktowane będzie jako naruszenie obowiązków pracowniczych.

§ 29

ABI po zapoznaniu z sytuacją i podjęciu czynności wyjaśniających lub naprawczych opracowuje raport końcowy, w którym przedstawia przyczyny i skutki zdarzenia oraz wnioski, w tym kadrowe, ograniczające możliwość wystąpienia zdarzenia w przyszłości; wzór raportu końcowego stanowi załącznik nr 15 do Polityki Bezpieczeństwa Informacji.

Załączniki nr 2 do Zarządzenia nr ..... Wójta Gminy Dąbrowa Chełmińska
z dnia.....

ZATWIERDZAM

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy w Dąbrowie Chełmińskiej

ADMINISTRATOR
Bezpieczeństwa Informacji
Robert Bagiński

.....

§ 1
Wprowadzenie

1. Niniejszą instrukcja określa zasady eksploatacji i zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie Gminy w Dąbrowie Chełmińskiej.
2. Zasady opisane w niniejszym dokumencie są zgodne z obowiązującymi wymaganiami prawnymi, w szczególności:
    1) ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz.U. z 2015 r. poz. 2135 ze zm.), zwaną dalej „OchrDanychU",
    2) 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, zwanym dalej „DokPrzetwR".
3. W instrukcji stosuje się następujące skróty:
    1) ABI – Administrator Bezpieczeństwa Informacji, realizujący czynności określone w art. 36a OchrDanychU;
    2) ASI/Informtyk – Administrator Systemu Informatycznego, odpowiedzialny za administrację systemami informatycznymi Urzędu.

§ 2
Procedura nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności

1. Podstawą do nadania uprawnień do przetwarzania danych osobowych w systemie informatycznym Urzędu jest upoważnienie do przetwarzania danych osobowych. Upoważnienie wydawane jest przez Administratora Danych Osobowych.
2. Upoważnienie wydawane jest na wniosek przełożonego danego pracownika, a w przypadku osoby zatrudnionej na podstawie umowy cywilno-prawnej na wniosek pracownika Urzędu koordynującego działania osoby, dla której upoważnienie jest wydawane.
3. Administrator Bezpieczeństwa Informacji przy nadawaniu uprawnień przez ADO stosuje przy następujące procedury:
    1) w przypadku gdy dana osoba otrzymuje po raz pierwszy upoważnienie do przetwarzania danych osobowych informuje ją o obowiązkach związanych z zapewnieniem ochrony danych osobowych;
    2) odbiera od powyższej osoby oświadczeniem o zapoznaniu się z obowiązującymi zasadami ochrony danych osobowych.
4. ABI prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych. Każda zmiana w zakresie informacji zawartych w ewidencji podlega niezwłocznemu odnotowaniu przez ABI.
5. Uprawnienia dostępu do systemu informatycznego nadawane są na podstawie wniosku przełożonego danego pracownika, a w przypadku osoby nie będącej pracownikiem Urzędu na wniosek pracownika Urzędu koordynującego działania danej osoby. Wniosek niniejszy kierowany jest do ABI i może być połączony z wnioskiem o nadanie upoważnienia do przetwarzania danych osobowych (wzór wniosku – załącznik nr 6 do PBI)

6. Za nadanie uprawnień w systemie informatycznym odpowiada ASI/Informatyk. Uprawnienia nie mogą być nadane w przypadku, jeżeli dana osoba nie posiada upoważnienia do przetwarzania danych osobowych w wymaganym zakresie.
7. ABI informuje osobę wnioskującą o fakcie nadania lub odmowy nadania upoważnienia - uprawnień.
8. W przypadku nadawania użytkownikowi uprawnień do danego systemu informatycznego po raz pierwszy, ASI/Informatyk dokonuje nadania użytkownikowi identyfikatora, wygenerowania hasła oraz przekazuje ABI nadany osobie identyfikator w celu aktualizacji ewidencji osób upoważnionych do przetwarzania danych osobowych.
9. Identyfikator użytkownika w systemie informatycznym musi być unikalny dla użytkownika i zawierać minimum 3 znaki. Nie może być to identyfikator, który w przeszłości był już stosowany w systemie informatycznym. Sprawdzenie unikalności identyfikatora odbywa się na podstawie ewidencji osób upoważnionych do przetwarzania danych osobowych.
10. Hasło użytkownika jest przydzielane indywidualnie każdemu z użytkowników i znane jest tylko użytkownikowi, który się nim posługuje.
11. ASI/Informatyk przekazuje użytkownikowi identyfikator i hasło.
12. Użytkownik jest zobowiązany do zmiany hasła przy pierwszym dostępie do systemu informatycznego.

