Załącznik Nr 1 do zarządzenia Nr 42/07 Wójta Gminy Brańsk z dnia 8 października 2007 r.

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

W ZAKRESIE WYMOGÓW BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH

W

URZĘDZIE GMINY BRAŃSK

I. Postanowienia ogólne

§1.

1. Instrukcja określa procedury zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, zwanych dalej danymi, ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji w Urzędzie Gminy Brańsk zwanym dalej Urzędem.
2. Instrukcja pozwala stosować ujednolicone zasady ochrony danych w systemie i sieci informatycznej Urzędu.
3. Celem utworzenia instrukcji jest podniesienie poziomu bezpieczeństwa systemu informatycznego, w którym są gromadzone i przetwarzane dane oraz określenie odpowiedzialności pracowników Urzędu za prawidłowe działanie systemu i bezpieczeństwo przetwarzanych w nim danych.

§2.

Instrukcja w szczególności zawiera:

1. określenie procedury przydziału haseł dla użytkowników i częstotliwość ich zmiany, ze wskazaniem osoby odpowiedzialnej za te czynności,
2. określenie procedury rejestrowania i wyrejestrowywania użytkowników oraz wskazanie osoby odpowiedzialnej za te czynności,
3. procedury rozpoczęcia i zakończenia pracy w systemie informatycznym,
4. opis metod zabezpieczenia systemu informatycznego,
5. opis metod i harmonogram sprawdzania obecności wirusów komputerowych oraz metody ich usuwania,
6. procedurę i harmonogram dokonywania przeglądów i konserwacji systemu oraz zbiorów danych osobowych,

§3.

Określenia użyte w instrukcji oznaczają:

1. Ustawa – Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2002r. Nr 101 poz. 926, 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. 2004r. Nr 100 poz. 1024),
3. Urząd – Urząd Gminy Brańsk,

4. Naruszenie bezpieczeństwa systemu informatycznego – jakiekolwiek naruszenie poufności, integralności, dostępności do systemu informatycznego spowodowane przez ludzi, jak też powstałe na skutek oddziaływania sił przyrody, katastrof, itp.,
5. Administrator Danych - Wójt Gminy Brańsk,
6. Administrator Bezpieczeństwa - Administrator Bezpieczeństwa Informacji (osoba wyznaczona przez Wójta),
7. Administrator systemu – osoba zarządzająca bieżącą pracą systemu informatycznego i zbiorami danych (osoba wyznaczona przez Wójta).
8. System informatyczny Urzędu zwany dalej systemem – zespoły współpracujących ze sobą urządzeń, programów, procedur gromadzenia i przetwarzania informacji, narzędzi programowych zastosowanych do przetwarzania danych wraz ze zgromadzonymi danymi oraz osobami upoważnionymi do pracy na tym systemie (w tym obsługa techniczna urządzeń),
9. Przetwarzanie danych – jakiekolwiek operacje wykonywane na danych, takie jak utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie, przekazywanie i usuwanie, a zwłaszcza te, które wykonuje się w systemie informatycznym,
10. Obszar przetwarzania danych – obiekty, pomieszczenia, w których odbywa się gromadzenie i przetwarzanie danych w układach elektronicznych na nośnikach magnetycznych, optycznych (również w postaci papierowej np. kartoteki czy inne zbiory informacji), urządzenia, elementy techniczne, z których charakteru pracy wynika wydawanie informacji na zewnątrz tzn. monitory, drukarki itp.,
11. Zabezpieczenie danych w systemie – wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym pozyskiwaniem, gromadzeniem i przetwarzaniem,
12. Użytkownik systemu zwany dalej użytkownikiem:
    1) osoba zatrudniona przy przetwarzaniu danych, która posiada upoważnienie do obsługi systemu oraz urządzeń wchodzących w jego skład, a także osoba przetwarzająca dane w toku wykonywania umowy cywilnoprawnej zawartej z Urzędem (np. umowy zlecenia, umowy o dzieło, itp.),
    2) pracownik innego podmiotu, który świadczy usługi związane z pracą w systemie Urzędu, na podstawie odrębnych umów z tym podmiotem (np. serwis, zlecenie przetwarzania danych, itp.),
13. Gromadzenie danych – zbieranie na nośnikach elektronicznych oraz wydrukach danych.

§4.

