Załącznik do zarządzenia nr 120/2011
Wójta Gminy Dobra z dnia 1.08.2011r.

Polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych

w Urzędzie Gminy Dobra

Opracował : Łukasz Dziuban
/ imię i nazwisko /

Administrator Bezpieczeństwa Informacji

SPIS TREŚCI:

WPROWADZENIE

Niniejszy dokument opisuje reguły dotyczące bezpieczeństwa danych osobowych zawartych w systemach informatycznych w Urzędzie Gminy Dobra. Opisane reguły określają granice dopuszczalnego zachowania wszystkich użytkowników systemów informatycznych wspomagających pracę Urzędu. Dokument zwraca uwagę na konsekwencje jakie mogą ponosić osoby przekraczające określone granice oraz procedury postępowania dla zapobiegania i minimalizowania skutków zagrożeń.

Odpowiednie zabezpieczenia, ochrona przetwarzanych danych oraz niezawodność funkcjonowania są podstawowymi wymogami stawianymi współczesnym systemom informatycznym.

Dokument „Polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Dobra", zwany dalej „Polityką bezpieczeństwa", wskazujący sposób postępowania w sytuacji naruszenia bezpieczeństwa danych osobowych w systemach informatycznych, przeznaczony jest dla osób zatrudnionych przy przetwarzaniu tych danych.

Potrzeba jego opracowania wynika z § 4 rozporządzenia Prezesa Rady Ministrów z dnia 25 sierpnia 2005 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz. U. Nr 171, poz. 1433) oraz § 3 i 4 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. Nr 100, poz. 1024).

1. „Polityka bezpieczeństwa" określa tryb postępowania w przypadku, gdy:

    1) stwierdzono naruszenie zabezpieczenia systemu informatycznego,
    2) stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci informatycznej mogą wskazywać na naruszenie zabezpieczeń tych danych.

2. „Polityka bezpieczeństwa" obowiązuje wszystkich pracowników Urzędu Gminy Dobra.

3. Wykonywanie postanowień tego dokumentu ma zapewnić właściwą reakcję, ocenę i udokumentowanie przypadków naruszenia bezpieczeństwa systemów oraz zapewnić właściwy tryb działania w celu przywrócenia bezpieczeństwa danych przetwarzanych w systemach informatycznych Urzędu.

4. Administrator danych, którym jest Wójt, swoją decyzją wyznacza Administratora Bezpieczeństwa Informacji danych zawartych w systemach informatycznych Urzędu, zwanego dalej "Administratorem Bezpieczeństwa" oraz osobę upoważnioną do zastępowania „Administratora Bezpieczeństwa".

5. ”Administrator bezpieczeństwa” realizuje zadania w zakresie ochrony danych, a w szczególności:

   1) ochrony i bezpieczeństwa danych osobowych zawartych w zbiorach systemów informatycznych Urzędu,
   2) podejmowania stosownych działań zgodnie z niniejszą „Polityką bezpieczeństwa” w przypadku wykrycia nieuprawnionego dostępu do bazy danych lub naruszenia zabezpieczenia danych znajdujących się w systemie informatycznym,
   3) niezwłocznego informowania Administratora danych lub osoby przez niego upoważnionej o przypadkach naruszenia przepisów ustawy o ochronie danych osobowych,
   4) nadzoru i kontroli systemów informatycznych służących do przetwarzania danych osobowych i osób przy nim zatrudnionych.

6. Osoba zastępująca Administratora Bezpieczeństwa powyższe zadania realizuje w przypadku nieobecności Administratora Bezpieczeństwa.

7. Osoba zastępująca składa Administratorowi Bezpieczeństwa relację z podejmowanych działań w czasie jego zastępstwa.

Rozdział 1

OPIS ZDARZEŃ NARUSZAJĄCYCH OCHRONĘ DANYCH OSOBOWYCH

1. Podział zagrożeń:

   1) zagrożenia losowe zewnętrzne (np. klęski żywiołowe, przerwy w zasilaniu), ich występowanie może prowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej systemu, ciągłość systemu zostaje zakłócona, nie dochodzi do naruszenia poufności danych,
   2) zagrożenia losowe wewnętrzne (np. niezamierzone pomyłki operatorów, administratora, awarie sprzętowe, błędy oprogramowania), może dojść do zniszczenia danych, może zostać zakłócona ciągłość pracy systemu, może nastąpić naruszenie poufności danych,
   3) zagrożenia zamierzone, świadome i celowe - najpoważniejsze zagrożenia, naruszenia poufności danych, (zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy), zagrożenia te możemy podzielić na: nieuprawniony dostęp do systemu z zewnątrz (włamanie do systemu), nieuprawniony dostęp do systemu z jego wnętrza, nieuprawniony przekaz danych, pogorszenie jakości sprzętu i oprogramowania, bezpośrednie zagrożenie materialnych składników systemu.

2. Przypadki zakwalifikowane jako naruszenie lub uzasadnione podejrzenie naruszenia zabezpieczenia systemu informatycznego, w którym przetwarzane są dane osobowe to głównie:

   1) sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu jak np.: wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej itp.,
   2) niewłaściwe parametry środowiska, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy lub wibracje pochodzące od urządzeń przemysłowych,
   3) awaria sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych lub wręcz sabotaż, a także niewłaściwe działanie serwisu, a w tym sam fakt pozostawienia serwisantów bez nadzoru,
   4) pojawienie się odpowiedniego komunikatu alarmowego od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu,
   5) jakość danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie,
   6) nastąpiło naruszenie lub próba naruszenia integralności systemu lub bazy danych w tym systemie,
   7) stwierdzono próbę lub modyfikację danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji),
   8) nastąpiła niedopuszczalna manipulacja danymi osobowymi w systemie,
   9) ujawniono osobom nieupoważnionym dane osobowe lub objęte tajemnicą procedury ochrony przetwarzania albo inne strzeżone elementy systemu zabezpieczeń,
   10) praca w systemie lub jego sieci komputerowej wykazuje nieprzypadkowe odstępstwa od założonego rytmu pracy wskazujące na przełamanie lub zaniechanie ochrony danych osobowych - np. praca przy komputerze lub w sieci osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu, itp.,
   11) ujawniono istnienie nieautoryzowanych kont dostępu do danych lub tzw. "bocznej furtki", itp.,

12) podmieniono lub zniszczono nośniki z danymi osobowymi bez odpowiedniego upoważnienia lub w sposób niedozwolony skasowano lub skopiowano dane osobowe,
13) rażąco naruszono dyscyplinę pracy w zakresie przestrzegania procedur bezpieczeństwa informacji (nie wylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych osobowych w drukarce, na ksero, nie zamknięcie pomieszczenia z komputerem, nie wykonanie w określonym terminie kopii bezpieczeństwa, prace na danych osobowych w celach prywatnych, itp.).

3. Za naruszenie ochrony danych uważa się również stwierdzone nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania danych osobowych (otwarte szafy, biurka, regały, urządzenia archiwalne i inne) na nośnikach tradycyjnych tj. na papierze (wydrukach), kliszy, folii, zdjęciach, dyskietkach w formie niezabezpieczonej itp.