§ 3

Procedura odbierania uprawnień do przetwarzania danych w systemie informatycznym

1. W przypadku konieczności odebrania lub zmiany zakresu upoważnienia – w związku ze zmianą zakresu obowiązków służbowych pracownika lub zakończeniem pracy – jego przełożony wnioskuje do ADO poprzez ABI o wykonanie powyższej czynności. ABI na podstawie decyzji ADO dokonuje, odebrania lub zmiany zakresu upoważnienia, o czym informuje ASI/Informatyka, który dokonuje odebrania lub zmiany zakresu uprawnień w systemie informatycznym. O powyższym ABI informuje osobę wnioskującą.
2. W przypadku konieczności odebrania lub zmiany zakresu upoważnienia dla osób nie będących pracownikami Urzędu o wykonanie powyższej czynności wnioskuje pracownik Urzędu koordynujący działania danej osoby.

§ 4

Stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem

1. Użytkownicy systemu informatycznego przetwarzającego dane osobowe wykorzystują w procesie uwierzytelnienia identyfikatory i hasła.
2. Identyfikator jest w sposób jednoznaczny przypisany użytkownikowi i nie podlega zmianie.
3. Nowe hasło jest przekazywane użytkownikowi przez ASI/Informatyk.
4. Po zalogowaniu do systemu z wykorzystaniem otrzymanego hasła użytkownik jest zobowiązany do dokonania jego natychmiastowej zmiany, nawet, jeżeli system informatyczny nie wymusza takiego działania.
5. Hasła dostępu do systemu informatycznego muszą spełniać poniższe warunki:
   1) posiadać długość co najmniej 8 znaków,
   2) zawierać litery małe i duże,
   3) zawierać cyfry lub znaki specjalne.

6. Użytkownik jest zobowiązany do zmiany hasła nie rzadziej niż co 30 dni, chyba że zmiana hasła jest wymuszona przez system informatyczny lub niezwłocznie w przypadku podejrzenia, iż mogły z nim się zapoznać nieuprawnione osoby. Hasło powinno różnić się od poprzednio używanego.
7. Użytkownik zobowiązany jest do:
   1) nieujawniania hasła innym osobom, w tym innym użytkownikom,
   2) zachowania hasła w tajemnicy, również po jego wygaśnięciu,
   3) niezapisywania hasła,
   4) postępowania z hasłami w sposób uniemożliwiający dostęp do nich osobom trzecim,
   5) przestrzegania zasad dotyczących jakości i częstości zmian hasła,
   6) wprowadzania hasła do systemu w sposób minimalizujący podejrzenie go przez innych użytkowników systemu.
8. W przypadku zapomnienia hasła użytkownik powinien zwrócić się do ASI/Informatyka o wygenerowanie nowego hasła.
9. W przypadku podejrzenia zapoznania się z hasłem przez osobę nieuprawnioną użytkownik jest zobowiązany do natychmiastowej zmiany hasła oraz powiadomienia o zaistniałym fakcie ABI.

§ 5

Procedura rozpoczęcia, zawieszenia i zakończenia pracy przeznaczona dla użytkowników systemu

