Załącznik do zarządzenia Nr 107 /2011
Wójta Gminy Kobylanka z dnia 19.10.2011r.

Polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Kobylanka

Opracował :
Jolanta Kazberuk
Administrator Bezpieczeństwa Informacji

SPIS TREŚCI:

WPROWADZENIE

Niniejszy dokument opisuje reguły dotyczące bezpieczeństwa danych osobowych zawartych w systemach informatycznych w Urzędzie Gminy Kobylanka. 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 Kobylanka", 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 Kobylanka.
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 nich 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 Kobylanka 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 ochrony fizycznej i technicznej należy:

1) przetwarzanie danych osobowych w wydzielonych pomieszczeniach położonych w strefie administracyjnej,
2) zabezpieczenie wejścia do pomieszczeń, o których mowa w pkt. 1 poprzez zastosowanie zamków patentowych,
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 Kobylanka zawierają następujące załączniki do niniejszego dokumentu:

1) **załącznik nr 1** - budynek Urzędu Gminy, ul. Szkolna 12, Kobylanka,
2) **załącznik nr 2** - budynek Gminnego Centrum Informacji, ul. Jeziorna 6, Kobylanka ,
3) **załącznik nr 3** - budynek Straż y Gminnej , ul. Szczecińska 17,Morzyczyn

7. W celu ochrony przed utratą danych w Urzędzie Gminy Kobylanka stosowane są następujące zabezpieczenia:

1) Budynek Urzędu Gminy – ul. Szkolna 12, Kobylanka:

a) obszar, w których przetwarza się dane osobowe zabezpieczony jest przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania tych danych poprzez zamykanie tych pomieszczeń na zamki nawierzchniowe patentowe ,
b) serwer i osprzęt sieciowy znajduje się w specjalnie wydzielonej szafie zamykanej na klucz, do której dostęp posiada Administrator Bezpieczeństwa Informacji, w razie nieobecności osoba przez niego upoważniona,
c) dostęp do danych osobowych mają tylko pracownicy posiadający pisemne upoważnienie wydane przez Administratora Danych Osobowych,
d) szafy, w których przechowywane są dane osobowe są zamykane na klucz. Klucze do tych szaf posiadają upoważnieni pracownicy danej komórki.
e) jednostki komputerowe podłączone są pod zasilacze UPS,
f) serwer podłączony jest pod zasilacz UPS,
g) pracownicy mający dostęp do programów i baz danych dodatkowo wykonują kopie zapasową używanych przez siebie programów na dysk przenośny lub pamięć pendrive,
h) jednostki komputerowe oraz serwer są wyposażone w system antywirusowy.

2) Budynek Gminnego Centrum Informacji ul. Jeziorna 6, Kobylanka:

a) obszar, w których przetwarza się dane osobowe zabezpieczony jest przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania tych danych poprzez zamykanie tych pomieszczeń na zamki nawierzchniowe patentowe ,
b) dostęp do danych osobowych mają tylko pracownicy posiadający pisemne upoważnienie wydane przez Administratora Danych Osobowych,
c) szafy w których przechowywane są dane osobowe są zamykane na klucz. Klucze do szafy posiadają upoważnieni pracownicy danej komórki
d) klucze do pomieszczeń posiadają tylko pracownicy upoważnieni przez Administratora Danych Osobowych, oraz przechowywane są w szafie pancernej Urzędu Gminy,
e) dodatkowo obszar, w których przetwarza się dane osobowe jest wyposażony w kraty na oknach i system alarmowy,
f) jednostki komputerowe podłączone są pod zasilacze UPS,
g) na jednostce pełniącej rolę serwera plików jest wykonywana codzienna kopia zapasowa plików.,

h) jednostki komputerowe są wyposażone są w system antywirusowy.

3) Budynek Straży Gminnej ul. Szczecińska 17, Morzyczyn:

a) obszar, w których przetwarza się dane osobowe zabezpieczony jest przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania tych danych poprzez zamykanie tych pomieszczeń na zamki nawierzchniowe patentowe ,
b) dodatkowo obszar, w których przetwarza się dane osobowe jest wyposażony w kraty na oknach,
c) dostęp do danych osobowych mają tylko pracownicy posiadający pisemne upoważnienie wydane przez Administratora Danych Osobowych,
d) szafa pancerna w której przechowywane są dane osobowe są zamykane na klucz. Klucze do szafy posiadają upoważnieni pracownicy danej komórki oraz zapasowe znajdują się w szafie pancernej w Urzędzie Gminy,
e) klucze do pomieszczeń posiadają tylko pracownicy upoważnieni przez Administratora Danych Osobowych, oraz przechowywane są w szafie pancernej Urzędu Gminy,
f) jednostki komputerowe podłączone są pod zasilacze UPS,
g) jednostki komputerowe są wyposażone są w system antywirusowy,
h) pracownicy mający dostęp do baz danych raz dziennie wykonują kopię zapasową na pamięć pendrive.