1. Ochrona zasobów danych Urzędu jako całości, przed ich nieuprawnionym użyciem lub zniszczeniem, jest jednym z podstawowych obowiązków każdego pracownika Urzędu.

2. Obowiązkiem każdego pracownika Urzędu jest zachowanie tajemnicy służbowej, w tym ochrony danych osobowych gromadzonych i przetwarzanych przez Urząd. Obowiązek ten istnieje również po ustaniu zatrudnienia.
3. Osoby zatrudnione przy przetwarzaniu danych (także poza systemami) są zobowiązane do szczególnej dbałości o zachowanie poufności, integralności i dostępności do danych gromadzonych w kartotekach, skorowidzach itp. oraz infrastruktury sprzętowo – programowej systemu.

§5.

1. Za bezpieczeństwo danych osobowych Urzędu, odpowiadają:
   1) Administrator Danych Osobowych – Wójt Gminy Brańsk,
   2) Administrator Bezpieczeństwa Informacji – osoba wyznaczona przez Wójta.

§6.

1. Obszary przetwarzania danych w obiektach i pomieszczeniach Urzędu nie mogą być dostępne dla osób nieuprawnionych.
2. W pomieszczeniach, w których przyjmowani są interesanci należy stosować szczególne środki ostrożności, w tym:
   1) interesanci powinni pozostawać w pomieszczeniu tylko w obecności użytkownika systemu,
   2) kartoteki tradycyjne należy zabezpieczyć przed dostępem osób nieuprawnionych,
   3) nie należy pozostawiać dokumentów papierowych i nośników elektronicznych w miejscach umożliwiających ich wykorzystanie, przez osoby nieuprawnione,
   4) monitory powinny być usytuowane tak, aby ekrany były niewidoczne dla osób nieuprawnionych,
   5) drukarki i urządzenia peryferyjne powinny być usytuowane tak, aby nie znajdowały w przestrzeni, po której poruszają się osoby nieuprawnione,

§7.

System informatyczny w Urzędzie powinien być tak zaprojektowany, aby wymuszać autoryzację osoby przystępującej do pracy na zbiorach danych osobowych.

§8.

Odpowiedzialność za ochronę danych zawartych na komputerach przenośnych i innych przenośnych urządzeniach umożliwiających gromadzenie danych, spoczywa wyłącznie na dysponentach tych urządzeń; minimalnym wymaganym zabezpieczeniem każdego komputera PC

jak również komputera przenośnego jest ograniczenie dostępu do tego komputera hasłem, wygaszasz ekranu.

§9.

1. Wszelkie informacje zawierające dane, udostępniane podmiotom zewnętrznym, mogą zostać przekazane tylko za pośrednictwem kancelarii ogólnej.
2. W uzasadnionych przypadkach dane mogą być przesyłane drogą elektroniczną w formie zaszyfrowanej.

§10.

1. Zabrania się:
   1) udostępniania indywidualnych haseł dostępu innym osobom,
   2) dokonywania samowolnych napraw sprzętu informatycznego oraz modyfikowania oprogramowania,
   3) autoryzacji w systemie jako inny użytkownik,
   4) samodzielnego wgrywania oprogramowania,
   5) w celach innych niż służbowe, wynoszenia dokumentacji, w tym na nośnikach elektronicznych zawierającej dane, poza obszar jednostki organizacyjnej,
   6) wykorzystywania Internetu do celów innych niż służbowe.
2. Identyfikator i hasło osoby, która utraciła uprawnienia do korzystania z systemu są likwidowane niezwłocznie po utracie uprawnień lub ustaniu zatrudnienia przez Administratora Systemu
3. Identyfikator osoby, która utraciła uprawnienia i została wyrejestrowana z systemu nie może być przydzielony innej osobie.
4. Dostęp do poszczególnych elementów systemów bazodanowych powinien być realizowany tylko w zakresie określonym nadanymi uprawnieniami, po wydaniu upoważnienia użytkownikowi.

§11.

1. Administrator Bezpieczeństwa prowadzi następujące ewidencje:
   1) ewidencję osób upoważnionych do przetwarzania danych osobowych w systemie,
   2) rejestr zbiorów danych osobowych Urzędu (przetwarzanych metodą tradycyjną lub w systemie).
   3) wykaz oprogramowania w Urzędzie,
   4) ewidencję awaryjnego użycia haseł administratora systemu,

II. Procedury rejestrowania i wyrejestrowywania użytkowników

§12.