1. Rozpoczynając pracę w systemie informatycznym przetwarzającym dane osobowe, użytkownik:
   1) uruchamia komputer,
   2) wprowadza niezbędne do pracy identyfikatory i hasła,
   3) hasła są wprowadzane w sposób minimalizujący ryzyko podejrzenia ich przez osoby trzecie,
   4) w przypadku problemów z rozpoczęciem pracy, spowodowanych odrzuceniem przez system wprowadzonego identyfikatora i hasła, zweryfikować poprawność wpisanych znaków (capslook, num lock, układ klawiatury), jeśli te czynności okażą się nieskuteczne skontaktować się z ASI/informatykiem,
   5) w przypadku niestandardowego zachowania aplikacji przetwarzającej dane osobowe pracownik natychmiast powiadamia o zaistniałym fakcie ABI.
2. Zawieszając pracę w systemie informatycznym (w tym odchodząc od stanowiska pracy), użytkownik blokuje stację roboczą. Kontynuacja pracy może nastąpić po odblokowaniu stacji roboczej po wprowadzeniu hasła, w sposób gwarantujący jego zachowanie jego poufności.
3. Na stacjach roboczych stosuje się wygaszacze ekranów aktywujące się po 5 minutach od moment braku aktywności w systemie informatycznym. Ponowne rozpoczęcie pracy następuje po wprowadzeniu identyfikatora oraz hasła.
4. Opuszczając pomieszczenie, w którym przetwarzane są dane osobowe, jeżeli w pomieszczeniu tym nie przebywa inna osoba upoważniona do przetwarzania danych osobowych, pracownik zobowiązany jest do zamknięcia pomieszczenia na klucz. Zabronione jest pozostawianie bez nadzoru pomieszczeń, w których przetwarzane są dane osobowe.
5. Kończąc pracę w systemie informatycznym pracownik wylogowuje się ze wszystkich aplikacji, z których korzystał, wyłącza stację roboczą i zabezpiecza nośniki danych. W przypadku gdy

pracownik jest ostatnią osobą opuszczającą pomieszczenie, sprawdza zamknięcie okien, zamyka na klucz drzwi do pomieszczenia oraz zdaje klucz w sekretariacie Urzędu.

§ 6

Procedura tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania

1. Za tworzenie i przechowywanie kopii zapasowych danych znajdujących się na serwerze odpowiedzialny jest ASI/Informatyk.
2. Kopie zapasowe systemów przetwarzających dane osobowe są codziennie zapisywane na zewnętrznych nośnikach pamięci. Zapis odbywa się po godzinach pracy Urzędu.
3. Nośniki pamięci oznaczane są w sposób umożliwiający określenie daty utworzenia kopii oraz nazwy systemu.
4. Utworzone kopie zapasowe podlegają weryfikacji ze względu na sprawdzenie możliwości odczytu danych.
5. ASI/Informatyk odpowiedzialny jest za realizację działań odtworzeniowych w przypadku konieczności podjęcia takich działań w związku z awarią systemu informatycznego Urzędu. Po odtworzeniu systemu informatycznego ASI/Informatyk odpowiedzialny jest za przeprowadzenie we współpracy z użytkownikiem testów poprawności działania systemu przed jego oddaniem do użytkowania.

§ 7

Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz nośników kopii zapasowych

1. Czas przechowywania tygodniowych kopii zapasowych określa się na jeden miesiąc od dnia wytworzenia.
2. Czas przechowywania miesięcznych kopii zapasowych określa się na jeden rok od dnia wytworzenia.
3. Czas przechowywania rocznej kopii zapasowej określa się na jeden rok od dnia wytworzenia.
4. Nośnik pamięci z kopiami zapasowymi przechowywane jest w szafie metalowej znajdującej się w kancelarii dokumentów niejawnych Urzędu.
5. Kopia zapasowa ustawień systemu operacyjnego dokonywana jest raz na kwartał i przechowywyana przez rok od dnia wytworzenia.
6. Dane osobowe przechowywane są w postaci elektronicznej na nośnikach elektronicznych wbudowanych w sprzęt informatyczny lub stanowiących element tego systemu.
7. Na nośnikach przenośnych dane przechowywane są jedynie w przypadkach, gdy jest to konieczne, nośnik powinien być opisany w sposób umożliwiający identyfikację zawartości danych na nim się znajdujących. Czas przechowywania danych na nośniku ma być niezbędny do spełnienia celu, w jakim zostały one na nośniku zapisane. Po ustaniu czasu przechowywania zawartość nośnika podlega on skasowaniu, a w przypadku nośników optycznych stosuje się niszczenie w niszczarkach umożliwiających niszczenie tego typu nośników (wzór protokołu załącznik nr 2 Instrukcji).
8. Obowiązek usunięcia danych z nośnika lub jego zniszczenie spoczywa na użytkowniku.
9. Dane osobowe w systemie informatycznym przechowywane są przez czas wymagany do spełnienia celu, dla którego są one przetwarzane. Po jego upływie dane podlegają skasowaniu lub anonimizacji.