8. 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 wybranej 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.

9. 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.

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.)

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

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 5, 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. Kopią zapasową i awaryjną objęte są dane znajdujące się na serwerach sieci informatycznej.
2. Za sporządzenie i bezpieczeństwo kopii zapasowych i awaryjnych odpowiedzialny jest

Administrator Systemu Informatycznego.
3. W wyjątkowych przypadkach sporządzenie kopii zapasowych i awaryjnych można powierzyć osobie upoważnionej przez Administratora Systemu Informatycznego w porozumieniu z Administratorem Bezpieczeństwa Informacji.
4. Kopia zapasowa wykonywana jest przez kopiowanie całości danych.
5. Harmonogram sporządzania kopii zapasowych musi gwarantować dostępność w każdej chwili czterech kopii: z ostatniego dnia, z końca ubiegłego tygodnia, z końca ubiegłego miesiąca oraz z końca ubiegłego roku. Kopie dzienne i tygodniowe zapisywane są na lokalnym dysku twardym komputera znajdującego się pod stałym nadzorem Administratora Systemu Informatycznego, kopie miesięczne i roczne zapisywane są na nośnikach optycznych, które przechowuje się w szafie metalowej.
6. Kopie awaryjne tworzone są przed każdą aktualizacją systemu informatycznego, składników systemu informatycznego lub poszczególnych programów służących do przesyłania lub przetwarzania danych. Kopie awaryjne zapisywane są na lokalnym dysku twardym komputera znajdującego się pod stałym nadzorem Administratora Systemu Informatycznego.
7. Użytkownicy we własnym zakresie odpowiadają za sporządzanie kopii zapasowych i awaryjnych wytworzonych przez siebie dokumentów i danych znajdujących się na lokalnych dyskach twardych wykorzystywanych przez nich stacji roboczych, przy jednoczesnym obowiązku dopilnowania, aby dane na lokalnym dysku twardym nie zawierały danych osobowych.
8. W czasie wykonywania kopii zapasowej dostęp do kopiowanych danych dla wszystkich użytkowników jest zablokowany.
9. Po wykonaniu kopii zapasowej i awaryjnej Administrator Systemu Informatycznego ma obowiązek sprawdzić poprawność i kompletność skopiowanych danych oraz zweryfikować możliwość ich przywrócenia i wykorzystania.

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 6** 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 Kobylanka 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 Urzędu Gminy, ul. Szkolna 12 , Kobylanka

PARTER	**POKÓJ Nr 1**
1.Rejestry,dokumenty w wersji papierowej: ✓ Ewidencja zmarłych pochowanych na cmentarzach, ✓ Decyzje o nałożeniu zobowiązań do świadczeń rzeczowych i osobistych	Zarządzanie kryzysowe, obrony cywilnej, spraw obronnych, gospodarki komunalnej
	Stanowisko : dwuosobowe –podinspektorzy
PARTER	
1.Rejestr korespondencji przychodzącej 2.Rejestr korespondencji wysłanej	Punkt obsługi interesanta
PARTER	POKÓJ Nr 2
1.Rejestry ,dokumenty w wersji papierowej: ✓ rejestr psów ✓ rejestr zezwoleń na wycinkę drzew, ✓ ewidencja zabytków, ✓ rejestr przydomowych oczyszczalni ścieków,	Stanowisko ds. Ochrony środowiska i rolnictwa
PARTER	POKÓJ Nr 3
1.Rejestry elektroniczne : ✓ rejestr decyzji o warunkach zabudowy i zagospodarowania przestrzennego, ✓ rejestr decyzji o ustaleniu celu publicznego, 2.Rejestry ,dokumenty w wersji papierowej : ✓ rejestr zaświadczeń z planu i wypisów ✓ i wyrysów, ✓ rejestr wniosków do zmian w planie zagospodarowania przestrzennego	Dwa samodzielne stanowiska ds. planowania przestrzennego i warunków zabudowy