1. Pracownika Urzędu korzystającego z systemu i jego oprogramowania rejestruje się jako użytkownika.
2. Niedopuszczalna jest praca w systemie na koncie innego użytkownika.

§13.

W celu zarejestrowania osoby jako użytkownika systemu, Kierownik Referatu, w którym zatrudniona jest osoba, kieruje wniosek do Administratora Bezpieczeństwa, w którym określa konieczne uprawnienia (bądź zmianę, wycofanie uprawnień) ze szczególnym uwzględnieniem uprawnień do przetwarzania danych,

1. Osoby zatrudnione w Urzędzie potwierdzają własnoręcznym podpisem zapoznanie się z indywidualnym zakresem czynności osoby zatrudnionej przy przetwarzaniu w danych.
2. Osoby zatrudnione w Urzędzie podlegają szkoleniu przez Administratora Bezpieczeństwa w zakresie ochrony danych, po którym otrzymują upoważnienie do obsługi systemu informatycznego w zakresie przetwarzania danych.
3. Upoważnienie do obsługi systemu w zakresie przetwarzania danych podpisuje Administrator Danych, wprowadza do systemu Administrator Systemu

§14.

Nadawanie i rozszerzanie uprawnień użytkowników koordynuje Administrator Bezpieczeństwa.

§15.

Identyfikator użytkownika powinien spełniać następujące wymagania:

1. długość minimum trzy znaki,
2. musi być niepowtarzalny w skali systemu,
3. jednym identyfikatorem może posługiwać się tylko jeden użytkownik,
4. identyfikator pracownika, który rozwiązał umowę o pracę nie może zostać przydzielony innemu pracownikowi.

III. Budowa i procedura przydziału haseł dla administratora systemu i użytkowników oraz częstotliwość ich zmiany

§16.

Określa się następujące zasady tworzenia haseł.

1. Hasło musi mieć nie mniej niż 8 znaków.

2. Hasło musi zawierać znaki z wszystkich niżej wymienionych grup:

1) małe i duże litery,

2) cyfry, lub znaki specjalne,

3. W haśle nie wolno używać polskich znaków diakrytycznych lub innych znaków narodowych.

4. Hasło jest obowiązkowe dla każdego użytkownika, posiadającego identyfikator w systemie.

5.Po założeniu hasła przez administratora użytkownik ma obowiązek zarejestrować się do systemu i zmienić hasło.

§17.

Określa się następujące zasady korzystania z haseł:

1. Nie wolno powtórnie używać hasła raz użytego.
2. Hasło znane jest tylko użytkownikowi.
3. Przy wpisywaniu hasła nie jest ono wyświetlane na ekranie.
4. Użytkownik odpowiada za systematyczną zmianę haseł.
5. Hasła zmienia się nie rzadziej niż raz w miesiącu

§18.

Niedopuszczalne jest podawanie swojego hasła innym użytkownikom bądź osobom nie uprawnionym do pracy w systemie lub nie posiadającym uprawnień do przetwarzania danych.

§19.

1. Administrator systemu tworzy i zmienia hasła zgodnie z zasadami określonymi w niniejszej Instrukcji.
2. Hasła Administratora systemu, hasła do serwerów, aktywnych urządzeń sieci i istotnych programów konfiguracyjnych, administrator systemu umieszcza w zapieczętowanych kopertach i składa w obecności Administratora Bezpieczeństwa w metalowej szafie.

§20.

1. Zabrania się nadawania użytkownikom stacji roboczych uprawnień administratora stacji roboczej.

§21.

Zobowiązuje się administratora systemu do uruchomienia na stacjach lokalnych (roboczych) procedury automatycznego wymuszania przez te systemy zmiany hasła.

IV. Procedura rozpoczęcia i zakończenia pracy w systemie informatycznym

§22.

1. Użytkownik systemu musi być zarejestrowany przez administratora systemu jako użytkownik odpowiedniej aplikacji.
2. Włączając komputer w celu podjęcia pracy użytkownik dokonuje autoryzacji zgodnie z poleceniami wydawanymi przez system komputerowy ukazującymi się na ekranie monitora.
3. W przypadku pojawienia się trudności w autoryzacji, pomimo prawidłowo wykonanych czynności, użytkownik zobowiązany jest skontaktować się z administratorem systemu.
4. Jeżeli autoryzacja przebiegła prawidłowo, użytkownik dokonuje wyboru aplikacji, w której zamierza pracować.