10. Przenośne elektroniczne nośniki informacji zawierające dane osobowe są przechowywane przez pracowników w sposób minimalizujący ryzyko ich uszkodzenia lub zniszczenia, w szczególności w zamykanych szafach i meblach biurowych.
11. W przypadku wycofania sprzętu komputerowego z użycia dane osobowe na nim zapisane są kasowane przy użyciu dedykowanego oprogramowania do bezpiecznego usuwania danych . W przypadku braku możliwości programowego usunięcia danych, dysk podlega fizycznemu zniszczeniu. Za zniszczenie danych odpowiada ASI/Informatyk. Zniszczenie nośnika potwierdzane jest protokołem przechowywanym przez ABI, w skład komisji wchodzą ASI/Informatyk oraz użytkownik lub ABI oraz użytkownik, w uzasadnionych przypadkach Sekretarz Gminy lub kierownik komórki organizacyjnej użytkownika.(wzór protokołu załącznik nr 2 Instrukcji).
12. Dopuszcza się powierzenie niszczenia nośników danych wyspecjalizowanym podmiotom zewnętrznym, pod warunkiem:
    1) zawarcia umowy, o której mowa w art. 31 OchrDanychU,
    2) zagwarantowania poufności danych przez usługodawcę,
    3) umożliwienia prowadzenia nadzoru nad procesem niszczenia nośników przez ABI lub upoważnionego przez niego pracownika Urzędu,
    4) udokumentowania faktu zniszczenia nośników protokołem.

§ 8

Zasady korzystania z komputerów przenośnych, na których są przetwarzane dane osobowe

1. Przetwarzanie danych osobowych na komputerach przenośnych powinno być ograniczone do niezbędnych przypadków. Przetwarzanie danych osobowych przy użyciu komputerów przenośnych poza strefą przetwarzania danych osobowych może odbywać się wyłącznie za zgodą ADO i za wiedzą ABI. Zakres danych przetwarzanych na komputerze przenośnym oraz zakres uprawnień do przetwarzanych danych ustala przełożony pracownika za wiedzą ABI.
2. Osoba korzystająca z komputera przenośnego w celu przetwarzania danych osobowych zobowiązana jest do zwrócenia szczególnej uwagi na zabezpieczenie przetwarzanych informacji, zwłaszcza przed dostępem do nich osób nieupoważnionych oraz przed zniszczeniem. Użytkownik komputera przenośnego zobowiązany jest do:
    1) transportu komputera w sposób minimalizujący ryzyko kradzieży lub zniszczenia, a w szczególności:
        a) transportowania komputera w bagażu podręcznym,
        b) nie pozostawiania komputera w samochodzie, przechowalni bagażu, itp,
        c) zaleca się przenoszenie komputera w torbie przeznaczonej do przenoszenia komputerów przenośnych.
    2) korzystania z komputera w sposób minimalizujący ryzyko podejrzenia przetwarzanych danych przez osoby nieupoważnione, w szczególności zabrania się korzystania z komputera w miejscach publicznych i w środkach transportu publicznego,
    3) nie zezwalania osobom nieupoważnionym do korzystania z komputera przenośnego, na którym przetwarzane są dane osobowe,
    4) zabezpieczania komputera przenośnego hasłem,

5) blokowanie dostępu do komputera przenośnego w przypadku gdy nie jest on wykorzystywany przez pracownika,
6) kopiowanie danych osobowych przetwarzanych na komputerze przenośnym do systemu informatycznego w celu umożliwienia wykonania kopii awaryjnej tych danych,
7) umożliwienia, poprzez podłączenie komputera do sieci informatycznej aktualizacji wzorców wirusów w programie antywirusowym,
8) utrzymanie konfiguracji oprogramowania systemowego w sposób wymuszający zmianę z haseł, bądź zmianę hasła co 30 dni,
9) wykorzystywanie haseł odpowiedniej jakości zgodnie z wytycznymi dotyczącymi tworzenia haseł w systemie informatycznym przetwarzającym dane osobowe,
10) zmianę haseł zgodnie z wymaganiami dla systemu informatycznego przetwarzającego dane osobowe.

3. ASI/Informatyk zobowiązany jest do podjęcia działań mających na celu zabezpieczenie komputerów przenośnych, w szczególności aby:
   1) dokonano konfiguracji oprogramowania na komputerach przenośnych w sposób wymuszający korzystanie z haseł, jeżeli system umożliwia taką konfigurację. Wykorzystywanie haseł odpowiedniej jakości zgodnie z wytycznymi dotyczącymi tworzenia haseł w systemie informatycznym przetwarzającym dane osobowe oraz wymuszającym okresową zmianę haseł zgodnie z wymaganiami dla systemu informatycznego przetwarzającego dane osobowe,
   2) dokonano instalacji i konfiguracji oprogramowania antywirusowego na komputerze przenośnym.
4. W razie zgubienia lub kradzieży pracownik zobowiązany jest do natychmiastowego powiadomienia ADO lub ABI zgodnie z zasadami informowania o naruszeniu ochrony danych osobowych.