Rozdział 2

ZABEZPIECZENIE DANYCH OSOBOWYCH

1. Administratorem danych osobowych zawartych i przetwarzanych w systemach informatycznych Urzędu Gminy Dobra jest Wójt.

2. Administrator danych osobowych jest obowiązany do zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych w systemach informatycznych Urzędu, a w szczególności:

   1) zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym,
   2) zapobiegać przed zabraniem danych przez osobę nieuprawnioną,
   3) zapobiegać przetwarzaniu danych z naruszeniem ustawy oraz zmianie, utracie, uszkodzeniu lub zniszczeniu tych danych.

3. Do zastosowanych środków technicznych należy:

   1) przetwarzanie danych osobowych w wydzielonych pomieszczeniach położonych w strefie administracyjnej,
   2) zabezpieczenie wejścia do pomieszczeń, o których mowa w pkt. 1,
   3) szczególne zabezpieczenie centrum przetwarzania danych (komputer centralny, serwerownia) poprzez zastosowanie systemu kontroli dostępu,
   4) wyposażenie pomieszczeń w szafy dające gwarancję bezpieczeństwa dokumentacji.

4. Do zastosowanych środków organizacyjnych należą przede wszystkim następujące zasady:

   1) zapoznanie każdej osoby z przepisami dotyczącymi ochrony danych osobowych, przed dopuszczeniem jej do pracy przy przetwarzaniu danych osobowych,
   2) przeszkolenie osób, o których mowa w pkt. 1, w zakresie bezpiecznej obsługi urządzeń i programów związanych z przetwarzaniem i ochroną danych osobowych,
   3) kontrolowanie otwierania i zamykania pomieszczeń, w których są przetwarzane dane osobowe, polegające na otwarciu pomieszczenia przez pierwszą osobę, która rozpoczyna pracę oraz zamknięciu pomieszczenia przez ostatnią wychodzącą osobę.

5. Niezależnie od niniejszych zasad opisanych w dokumencie „Polityka bezpieczeństwa" w zakresie bezpieczeństwa mają zastosowanie wszelkie wewnętrzne regulaminy lub instrukcje dotyczące bezpieczeństwa ludzi i zasobów informacyjnych oraz indywidualne zakresy zadań osób zatrudnionych przy przetwarzaniu danych osobowych w określonym systemie.

6. Wykaz pomieszczeń w których przetwarzane są dane osobowe oraz opis systemów informatycznych Urzędu Gminy Dobra zawierają następujące załączniki do niniejszego dokumentu:
   1) **załącznik nr 1** - budynek główny, ul. Szczecińska 16A, Dobra,
   2) **załącznik nr 2** - budynek Wydział ds. Komunalnych i Inwestycji – ul. Szczecińska 24A, Dobra ,
   3) **załącznik nr 3** - budynek Wydział ds. Obywatelskich – ul. Lipowa 52 Wołczkowo,
   4) **załącznik nr 4** – Budynek Straży Gminnej – ul. Daniela 32, Dołuje,
   5) **załącznik nr 5** - Pomieszczenie Gminnego Centrum Informacji – ul. Żubrza 7, Dołuje

7. Opis struktur zbiorów danych określa **załącznik nr 6**.

8. W celu ochrony przed utratą danych w Urzędzie Gminy Dobra stosowane są następujące zabezpieczenia:

   1) Budynek główny – ul. Szczecińska 16A, Dobra:
   a) jednostki komputerowe podłączone są pod zasilacze UPS,
   b) serwer podłączony jest pod zasilacz UPS,
   c) na serwerze wykonywana jest codzienna podwójna kopia zapasowa – jedna na dodatkowy dysk zamontowany w serwerze, zaś druga na dysk zewnętrzny. Raz w miesiącu kopie zapasowe zlokalizowane na dysku zewnętrznym zgrywane są na nośnik optyczny, po czym trafiają do szafy pancernej,
   d) pracownicy mający dostęp do programów i baz danych dodatkowo wykonują kopie zapasową używanych przez siebie programów na dysk przenośny lub pamięć pendrive,
   e) jednostki komputerowe oraz serwer są wyposażone w system antywirusowy.

   2) Budynek Wydział ds. Komunalnych i Inwestycji – ul. Szczecińska 24A, Dobra:
   a) jednostki komputerowe podłączone są pod zasilacze UPS,
   b) jednostka komputerowa pełniąca rolę serwera plików podłączona jest do zasilacza UPS,
   c) na jednostce pełniącej rolę serwera plików jest wykonywana codzienna kopia zapasowa plików. Raz w miesiącu kopie zapasowe zgrywane są na nośnik optyczny, po czym trafiają do szafy pancernej,
   d) jednostki komputerowe są wyposażone są w system antywirusowy.

   3) Budynek Wydział ds. Obywatelskich – ul. Lipowa 52, Wołczkowo:
   a) jednostki komputerowe podłączone są pod zasilacze UPS,
   b) jednostki komputerowe są wyposażone są w system antywirusowy.

c) pracownicy mający dostęp do baz danych raz dziennie wykonują kopię zapasową na pamięć pendrive. Raz w miesiącu kopie zapasowe zgrywane są na nośnik optyczny, po czym trafiają do szafy pancernej.
d) jednostki komputerowe są wyposażone w system antywirusowy.

4) Budynek Straży Gminnej – ul. Daniela 32, Dołuje:
a) jednostki komputerowe podłączone są pod zasilacze UPS,
b) pracownicy mający dostęp do baz danych raz dziennie wykonują kopię zapasową na pamięc pendrive. Raz w miesiącu kopie zgrywane są na nośnik optyczny, po czym trafiają do szafy pancernej,
c) jednostki są wyposażone w system antywirusowy.

5) Pomieszczenie Gminnego Centrum Informacji – ul. Żubrza 7, Dołuje:
a) jednostki komputerowe podłączone są pod zasilacze UPS,
b) pracownik mający dostęp do baz danych raz dziennie wykonują kopię zapasową na pamięc pendrive. Raz w miesiącu kopie zgrywane są na nośnik optyczny, po czym trafiają do szafy pancernej,
c) jednostki są wyposażone w system antywirusowy.

9. W celu zabezpieczenia przed nieautoryzowanym dostępem do baz danych i programów zastosowano:
a) w systemie informatycznym zastosowano potrójną autoryzację użytkownika: hasło BIOS, hasło do systemu oraz hasło do programu,
b) dostęp do wypranej bazy danych uzyskuje się dopiero po poprawnym podaniu 3 haseł dostępu.
c) podłączenie danego użytkownika do sieci komputerowej dokonuje Administrator Bezpieczeństwa Informacji,
d) aby uzyskać dostęp do zasobów sieci, należy zwrócić się do Administratora Bezpieczeństwa Informacji z odpowiednim wnioskiem, w którym podane będą dane nowego użytkownika oraz zasoby jakie ma on mieć udostępnione.

10. W celu zabezpieczenia przed nieautoryzowanym dostępem do sieci poprzez Internet zastosowano:
a) zastosowano firewale programowe oraz oprogramowanie antywirusowe monitorujące próby włamania oraz skanujące pocztę elektroniczną,
b) zastosowano blokowanie i filtrowanie niektórych usług,
c) dane ściągane z Internetu są monitorowane przez system antywirusowy.
d) elementy sieci bezprzewodowej są zabezpieczone kluczami WPA i WPA2. Dodatkowo urządzenia filtrują karty MAC.