§23.

Obowiązkiem każdego pracownika jest dbałość o nie pozostawianie stanowiska informatycznego z dostępem do systemu bazodanowego, bez należytego zabezpieczenia, w tym:

1. opuszczając stanowisko pracy należy wylogować się z systemu,
2. przy krótkotrwałych przerwach w pracy należy zablokować stację roboczą.

§24.

Kończąc pracę w systemie użytkownik zamyka wszystkie otwarte aplikacje, a następnie zamyka system postępując zgodnie z ukazującymi się na ekranie monitora komunikatami.

V. Obszary przetwarzania danych

§25.

W celu zapewnienia bezpiecznych warunków przetwarzania danych określa się obszary przetwarzania danych jako:

1. wydzielone pomieszczenia lub części pomieszczeń, w których przetwarzane są dane (także w postaci tradycyjnej – papierowej),
2. części obiektów, w których znajdują się informatyczne urządzenia wyjścia (np. monitory, drukarki itp.).

§26.

Pomieszczenie określone jako obszar przetwarzania danych powinno spełniać następujące warunki:

1. być wyposażone w zamek mechaniczny lub elektroniczny zamykany każdorazowo, gdy opuszczają je pracownicy,

2. jeżeli pomieszczenie znajduje się na parterze, lub istnieje możliwość podglądu z zewnątrz, ekrany monitorów umieszcza się w sposób uniemożliwiający taki podgląd,
3. monitory komputerów, na których wykonuje się przetwarzanie danych powinny być ustawione w sposób uniemożliwiający ich podgląd osobom nieuprawnionym.

§27.

Wydzielona część pomieszczenia określona jako obszar przetwarzania danych powinna spełniać następujące warunki:

1. wyposażenie (meble) w tej części pomieszczenia muszą być tak ustawione, aby uniemożliwić lub istotnie utrudnić dostęp do tego obszaru osobom nieuprawnionym,
2. monitory komputerów, na których dokonuje się przetwarzania danych powinny być ustawione w sposób uniemożliwiający ich podgląd osobom nieuprawnionym.

§28.

Nadzór nad przestrzeganiem zasad ochrony przetwarzanych danych sprawuje Administrator Bezpieczeństwa.

VI. Opis metod i harmonogram sporządzania kopii bezpieczeństwa

§29.

1. Do sporządzania kopii zabezpieczających plików aplikacji i baz danych oraz systemów operacyjnych jest upoważniony administrator systemu i ponosi pełną odpowiedzialność w tym zakresie.
2. Z kopii bezpieczeństwa mogą być odtwarzane zbiory danych, uprawnienia użytkowników i ustawienia związane ze specyfiką i uwarunkowaniami systemu.
3. Odtwarzania dokonuje administrator systemu.

§30.

1. Kopie bezpieczeństwa powinny być przechowywane w metalowej szafie.
2. Dostęp do kopii bezpieczeństwa posiada administrator systemu, a w razie jego nieobecności: Administrator Bezpieczeństwa oraz Administrator Danych.
3. Elektroniczne nośniki informacji zawierające dane powinny być przechowywane w metalowej szafie.
4. Dane z magnetycznych nośników informacji usuwa się bezzwłocznie po ich wykorzystaniu służbowym w sposób trwały.

§31.

1. Co najmniej raz na kwartał administrator systemu dokonuje sprawdzenia zasobów kopii bezpieczeństwa pod kątem ich przydatności do odtworzenia danych w przypadku awarii systemu.
2. Kopie bezpieczeństwa, które uległy uszkodzeniu, lub zdezaktualizowały się, podlegają bezzwłocznemu zniszczeniu.
3. Zniszczenia kopii bezpieczeństwa lub innego nośnika zawierającego dane, dokonuje się komisyjne na polecenie Administratora Bezpieczeństwa. Z wykonanych czynności sporządza się protokół zniszczenia.(wzór – zał. Nr 4)

§32.

Opisu czynności sporządzania, okresowego sprawdzania, niszczenia kopii bezpieczeństwa, jak też odtwarzania danych z tych kopii, dokumentuje się w „Dzienniku ewidencji kopii bezpieczeństwa", który przechowywany jest przez administratora systemu. (wzór – zał. Nr 5)

§33.