§ 9

Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem działania jest uzyskanie nieuprawnionego dostępu do systemu informatycznego

1. W celu zabezpieczenia systemu informatycznego przed działaniem niebezpiecznego oprogramowania zabrania się:
   1) instalowania jakiegokolwiek oprogramowania w tym wtyczki, rozszerzenia, aktualizacje oprogramowania przez użytkowania nie będącego ADI/Informatykiem;
   2) otwierając pocztę elektroniczną, nie otwierać odnośników zawartych w przesłanych w wiadomościach tzw. linków, załączniki zaś skanować programem antywirusowym; w przypadkach wątpliwych należy skonsultować się z ASI;
   3) korzystania z Internetu w celach nie związanych z pełnionymi obowiązkami służbowymi;
   4) podłączania do komputerów jakichkolwiek urządzeń zewnętrznych.
2. W przypadku zauważenia objawów mogących wskazywać na obecność niebezpiecznego oprogramowania użytkownik jest zobowiązany powiadomić ASI/Informatyka, który powiadamia ABI.
3. System informatyczny jest zabezpieczony przed działaniem niebezpiecznego oprogramowania poprzez:

1) oprogramowanie antywirusowe,
2) zaporę sieciową,
3) aktualizację oprogramowania systemowego,
4) konfigurację oprogramowania minimalizującą ryzyko naruszenia bezpieczeństwa.

4. ASI/Informatyk jest odpowiedzialny za nadzór nad działaniem powyższych zabezpieczeń, a w szczególności za:
   1) weryfikację aktualności sygnatur systemu antywirusowego i podejmowanie ewentualnych działań korekcyjnych,
   2) weryfikację logów systemu antywirusowego i podejmowanie działań korekcyjnych,
   3) przegląd logów zapory sieciowej oraz podejmowanie działań mających na celu zablokowanie ataków sieciowych,
   4) weryfikację poprawności aktualizacji oprogramowania systemowego.

§ 10

Procedura wykonywania przeglądu i konserwacji systemów oraz nośników informacji służących do przetwarzania danych osobowych

1. Przegląd i konserwacja sprzętu informatycznego realizowany jest przez upoważnionych pracowników Urzędu oraz przez podmioty zewnętrzne.
2. Prace serwisowe wykonywane na terenie Urzędu przez podmioty zewnętrzne podlegają bezpośredniemu nadzorowi ASI/Informatyka.
3. Przekazanie sprzętu teleinformatycznego do naprawy poza teren Urzędu jest dopuszczalne, jeżeli spełnione zostaną poniższe warunki:
   1) sprzęt przekazywany jest bez nośników zawierających dane osobowe, zaś fakt usunięcia nośników danych lub stwierdzenia braku nośników danych jest potwierdzany protokołem,
   2) przekazanie sprzętu potwierdzane jest protokołem, pozwalającym na jednoznaczne wskazanie osoby przekazującej i osoby odbierającej sprzęt.
4. Protokoły, o których mowa w punkcie 3, lub ich kopie przechowywane są przez ASI/Informatyka.
5. Wszelkie prace serwisowe wykonywane przez podmioty zewnętrzne wymagają sporządzenia protokołu serwisowego, zawierającego co najmniej poniższe informacje:
   1) wskazanie osoby przeprowadzającej prace serwisowe oraz podmiotu, którego osoba ta jest pracownikiem,
   2) wskazanie osoby nadzorującej przebieg prac serwisowych (dotyczy sytuacji, gdy prace realizowane są w siedzibie Urzędu),
   3) przedmiot prac serwisowych (w szczególności identyfikator sprzętu w przypadku prac serwisowych dotyczących sprzętu),
   4) zakres prac serwisowych i ich wynik,
   5) czas przeprowadzania prac serwisowych.
6. Awarie systemu informatycznego oraz naprawy są odnotowywane przez ASI/Informatyka w dzienniku – wzór załącznik nr 1 do Instrukcji.