Rozdział 3

KONTROLA PRZESTRZEGANIA ZASAD ZABEZPIECZENIA DANYCH OSOBOWYCH

1. Administrator danych lub osoba przez niego wyznaczona, którą jest „Administrator Bezpieczeństwa Informacji" sprawuje nadzór nad przestrzeganiem zasad ochrony danych osobowych wynikających z ustawy o ochronie danych osobowych oraz zasad ustanowionych w niniejszym dokumencie.

2. Administrator Bezpieczeństwa sporządza półroczne plany kontroli zatwierdzone przez Wójta i zgodnie z nimi przeprowadza kontrole oraz dokonuje kwartalnych ocen stanu bezpieczeństwa danych osobowych.

3. Na podstawie zgromadzonych materiałów, o których mowa w ust. 2, Administrator Bezpieczeństwa sporządza roczne sprawozdanie i przedstawia Administratorowi danych (Wójtowi).

Rozdział 4

POSTĘPOWANIE W PRZYPADKU NARUSZENIA OCHRONY DANYCH OSOBOWYCH

1. W przypadku stwierdzenia naruszenia:

   1) zabezpieczenia systemu informatycznego,
   2) technicznego stanu urządzeń,
   3) zawartości zbioru danych osobowych,
   4) ujawnienia metody pracy lub sposobu działania programu,
   5) jakości transmisji danych w sieci telekomunikacyjnej mogącej wskazywać na naruszenie zabezpieczeń tych danych,
   6) innych zdarzeń mogących mieć wpływ na naruszenie danych osobowych (np. zalanie, pożar, itp.)

   <u>każda osoba zatrudniona przy przetwarzaniu danych osobowych jest obowiązana niezwłocznie powiadomić o tym fakcie Administratora Bezpieczeństwa.</u>

2. W razie niemożliwości zawiadomienia Administratora Bezpieczeństwa lub osoby przez niego upoważnionej, należy powiadomić bezpośredniego przełożonego.

3. Do czasu przybycia na miejsce naruszenia ochrony danych osobowych Administratora Bezpieczeństwa lub upoważnionej przez niego osoby, należy:

   1) niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego naruszenia, o ile istnieje taka możliwość, a następnie uwzględnić w działaniu również ustalenie przyczyn lub sprawców,

2) rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia,
3) zaniechać - o ile to możliwe - dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić udokumentowanie i analizę,
4) podjąć inne działania przewidziane i określone w instrukcjach technicznych i technologicznych stosownie do objawów i komunikatów towarzyszących naruszeniu,
5) podjąć stosowne działania, jeśli zaistniały przypadek jest określony w dokumentacji systemu operacyjnego, dokumentacji bazy danych lub aplikacji użytkowej,
6) zastosować się do innych instrukcji i regulaminów, jeżeli odnoszą się one do zaistniałego przypadku,
7) udokumentować wstępnie zaistniałe naruszenie,
8) nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia Administratora Bezpieczeństwa lub osoby upoważnionej.

4. Po przybyciu na miejsce naruszenia lub ujawnienia ochrony danych osobowych, Administrator Bezpieczeństwa lub osoba go zastępująca:

1) zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metody dalszego postępowania mając na uwadze ewentualne zagrożenia dla prawidłowości pracy Urzędu,
2) może żądać dokładnej relacji z zaistniałego naruszenia od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem,
3) rozważa celowość i potrzebę powiadamia o zaistniałym naruszeniu Administratora danych ,
4) nawiązuje bezpośredni kontakt, jeżeli zachodzi taka potrzeba, ze specjalistami spoza Urzędu.

5. Administrator Bezpieczeństwa dokumentuje zaistniały przypadek naruszenia oraz sporządza raport wg wzoru stanowiącego załącznik nr 2, który powinien zawierać w szczególności:

1) wskazanie osoby powiadamiającej o naruszeniu oraz innych osób zaangażowanych lub odpytanych w związku z naruszeniem,
2) określenie czasu i miejsca naruszenia i powiadomienia,
3) określenie okoliczności towarzyszących i rodzaju naruszenia,
4) wyszczególnienie wziętych faktycznie pod uwagę przesłanek do wyboru metody postępowania i opis podjętego działania,
5) wstępną ocenę przyczyn wystąpienia naruszenia,
6) ocenę przeprowadzonego postępowania wyjaśniającego i naprawczego.

6. Raport, o którym mowa w ust. 5, Administrator Bezpieczeństwa niezwłocznie przekazuje Administratorowi Danych (Wójtowi), a w przypadku jego nieobecności osobie uprawnionej.

7. Po wyczerpaniu niezbędnych środków doraźnych po zaistniałym naruszeniu Administrator Bezpieczeństwa zasięga niezbędnych opinii i proponuje postępowanie naprawcze, a w tym ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń oraz terminu wznowienia przetwarzania danych.

8. Zaistniałe naruszenie może stać się przedmiotem szczegółowej, zespołowej analizy prowadzonej przez Kierownictwo urzędu, Administratora Bezpieczeństwa Informacji, Pełnomocnika ds. Ochrony Informacji Niejawnych.

9. Analiza, o której mowa w ust. 8, powinna zawierać wszechstronną ocenę zaistniałego naruszenia, wskazanie odpowiedzialnych, wnioski co do ewentualnych przedsięwzięć proceduralnych, organizacyjnych, kadrowych i technicznych, które powinny zapobiec podobnym naruszeniom w przyszłości.

Rozdział 5

MONITOROWANIE ZABEZPIECZEŃ

1. Prawo do monitorowania systemu zabezpieczeń posiadają, zgodnie z zakresem czynności:
   1) Administrator Danych,
   2) Administrator Bezpieczeństwa Informacji.

2. W ramach kontroli należy zwracać szczególna uwagę na:

   1) okresowe sprawdzanie kopii bezpieczeństwa pod względem przydatności do możliwości odtwarzania danych,
   2) kontrola ewidencji nośników magnetycznych,
   3) kontrola właściwej częstotliwości zmiany haseł.

Rozdział 6

SZKOLENIA

1. Wszyscy pracownicy Urzędu mają obowiązek brać udział w szkoleniach.
2. Szkolenie powinno dotyczyć:
   1) obowiązujących przepisów i instrukcji wewnętrznych dotyczących ochrony danych osobowych, sposobu niszczenia wydruków i zapisów na nośnikach magnetycznych i optycznych,
   2) przedstawienie zasad ochrony danych osobowych dotyczących bezpośrednio wykonywanych obowiązków na stanowisku pracy.

Rozdział 7

NISZCZENIE WYDRUKÓW I ZAPISÓW NA NOŚNIKACH MAGNETYCZNYCH

1. Nośniki magnetyczne przekazywane na zewnątrz powinny być pozbawione zapisów zawierających dane osobowe.
2. Niszczenie poprzednich zapisów powinno odbywać się poprzez wymazywanie informacji oraz formatowanie nośnika.
3. Poprawność przygotowania nośnika magnetycznego powinna być sprawdzona przez Administratora Bezpieczeństwa Informacji.
4. Uszkodzone nośniki magnetyczne przed ich wyrzuceniem należy fizycznie zniszczyć poprzez przecięcie, przełamanie itp.
5. Wydruki po wykorzystaniu należy zniszczyć w mechanicznej niszczarce do papieru.