Nadzór nad procesem sporządzania, przechowywania i niszczenia kopii bezpieczeństwa sprawuje Administrator Bezpieczeństwa.

§34.

Sposób i częstotliwość tworzenia awaryjnych kopii systemu operacyjnego serwerów:

1. Kopia systemu operacyjnego powinna być wykonywana po każdej modyfikacji, zmianie, konfiguracji i instalacji nowej wersji oprogramowania.
2. Powinny istnieć przynajmniej dwa zestawy takiej kopii zapisywane naprzemiennie, kopie takie powinny być okresowo sprawdzane pod kątem ich przydatności – prawidłowości wykonania oraz możliwości odtwarzania.

§35.

Metoda i częstotliwość tworzenia awaryjnych kopii danych:

1. Pełna kopia zabezpieczająca plików aplikacji i bazy danych systemów wykonywana jest co najmniej raz w miesiącu.
2. Każda kopia powinna zostać opisana w taki sposób, by zawierała następujące informacje:
   1) data wykonania,
   2) nazwa systemu informatycznego,

3) nazwa zbioru danych.

VII. Opis metod zabezpieczenia systemu informatycznego

§36.

Każda stacja robocza na której przetwarza się dane osobowe powinna być wyposażona w zasilacz awaryjny

§37.

1. Bieżące sprawdzanie obecności wirusów komputerowych realizuje się przez stosowanie oprogramowania monitorującego występowanie wirusów.
2. Sprawdzaniu obecności wirusów podlegają wszystkie informatyczne nośniki danych.
3. Sprawdzanie obecności wirusów na dyskach serwerów przeprowadza Administrator systemu.
4. Administrator systemu zobowiązany jest do zapewnienia systematycznej aktualizacji programu antywirusowego.
5. Sprawdzanie obecności wirusów na dyskach stacji roboczej odbywa się automatycznie po uruchomieniu komputera.

§38.

1. O wykryciu wirusa na stacji roboczej użytkownik powiadamia administratora systemu.
2. Nie podejmuje dalszych działań do czasu przybycia administratora systemu.
3. Administrator systemu o przypadku stwierdzenia szczególnie groźnych lub trudnych do usunięcia wirusów komputerowych powiadamia Administratora Bezpieczeństwa Informacji.

§39.

Po dokonanej naprawie lub konserwacji należy przeprowadzić proces sprawdzenia pod kątem występowania wirusów.

§40.

Informatyczne nośniki informacji pochodzenia zewnętrznego podlegają sprawdzeniu programem antywirusowym przed rozpoczęciem korzystania z nich.

§41.

1. Nadzór nad prawidłowym funkcjonowaniem oprogramowania antywirusowego sprawuje administrator systemu.

2. Administrator systemu zobowiązany jest do przeprowadzania systematycznej kontroli antywirusowej serwerów.

§42.

Zabrania się użytkownikom dokonywania samodzielnej instalacji jakiegokolwiek oprogramowania. Instalacji oprogramowania dokonuje administrator systemu, lub pracownik innego podmiotu, który świadczy usługi związane z pracą w systemie Urzędu, na podstawie odrębnych umów z tym podmiotem (np. serwis)

VIII. Procedura i harmonogram dokonywania przeglądów i konserwacji systemów oraz zbiorów danych.

§43.

Przeglądu i konserwacji systemu i zbioru danych dokonuje administrator systemu, lub pracownik innego podmiotu, który świadczy usługi związane z pracą w systemie Urzędu, na podstawie odrębnych umów z tym podmiotem (np. serwis)

.

§44.

1. Przegląd systemu polega na sprawdzeniu jego konfiguracji oraz sprawdzeniu loginów systemowych.
2. Przeglądu systemu dokonuje się nie rzadziej niż co 6 miesięcy
3. W przypadku stwierdzenia nieprawidłowości w systemie, administrator systemu usuwa je, wykorzystując dostępne narzędzia.
4. Jeżeli stwierdzone nieprawidłowości wskazują na działanie osób nieuprawnionych w systemie, administrator systemu podejmuje czynności zgodnie z zapisami „Instrukcji postępowania w sytuacji naruszenia ochrony danych osobowych w Urzędzie".

§45.

1. Przegląd zbiorów danych polega na:
   1) sprawdzeniu dostępu do zbiorów danych na poziomie użytkowników o różnych prawach dostępu,
   2) ocenie stanu zbiorów danych,
   3) sprawdzeniu ustawień dostępu dla poszczególnych użytkowników.
2. Przeglądu zbiorów danych dokonuje się nie rzadziej niż co 6 miesięcy.
3. W przypadku stwierdzenia nieprawidłowości w stanie zbiorów danych lub naruszenia praw

dostępu, administrator systemu powiadamia o zaistniałym fakcie Administratora Bezpieczeństwa, a następnie podejmuje działania zmierzające do usunięcia nieprawidłowości i zidentyfikowania osoby, która doprowadziła do ich powstania.

4. W przypadku wykrycia użytkowników nieuprawnionych, których działania mogły doprowadzić do: przeglądania, przenikania, wnioskowania, zniekształcania, powtarzania, wstawiania, niszczenia, kradzieży, modyfikacji, szpiegostwa, blokowania usług systemu, itp., administrator systemu podejmuje czynności zgodnie z zapisami „Instrukcji postępowania w sytuacji naruszenia ochrony danych osobowych w Urzędzie".

IX. Postanowienia końcowe

§46.

Przestrzeganie postanowień niniejszej Instrukcji przez użytkowników systemu stanowi podstawę bezpiecznego posługiwania się systemem.

§47.

Administrator Bezpieczeństwa okresowo monitoruje przestrzeganie przez pracowników zasad i przepisów ochrony danych osobowych.

§48.

W kwestiach nie uregulowanych niniejszą Instrukcją mają zastosowanie unormowania Regulaminu Pracy Urzędu, przepisy Kodeksu Pracy i Ustawy o ochronie danych osobowych wraz z aktami wykonawczymi.

X. Spis załączników

Załącznik nr 1 – Wniosek o założenie profilu/nadanie uprawnień/modyfikację uprawnień

Załącznik nr 2 – Upoważnienie do obsługi systemu informatycznego w zakresie przetwarzania danych osobowych

Załącznik nr 3 - Ewidencja osób upoważnionych do przetwarzania danych osobowych w systemach informatycznych

Załącznik nr 4 – Protokół zniszczenia kopii bezpieczeństwa / innych nośników zawierających dane osobowe

Załącznik nr 5 – Dziennik ewidencji kopii bezpieczeństwa

Załącznik nr 1 do Instrukcji zarządzania systemami informatycznymi w zakresie wymogów bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy Brańsk.

Wniosek
o założenie profilu/nadanie uprawnień/modyfikację uprawnień *

Dane użytkownika

Nazwisko	
Imię	
Stanowisko służbowe	
Komórka organizacyjna.	

Wnioskuję o :

założenie profilu i nadanie uprawnień*)

modyfikację uprawnień na wymienione poniżej*)

zablokowanie profilu*)

Wnioskowane uprawnienia do systemu

.....

(nazwa bazy danych) [1]

Uprawnienie, które ma być przyznane pracownikowi, należy zaznaczyć w pierwszej kolumnie znakiem „x".

TAK	Opis uprawnienia	Uwagi
	zarządzanie bazą	
	edycja danych (w tym drukowanie, usuwanie)	
	zakładanie nowych kont	
	dodawanie i modyfikacja danych	
	przeglądanie danych na ekranie	
	drukowanie danych	
	wykonywanie kopii archiwalnych	

Wniosek o nadanie / modyfikację uprawnień złożył :

Nazwisko i imię : _____ Dnia : / / _____

Podpis : _____

* - niepotrzebne skreślić

1 - nazwa bazy danych z załącznika nr 2 do „Polityki bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Urzędzie Gminy Brańsk"

15□ / 19□

Załącznik nr 5 do Instrukcji zarządzania systemami informatycznymi w zakresie wymogów bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy Brańsk.

DZIENNIK EWIDENCJI KOPII BEZPIECZEŃSTWA

Lp.	Oznaczenie systemu/ zbioru danych	Określenie metody (całościowa, przyrostowa)	Oznaczenie nośnika, na którym utworzono kopię awaryjną	Kopię bezpieczeństwa utworzył:			Kopię bezpieczeństwa zniszczył:			Uwagi
				Nazwisko i imię administratora systemu	Data	Podpis	Nazwisko i imię przewodniczącego komisji	Data	Podpis	
1	2	3	4	5	6	7	8	9	10	11

19□ / 19□