Rozdział 8

ARCHIWIZACJA DANYCH

1. Dane systemów kopiowane są w systemie tygodniowym.
2. Kopie awaryjne danych zapisywanych w programach wykonywane są codziennie.
3. Odpowiedzialnym za wykonywanie kopii danych i kopii awaryjnych jest pracownik merytoryczny.
4. Na koniec danego miesiąca wykonywane są kopie bezpieczeństwa z całego programu przetwarzającego dane. Nośniki z kopiami bezpieczeństwa przechowywane są w szafie pancernej.
5. Kopie awaryjne przechowywane są w (szafie metalowej) - w Wydziałach Urzędu Gminy Dobra.
6. Pen drive, na których zapisywane są kopie bezpieczeństwa są każdorazowo wymazywane i formatowane, w taki sposób, by nie można było odtworzyć ich zawartości.
7. Płyty CD, DVD na których przechowuje się kopie awaryjne niszczy się w sposób mechaniczny, tak by nie można było użyć ich ponownie,
8. Administrator Bezpieczeństwa Informacji odpowiedzialny jest za dokonywanie wymiany kopii awaryjnych na aktualne.
9. Administrator Bezpieczeństwa Informacji dokonuje okresowej weryfikacji kopii bezpieczeństwa pod kątem ich przydatności.

Rozdział 9

POSTANOWIENIA KOŃCOWE

1. Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, wszczyna się postępowanie dyscyplinarne.

2. Administrator Bezpieczeństwa zobowiązany jest prowadzić ewidencję osób, które zostały zapoznane z niniejszym dokumentem i zobowiązują się do stosowania zasad w nim zawartych wg wzoru stanowiącego **załącznik nr 8** do niniejszego dokumentu.

3. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu mogą być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, w szczególności przez osobę, która wobec naruszenia zabezpieczenia systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie powiadomiła o tym Administratora Bezpieczeństwa.

4. Orzeczona kara dyscyplinarna, wobec osoby uchylającej się od powiadomienia administratora bezpieczeństwa informacji nie wyklucza odpowiedzialności karnej tej osoby zgodnie z ustawą z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (tekst jednolity Dz. U. z 2002 r. Nr 101, poz. 926 z późniejszymi zmianami) oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.

5. W sprawach nie uregulowanych niniejszym dokumentem mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (tekst jednolity Dz. U. z 2002 r. Nr 101, poz. 926 – z późniejszymi zmianami), 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. Nr 100, poz. 1024) oraz rozporządzenie Ministra Sprawiedliwości z dnia 28 kwietnia 2004 r. w sprawie sposobu technicznego przygotowania systemów i sieci do przekazywania informacji – do gromadzenia wykazów połączeń telefonicznych i innych przekazów informacji oraz sposobów zabezpieczenia danych informatycznych (Dz. U. Nr 100, poz. 1023).

6. Niniejsza „Polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Dobra wchodzi w życie z dniem jej podpisania przez Wójta.

Załącznik nr 1

Wykaz budynków i pomieszczeń w których przetwarzane są dane osobowe oraz opis systemów informatycznych - budynek główny, ul. Szczecińska 16 a, Dobra

<table>
<tr><td>PARTER</td><td>POKÓJ NR 1 - KASA</td></tr>
<tr><td colspan="2">1. Program: ,,Kasa”
2. Rejestry, dokumenty w wersji papierowej: raporty kasowe</td></tr>
<tr><td>Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji</td><td>Stanowisko: Inspektor</td></tr>
<tr><td>PARTER</td><td>POKÓJ NR 2</td></tr>
<tr><td colspan="2">1. Program: ,,Ewidencja gruntów”, ,, Finansowo- księgowy”
2. Rejestr w formie papierowej: rejestr postępowań egzekucyjnych</td></tr>
<tr><td>Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji</td><td>Stanowisko:
- ds. windykacji należności budżetowych</td></tr>
<tr><td>PARTER</td><td>POKÓJ NR 4</td></tr>
<tr><td colspan="2">1. Programy: ,, Finansowo księgowy”, ,, Kadry i płace”
2. Rejestry, dokumenty w formie papierowej:
- rejestr zaświadczeń- zarobki,
- rejestr faktur,
- dokumentacja PKZP,
- rejestr opłat za wieczyste użytkowanie,
- rejestr postępowań egzekucyjnych,</td></tr>
<tr><td>Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji</td><td>Stanowisko: ds. płac</td></tr>
<tr><td>PARTER</td><td>POKÓJ NR 5</td></tr>
<tr><td colspan="2">1. Programy: ,, Podatki” , Ewidencja gruntów”</td></tr>
<tr><td>Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji</td><td>Stanowiska: wieloosobowe stanowisko ds. wymiaru podatków i opłat
Stanowisko ds. księgowości budżetowej</td></tr>
</table>

PARTER	**POKÓJ NR 7**
1. Programy: ,,Pojazdy” 2. Rejestry, dokumenty w wersji papierowej: - rejestr postępowań egzekucyjnych - rejestr wydawanych decyzji dotyczących zwrotu podatku akcyzowego zawartego w cenie oleju napędowego wykorzystywanego do produkcji rolnej	
Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji	Stanowisko - ds. księgowości budżetowej - ds. egzekucji podatków (tylko program ,,Podatki”)
PIĘTRO	**POKÓJ NR 8**
1. Rejestry, dokumenty w wersji papierowej: - dziennik korespondencji wpływającej do urzędu, - rejestr wysłanej korespondencji.	
Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji	Stanowisko: ds. kancelaryjnych
PIĘTRO	**POKÓJ NR 10**
1. Programy: ,,Ewidencja gruntów” 2. Rejestry, dokumenty w wersji papierowej: - rejestr decyzji o warunkach zabudowy i zagospodarowania przestrzennego, - rejestr decyzji o ustaleniu celu publicznego, - rejestr wniosków.	
Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji	Stanowiska: ds. warunków zabudowy
PIĘTRO	**POKÓJ NR 11**
1. Programy: ,, Kadry i płace”, ,,Płatnik” 2. Rejestry, dokumenty w wersji papierowej: - dokumentacja związana z zatrudnieniem osób, naborem, - rejestr kandydatów na ławników, - rejestr oświadczeń majątkowych radnych, - rejestr oświadczeń majątkowych pracowników, - rejestr wydawanych upoważnieni i pełnomocnictw, - rejestr skarg na wójta i na kierowników gminnych jednostek organizacyjnych.	
Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji	Stanowiska: - ds. kadr (dokumentacja związana z zatrudnieniem osób, naborem, rejestr oświadczeń majątkowych pracowników, rejestr wydaw. upoważnień i peł.) - ds. obsługi Rady Gminy (rejestr kandydatów na ławników, rejestr oświadczeń majątkowych radnych, rejestr skarg na wójta i na kierowników gminnych jednostek organizacyjnych)

PIĘTRO	**POKÓJ NR 12**
1. Programy: ,, Finansowo-księgowy", ,,BESTIA"	
Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji	Stanowisko: Skarbnik Gminy
PIĘTRO	**POKÓJ NR 13**
1. Rejestry, dokumenty w wersji papierowej: - rejestr skarg na pracowników	
Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji	Stanowisko: Sekretarz Gminy
PIĘTRO	**POKÓJ NR 14**
1. Programy: ,, Finansowo-księgowy", ,,Środki trwałe", 2. Rejestry elektroniczne - rejestr kontrahentów. 3. Rejestry, dokumenty w wersji papierowej - rejestr kontrahentów.	
Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji	Stanowiska: - ds. księgowości budżetowej - ds. ewidencji środków trwałych, przedmiotów nietrwałych
PIĘTRO	**POKÓJ NR 15**
1. Programy: ,, Finansowo-księgowy", ,, BESTIA", 2. Rejestry elektroniczne - rejestr kontrahentów. 3. Rejestry, dokumenty w wersji papierowej - rejestr kontrahentów.	
Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji	Stanowiska ds. księgowości budżetowej

Załącznik nr 2

Budynek Wydziału ds. Komunalnych i Inwestycji, ul. Szczecińska 24A, Dobra

<table>
<tr><td colspan="2">SEKRETARIAT</td></tr>
<tr><td colspan="2">1. Rejestry elektroniczne:
- dziennik korespondencji wpływającej do urzędu,
- rejestr wysłanej korespondencji.
2. Rejestry, dokumenty w wersji papierowej:
- dziennik korespondencji wpływającej do urzędu</td></tr>
<tr><td>Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji</td><td>Stanowisko: ds. kancelaryjnych</td></tr>
<tr><td colspan="2">POKÓJ NR 3</td></tr>
<tr><td colspan="2">Rejestry, dokumenty w wersji papierowej:
- rejestr referencji,</td></tr>
<tr><td>Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji</td><td>Stanowisko: ds. melioracji</td></tr>
<tr><td colspan="2">POKÓJ NR 3</td></tr>
<tr><td colspan="2">Rejestry elektroniczne:
- rejestr wydanych dzienników budów gminy,
- rejestr umów na nadzory inwestorskie.</td></tr>
<tr><td>Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji</td><td>Stanowisko: ds. inwestycji</td></tr>
<tr><td colspan="2">POKÓJ NR 3</td></tr>
<tr><td colspan="2">1. Program: „ Ewidencja gruntów”
2. Rejestry elektroniczne:
- rejestr decyzji o warunkach zabudowy,
- rejestr wniosków.
3. Rejestry, dokumenty w wersji papierowej;
- rejestr decyzji o warunkach zabudowy,
- rejestr wniosków.</td></tr>
<tr><td>Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji</td><td>Stanowiska ds. warunków zabudowy dla budownictwa jednorodzinnego</td></tr>
</table>

POKÓJ NR 4	
1. Program: ,, Ewidencja gruntów” 2. Rejestry elektroniczne: - rejestr własności Gminy Dobra, 3. Rejestry, dokumenty w wersji papierowej: - rejestr własności Gminy Dobra, - rejestr umów dzierżawy, - rejestr umów reklam, - rejestr nabycia i zbycia nieruchomości, - rejestr umów lokali mieszkalnych i użytkowych, - rejestr osób oczekujących na lokale komunalne, - opłata adiacencka.	
Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji	Stanowiska ds. gospodarki gruntami
POKÓJ NR 5	
1. Program: ,, Ewidencja gruntów” (GEO-INFO V i Net), ,, GEO- SECMA”(infrastruktura komunalna) 2. Rejestry elektroniczne: - rejestr umów wodno-kanalizacyjnych i deszczowych	
Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji	Stanowiska ds. warunków technicznych woda-kanalizacja
POKÓJ NR 6	
1. Rejestry elektroniczne: - rejestr numeracji porządkowej, - rejestr zaświadczeń z planu i wypisów i wyrysów. 2. Rejestry, dokumenty w wersji papierowej: - rejestr wniosków do zmian w planie zagospodarowania przestrzennego.	
Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji	Stanowisko ds. planowania i zagospodarowania przestrzennego
POKÓJ NR 7	
1. Rejestry elektroniczne: - rejestr decyzji na zajęcie pasa drogowego	
Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji	Stanowisko ds. komunalnych (drogi)

POKÓJ NR 8	
1. Rejestry elektroniczne: - rejestr zamówień publicznych. 2. Rejestry, dokumenty w wersji papierowej: - rejestr zamówień publicznych, - rejestr umów. - rejestr decyzji na wbudowanie urządzenia w drogę.	
Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji	Stanowiska: - ds. zamówień publicznych. - ds. komunalnych (drogi)

Załącznik nr 3

Wykaz budynków i pomieszczeń w których przetwarzane są dane osobowe oraz opis systemów informatycznych - budynek Wydział ds. Obywatelskich, ul. Lipowa 52, Wołczkowo

<table>
<tr><td colspan="2">POKÓJ NR 1</td></tr>
<tr><td colspan="2">1. Programy: ,, Ewidencja ludności ’’, ,,SWDO”
2. Rejestry elektroniczne: - rejestr wyborców,
3. Rejestry, dokumenty w wersji papierowej:
- rejestr cudzoziemców zameldowanych czasowo do 3 miesięcy
- lista przedpoborowych i poborowych</td></tr>
<tr><td>Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji</td><td>Stanowiska ds. meldunków
Stanowisko ds. dowodów osobistych</td></tr>
<tr><td colspan="2">POKÓJ NR 2/1</td></tr>
<tr><td colspan="2">1. Program: ,,Ewidencja gruntów”
2. Rejestry, dokumenty w wersji papierowej:
- rejestr zezwoleń na posiadanie psów ras uznanych za agresywne,
- rejestr zezwoleń na wycinkę drzew,
- ewidencja zmarłych pochowanych na cmentarzach,
- ewidencja zabytków,
- ewidencja zezwoleń na uprawę maku.</td></tr>
<tr><td>Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji</td><td>Stanowisko - ds. ochrony środowiska</td></tr>
<tr><td colspan="2">POKÓJ NR 2/2</td></tr>
<tr><td colspan="2">1. Program: Ewidencja Działalności Gospodarczej
2. Rejestry elektroniczne:
- ewidencja działalności gospodarczej
3. Rejestry, dokumenty w wersji papierowej
- rejestr wydanych licencji na taksówki osobowe,
- rejestr wydanych zezwoleń na sprzedaż napojów alkoholowych,
- rejestr innego obiektu świadczącego usługi hotelarskie,
- rejestr zezwoleń na organizację imprez masowych.</td></tr>
<tr><td>Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji</td><td>Stanowisko ds. działalności gospodarczej</td></tr>
</table>

POKÓJ NR 2/3	
1. Program: ,,GOMiG" Gospodarka odpadami 2. Rejestry elektroniczne: - rejestr umów na wywóz odpadów komunalnych i opróżniania zbiorników bezodpływowych, - rejestr przedsiębiorców uzyskujących decyzje na transport i odbieranie odpadów komunalnych i opróżniania zbiorników bezodpływowych, 4. Rejestry, dokumenty w wersji papierowej: - rejestr decyzji o środowiskowych uwarunkowaniach	
Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji	Stanowiska ds. ochrony środowiska

ZESPÓŁ ds. POZYSKIWANIA FUNDUSZY UNIJNYCH

POKÓJ NR 4	
1. Program: ,,PEFS" 2. Rejestry, dokumenty w wersji papierowej: - rejestr beneficjentów	
Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji	Stanowiska ds. pozyskiwania funduszy unijnych

Pełnomocnik ds. Ochrony Informacji Niejawnych, któremu powierzono obowiązki Głównego specjalisty ds. Obronnych i Zarządzania Kryzysowego Pełnomocnik

1. Rejestry, dokumenty w wersji papierowej: - Akcja kurierska - Obrona cywilna - Gminny Zespół Zarządzania Kryzysowego, - Decyzje o nałożeniu zobowiązań do świadczeń rzeczowych i osobistych.	
Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji	Stanowisko: Pełnomocnik ds. Ochrony Informacji Niejawnych, któremu powierzono obowiązki Głównego specjalisty ds. Obronnych i Zarządzania Kryzysowego Pełnomocnik

Załącznik nr 4

Wykaz budynków i pomieszczeń w których przetwarzane są dane osobowe oraz opis systemów informatycznych - budynek Straży Gminnej, ul. Daniela 32, Dołuje

<table>
<tr><td colspan="2">SEKRETARIAT</td></tr>
<tr><td colspan="2">Rejestry, dokumenty w wersji papierowej:
- rejestr interwencji,
- rejestr założonych blokad,
- dziennik korespondencji,
- rejestr nałożonych mandatów karnych,
- rejestr kart MRD-5,
- rejestr postępowań egzekucyjnych.</td></tr>
<tr><td>Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji</td><td>Stanowisko – pomoc administracyjna</td></tr>
<tr><td colspan="2">POMIESZCZENIE STRAŻNIKÓW</td></tr>
<tr><td colspan="2">1. Program- Emandat.
2. Rejestry, dokumenty w wersji papierowej:
- rejestr spraw o wykroczenia,
- notatniki służbowe,
- kopie wniosków o ukaranie kierowanych do sądu.</td></tr>
<tr><td>Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji</td><td>Stanowiska:
- Komendant
- Pomoc administracyjna
- Strażnicy Gminni
Pozostałe osoby nie maja dostępu do RSoW i kopii wniosków o ukaranie kierowanych do sądu:
- Strażnicy Gminni</td></tr>
<tr><td colspan="2">POMIESZCZENIE KOMENDANTA</td></tr>
<tr><td colspan="2">1. Rejestry, dokumenty w wersji papierowej:
- grzbiety wykorzystanych bloczków mandatów karnych.</td></tr>
<tr><td>Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji</td><td>Stanowisko – Komendant SG</td></tr>
</table>

Załącznik nr 5

Wykaz budynków i pomieszczeń w których przetwarzane są dane osobowe oraz opis systemów informatycznych Pomieszczenie Gminnego Centrum Informacji, ul. Żubrza 7, Dołuje

POMIESZCZENIE GCI	
Zbiór danych przetwarzanych w związku z działalnością GKRPA	
Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji	Stanowisko – samodzielny referent

Załącznik nr 6

Opis struktur zbiorów danych

1. Raporty kasowe

• imiona i nazwiska,
• adres zamieszkania.
• kod pocztowy,

2. Rejestr postępowań egzekucyjnych

• imiona i nazwiska,
• imię ojca i matki
• adres zamieszkania.
• kod pocztowy,
• pesel
• data urodzenia
• rodzaj i kwota należności

3. Rejestr zaświadczeń - zarobki

• imiona i nazwiska,
• imię ojca i matki
• adres zamieszkania.
• kod pocztowy,
• pesel
• data urodzenia
• wysokość zarobków

4. Rejestr faktur

• imiona i nazwiska,
• adres zamieszkania.
• kod pocztowy,
• NIP

5. Rejestr opłat za wieczyste użytkowanie gruntów

• imiona i nazwiska,
• imię ojca i matki
• adres zamieszkania.
• kod pocztowy,
• pesel
• data urodzenia
• nr dowodu osobistego
• nr konta bankowego
• nr działki
• NIP

6. Podatki

• imiona i nazwiska,
• imię ojca i matki
• adres zamieszkania.
• rodzaj zameldowania,
• kod pocztowy,
• pesel
• NIP
• data urodzenia
• nr telefonu
• nr działki

7. Pojazdy

• imiona i nazwiska,
• imię ojca i matki
• adres zamieszkania.
• NIP
• kod pocztowy,
• Pesel
• data urodzenia
• nr telefonu
• REGON

8. Rejestr decyzji dotyczących zwrotu podatku akcyzowego zawartego w cenie oleju napędowego wykorzystywanego do produkcji rolnej

• imiona i nazwiska,
• imię ojca i matki
• adres zamieszkania.
• kod pocztowy,
• NIP
• pesel
• Nr dowodu osobistego
• nr działki
• posiadane nieruchomości
• nr konta bankowego

9. Dziennik korespondencji wpływającej do urzędu

• imiona i nazwiska,
• adres zamieszkania.
• kod pocztowy,

10. Rejestr wysyłanej korespondencji

• imiona i nazwiska,
• adres zamieszkania.
• kod pocztowy,

11. Rejestr decyzji o warunków zabudowy i zagospodarowania terenu.

• imiona i nazwiska,
• adres zamieszkania.
• kod pocztowy,
• nr działki

12. Rejestr decyzji o ustaleniu celu publicznego.

• imiona i nazwiska,
• adres zamieszkania.
• kod pocztowy,
• nr działki

13. Rejestr wniosków.

• imiona i nazwiska
• adres zamieszkania
• kod pocztowy
• nr działki

14. Kadry i płace

• imiona i nazwiska
• imię ojca i matki
• nazwisko panieńskie w przypadku mężatek
• Pesel
• NIP
• nr dowodu osobistego
• adres zamieszkania
• kod pocztowy
• nr konta
• nr telefonu

15. Płatnik

• imiona i nazwiska
• imię ojca i matki
• nazwisko panieńskie w przypadku mężatek
• Pesel
• NIP
• nr dowodu osobistego
• adres zamieszkania
• kod pocztowy

16. Rejestr kandydatów na ławników.

• imiona i nazwiska,
• imię ojca i matki
• data urodzenia
• adres zamieszkania.
• kod pocztowy,

• zaświadczenie o niekaralności
• oświadczenie o niepozbawieniu władzy rodzicielskiej
• oświadczenie – brak postępowań ściganych z oskarżenia publicznego lub przestępstw skarbowych
• zaświadczenie o stanie zdrowia
• zdjęcia

17. Rejestr oświadczeń majątkowych radnych

• imiona i nazwiska,
• imię ojca i matki
• adres zamieszkania.
• rodzaj zameldowania,
• kod pocztowy,
• oświadczenie o niekaralności
• data urodzenia
• informacja o zobowiązaniach pieniężnych
• adresy posiadanych nieruchomości wraz z wartością
• składniki mienia ruchomego powyżej 10 000 zł

18. Rejestr oświadczeń majątkowych pracowników

• imiona i nazwiska,
• imię ojca i matki
• adres zamieszkania.
• kod pocztowy,
• oświadczenie o niekaralności
• data urodzenia
• informacja o zobowiązaniach pieniężnych
• adresy posiadanych nieruchomości wraz z wartością
• składniki mienia ruchomego powyżej 10 000 zł

19. Rejestr skarg i wniosków

• imiona i nazwiska,
• adres zamieszkania.
• kod pocztowy,

20. Program finansowo-księgowy

• imiona i nazwiska
• adres zamieszkania

21. Rejestr kontrahentów

• imiona i nazwiska
• nazwa firmy
• adres zamieszkania
• kod pocztowy

22. Rejestr referencji

• imiona i nazwiska,
• adres zamieszkania.
• kod pocztowy,
• nazwa i siedziba firmy

23. Rejestr umów dzierżawy

• imiona i nazwiska,
• adres zamieszkania.
• kod pocztowy,
• pesel
• NIP
• nr działki

24. Rejestr umów reklam

• imiona i nazwiska,
• adres zamieszkania.
• kod pocztowy,
• pesel
• NIP
• nazwa i adres firmy

25. Rejestr umów nabycia i zbycia nieruchomości

• imiona i nazwiska,
• imię ojca i matki
• adres zamieszkania.
• kod pocztowy,
• pesel
• NIP

26. Rejestr umów lokali mieszkalnych i użytkowych

• imiona i nazwiska,
• imię ojca i matki
• adres zamieszkania.
• kod pocztowy,
• pesel

27. Rejestr osób oczekujących na lokale komunalne

• imiona i nazwiska,
• adres zamieszkania.
• kod pocztowy,
• pesel
• data urodzenia

28. Rejestr opłat adiacenckich

• imiona i nazwiska,
• adres zamieszkania.
• kod pocztowy,
• nr działki

29. Rejestr umów wodno kanalizacyjnych i deszczowych

• imiona i nazwiska,
• adres zamieszkania.
• kod pocztowy,
• nazwa i siedziba firmy
• nr działki

30. Rejestr nadawanych numerów porządkowych.

• imiona i nazwiska,
• adres zamieszkania.
• kod pocztowy,
• nr działki

31. Rejestr zaświadczeń z planu i wypisów i wyrysów.

• imiona i nazwiska,
• adres zamieszkania.
• kod pocztowy,
• nr działki

32. Rejestr wniosków do zmian w planie zagospodarowania przestrzennego.

• imiona i nazwiska,
• adres zamieszkania.
• kod pocztowy,
• nazwa i adres firmy
• nr działki

33. Rejestr decyzji na zajęcie pasa drogowego.

• imiona i nazwiska,
• adres zamieszkania.
• kod pocztowy,
• nazwa i siedziba firmy
• nr działki

34. Rejestr zamówień publicznych

• imiona i nazwiska,
• adres zamieszkania.
• kod pocztowy,
• nazwa i adres firmy
• NIP

35. Rejestr decyzji na wbudowanie urządzenia w drogę.

• imiona i nazwiska,
• adres zamieszkania.
• kod pocztowy,
• nazwa i siedziba firmy
• nr działki

36. Ewidencja ludności i dowody osobiste

Dane osobowe
- nazwiska i imiona
- nazwisko rodowe i z poprzedniego małżeństwa,
- imiona rodziców,
- data urodzenia,
- miejsce urodzenia,
- akta urodzenia, data i nr USC
Dane osobowe archiwalne
- nazwiska i imiona,
- nazwisko rodowe i z poprzedniego małżeństwa.
Adres zamieszkania lub pobytu stałego oraz data zameldowania
Archiwalne adresy zamieszkania lub pobytu stałego oraz data zameldowania
Adres czasowy oraz czas pobytu czasowego
Archiwalne adresy czasowe oraz okresy pobytów czasowych
Dokument tożsamości
- rodzaj dokumentu,
- seria i numer dowodu,
- wystawca dokumentu,
- rysopis :wzrost, kolor oczu, znaki szczególne;
Numer ewidencyjny PESEL
USC i nr aktu urodzenia
Stan cywilny:
- imię i nazwisko współmałżonka,
- nazwisko rodowe i nazwisko z poprzedniego małżeństwa,
- data zawarcia małżeństwa,
- USC i numer aktu małżeństwa,
- data wydania i wydający dokument tożsamości,
Stan cywilny archiwalny
- imię i nazwisko małżonka,
- nazwisko rodowe i nazwisko z poprzedniego małżeństwa,
- data zawarcia małżeństwa,
- USC i numer aktu małżeństwa,
Data wydania i wydający dokument tożsamości
Archiwalne dokumenty tożsamości
Obowiązek wojskowy
- czy podlega obowiązkowi,
- nazwa i nr wojskowego dokumentu tożsamości,
- stopień wojskowy,
Data zgonu, USC i numer aktu zgonu
Imiona i nazwiska rodowe

Obywatelstwo (data zmiany , podstawa prawna)
Adnotacje o rozwodzie

37. Rejestr wyborców

• imiona i nazwiska,
• adres zamieszkania.
• imię ojca
• PESEL
• data urodzenia
• adres stałego zamieszkania
• adres zameldowania na pobyt stały

38. Rejestr cudzoziemców zameldowanych czasowo do 3 miesięcy

• imiona i nazwisko
• imiona rodziców
• data urodzenia
• kraj przybycia
• adres czasowego miejsca pobytu

39. Lista przedpoborowych i poborowych

• imiona i nazwiska,
• imię ojca
• PESEL
• nr dowodu osobistego
• adres stałego zameldowania

40. Rejestr zezwoleń na posiadanie psów ras uznawanych za agresywne.

• imiona i nazwiska,
• adres zamieszkania.
• kod pocztowy,
• rasa psa

41. Rejestr zezwoleń na wycinkę drzew.

• imiona i nazwiska,
• adres zamieszkania.
• rodzaj zameldowania,
• kod pocztowy,
• nr działki

42. Ewidencja zmarłych pochowanych na cmentarzu

• imiona i nazwiska,
• ostatnie miejsce zamieszkania
• data i miejsce urodzenia
• data i miejsce zgonu

43. Ewidencja ewidencji zabytków.

• imiona i nazwiska,
• adres zamieszkania.
• kod pocztowy,
• nr działki

44. Ewidencja działalności gospodarczej

• imiona i nazwiska
• adres zamieszkania
• PESEL
• NIP
• REGON
• imię ojca, imię matki
• nr dowodu osobistego
• miejsce i data urodzenia
• obywatelstwo
• nazwisko rodowe

45. Rejestr zezwoleń na uprawę maku.

• imiona i nazwiska,
• adres zamieszkania.
• rodzaj zameldowania,
• kod pocztowy,
• nr działki

46. Rejestr wydanych licencji na taksówki osobowe.

• imiona i nazwiska
• imię ojca i matki
• adres zamieszkania
• kod pocztowy
• Pesel
• NIP
• REGON
• data i miejsce urodzenia
• nr dowodu osobistego
• nr i kategoria prawa jazdy
• nr rej pojazdu
• zaświadczenie o niekaralności

47. Rejestr wydanych zezwoleń na sprzedaż napojów alkoholowych

• imiona i nazwiska,
• adres zamieszkania
• PESEL
• NIP
• REGON

48. Rejestr innego obiektu świadczącego usługi hotelarskie

• imiona i nazwiska
• adres zamieszkania
• REGON
• NIP

49. Rejestr zezwoleń na organizację imprez masowych

• imiona i nazwiska,
• adres zamieszkania.

50. Rejestr umów na wywóz odpadów komunalnych i opróżniania zbiorników bezodpływowych

• imiona i nazwiska
• adres zamieszkania
• adres zameldowania
• kod pocztowy
• nr działki

51. Rejestr przedsiębiorców uzyskujących decyzje na transport i odbieranie odpadów komunalnych i opróżniania zbiorników bezodpływowych

• imiona i nazwiska,
• adres zamieszkania.
• rodzaj zameldowania,
• kod pocztowy,
• nr działki

52. Rejestr decyzji o środowiskowych uwarunkowaniach

• imiona i nazwiska,
• adres zamieszkania.
• kod pocztowy,
• nr działki
• nr telefonu

53. Program PEFS

• imiona i nazwiska,
• adres zamieszkania.
• data urodzenia
• miejsce urodzenia
• rodzaj zameldowania,
• kod pocztowy,
• nr telefonu
• e-mail
• status na rynku pracy
• wykształcenie

54. Rejestr beneficjentów

• imiona i nazwiska,
• adres zamieszkania.
• data urodzenia
• miejsce urodzenia
• rodzaj zameldowania,
• kod pocztowy,
• nr telefonu
• e-mail
• status na rynku pracy
• wykształcenie

55. Akcja kurierska

• imiona i nazwiska,
• adres zamieszkania.
• kod pocztowy,
• nr telefonu
• e-mail

56. Obrona cywilna

• imiona i nazwiska,
• adres zamieszkania.
• data urodzenia
• imię ojca
• kod pocztowy,
• nr telefonu

57. Gminny Zespół Zarządzania Kryzysowego

• imiona i nazwiska,
• adres zamieszkania.
• kod pocztowy,
• nr telefonu
• e-mail

58. Decyzje o nałożeniu zobowiązań do świadczeń rzeczowych i osobistych.

• imiona i nazwiska,
• adres zamieszkania.
• rodzaj świadczenia

59. Rejestr interwencji

• imiona i nazwiska,
• adres zamieszkania.
• nr telefonu
• nr rej pojazdu

• powód interwencji
• nałożony mandat karny

60. Rejestr spraw o wykroczenia

• imiona i nazwiska,
• imię ojca
• data urodzenia
• miejsce urodzenia
• adres zamieszkania.
• popełnione wykroczenie
• nałożony mandat karny
• wyrok sądu

61. Rejestr nałożonych mandatów karnych

• imiona i nazwiska,
• imię ojca
• data urodzenia
• Pesel
• adres zamieszkania.
• popełnione wykroczenie
• nałożony mandat karny
• nr dokumentu tożsamości

62. Rejestr kart rejestracyjnych Mrd-5

• imiona i nazwiska,
• imię ojca
• imię matki
• dokument tożsamości
• Pesel
• adres zamieszkania.
• popełnione wykroczenie
• nałożony mandat karny
• nr i kat praw jazdy
• skierowanie wniosku o ukaranie do sądu

63. Rejestr usuniętych pojazdów

• imiona i nazwiska,
• data urodzenia
• adres zamieszkania.
• nr dokumentu tożsamości
• nr rej pojazdu

64. Program EMandat

• imiona i nazwiska,
• imię ojca
• imię matki
• nazwisko rodowe
• nazwisko panieńskie matki
• data urodzenia
• miejsce urodzenia
• Pesel
• adres zamieszkania.
• adres do korespondencji
• popełnione wykroczenie
• nałożony mandat karny
• nr dowodu osobistego
• nr prawa jazdy
• nr rej pojazdu
• nr działki
• skierowanie wniosku o ukaranie do sądu
• wyrok sądu

65. Zbiór danych przetwarzanych w związku z działalnością gminnej komisji rozwiązywania problemów alkoholowych.

• imiona i nazwiska,
• imię ojca i matki
• adres zamieszkania.
• rodzaj zameldowania,
• kod pocztowy,
• stan zdrowia
• nałogi
• orzeczenia wydane w postępowaniu sądowym

Załącznik nr 7

W z ó r

R a p o r t
z naruszenia bezpieczeństwa systemu informatycznego
w Urzędzie Gminy Dobra

1. Data: ..... Godzina: .....
(dd.mm.rrrr) *(00:00)*

2. Osoba powiadamiająca o zaistniałym zdarzeniu:

.....
(Imię, nazwisko, stanowisko służbowe, nazwa użytkownika (jeśli występuje))

3. Lokalizacja zdarzenia:

.....
(np. nr pokoju, nazwa pomieszczenia)

4. Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące:

.....

5. Podjęte działania:

.....

6. Przyczyny wystąpienia zdarzenia:

.....

7. Postępowanie wyjaśniające:

.....

.....
data, podpis Administratora Bezpieczeństwa Informacji

Załącznik nr 8

Wykaz osób, które zostały zapoznane z „Polityką bezpieczeństwa i obsługi systemów informatycznych służących do przetwarzania danych osobowych w Urzędzie Gminy Dobra, przeznaczonej dla osób zatrudnionych przy przetwarzaniu tych danych.

Przyjąłem/am/ do wiadomości i stosowania zapisy Polityki bezpieczeństwa.

Nazwisko i Imię	Komórka organizacyjna	Data, podpis

Załącznik nr 9

……..……..……
/imię i nazwisko pracownika/

……..

……..
/adres zamieszkania/

OŚWIADCZENIE

1. Stwierdzam własnoręcznym podpisem, że znana jest mi treść przepisów :
   a) o ochronie tajemnic prawnie chronionych stanowiących tajemnicę służbową wynikającą z Kodeksu Pracy,
   b) o ochronie danych osobowych wynikająca z ustawy o ochronie danych osobowych
   c) o odpowiedzialności karnej za naruszenie ochrony danych osobowych.

2. Zobowiązuję się nie ujawniać wiadomości, z którymi zapoznałem/am się w trakcie wykonywanych czynności służbowych .

…… ……
(podpis pracownika) (podpis złożono w obecności)

Załącznik nr 10

.....
/miejscowość, data/

U P O W A Ż N I E N I E Nr .....

Na podstawie art.37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2002 r. Nr 101, poz. 926 z późniejszymi zmianami)

U p o w a ż n i a m

.....
/imię i nazwisko/

zatrudnionego na stanowisku .....

do przetwarzania danych osobowych oraz do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych osobowych

W.....
/nazwa jednostki organizacyjnej/

Upoważnienie wydaje się na czas zatrudnienia w jednostce.

…….....
Administrator Danych

Załącznik nr 11

(nazwisko i imię)	*(stanowisko)*

L.p	Data nadania upoważnienia	Data ustania upoważnienia	Zakres upoważnienia	hasło	Uwagi
1					
2					
3					
4					

Zakres upoważnienia:

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

(Administrator Bezpieczeństwa Informacji)

……
(imię i nazwisko)

…….

(miejscowość, data)