PARTER	POKÓJ Nr 4,
1.Programy : „ Kadry i płace” „Płatnik”, ”SIO”, „TALES” 2.Rejestry ,dokumenty w wersji papierowej : ✓ dokumentacja związana z zatrudnieniem osób, naborem, ✓ rejestr zaświadczeń –zarobki ✓ rejestr oświadczeń majątkowych pracowników, ✓ dokumenty związane z ubezpieczeniem pracowników	Stanowisko pracy ds. wynagrodzeń, kadr , oświaty
PARTER	POKÓJ Nr 5
1.Rejestry,dokumenty w wersji papierowej : ✓ rejestr decyzji na zajecie pasa drogowego, ✓ rejestr decyzji na wbudowanie urządzenia w drogę, ✓ rejestr zamówień publicznych ✓ rejestr umów	Samodzielne stanowiska ds. inwestycji
PIĘTRO I	POKÓJ Nr 11
1.Programy:”Ewidencja podatków”, „Pojazdy” 2.Rejestry,dokumenty w wersji papierowej : ✓ rejestr zaświadczeń ✓ rejestr wydawanych decyzji dotyczących zwrotu podatku akcyzowego zawartego w cenie oleju napędowego wykorzystywanego do produkcji rolnej	Dwa stanowiska pracy ds. wymiaru podatków i opłat
PIĘTRO I	POKÓJ Nr 12
1.Programy : „Czynsze”, „Ewidencja podatków”, „Pojazdy” 2.Rejestry,dokumenty w wersji papierowej: ✓ rejestr tytułów wykonawczych ✓ rejestr upomnień	Stanowisko pracy ds. księgowości podatkowej, windykacji
PIĘTRO I	POKÓJ Nr 13
1.Programy :Finansowo –Księgowy FK, Bestia	Z-ca Skarbnika
PIĘTRO I	POKÓJ 15 -sekretariat
1.Rejestry,dokumenty w wersji papierowej: ✓ rejestr pełnomocnictw, upoważnień ✓ rejestr skarg i wniosków, ✓ rejestr zarządzeń Wójta, ✓ rejestr uchwał Rady Gminy ✓ rejestr informacji publicznej	Samodzielne stanowisko ds. organizacyjno – administracyjnych

✓ rejestr delegacji ✓ rejestr kontroli	
PIĘTRO I	POKÓJ Nr 19
1.Programy : „Finansowo –Księgowy FK, program do wystawiania faktur, program środków trwałych, program „Bestia”,	Dwa stanowiska pracy ds. księgowości budżetowej
PIĘTRO I	POKÓJ Nr 20
1.Programy :Ewidencji ludności „PESEL”, program- wydawania dowodów osobistych „Program Działalności Gospodarczej „SPUTNIK” 2.Rejestry w wersji papierowej : ✓ rejestr cudzoziemców zameldowanych czasowo do 3m-cy, ✓ lista przedpoborowych i poborowych, ✓ rejestr wyborców, ✓ rejestr wydanych zezwoleń na sprzedaż napojów alkoholowych,	Samodzielne stanowisko ds. obywatelskich i społecznych, ewidencji działalności gospodarczej
PIĘTRO II	POKÓJ Nr 24
1.Rejestry, dokumenty w wersji papierowej: ✓ rejestr skarg i wniosków, ✓ rejestr wniosków i interpelacji radnych, ✓ rejestr oświadczeń majątkowych radnych ✓ rejestr podjętych uchwał przekazanych na stanowiska ✓ rejestr projektów uchwał	Samodzielne stanowisko ds. obsługi rady, zaopatrzenia, transportu
PIĘTRO II	POKÓJ Nr 26
1.Program ewidencja gruntów i budynków 2. Rejestry w wersji papierowej : ✓ rejestr teczek własnościowych, ✓ rejestr umów dzierżawy ✓ rejestr nabycia i zbycia nieruchomości	Stanowisko ds. gospodarki nieruchomościami

Załącznik nr 2

Budynek Gminnego Centrum Informacji ul. Jeziorna -6, Kobylanka

Pomieszczenie GCI	
1.Rejestry, dokumenty w wersji papierowej: ✓ rejestr osób bezrobotnych ✓ indeks firm	

Załącznik nr 3

Budynek Straży Gminnej ul. Szczecińska 17, Morzyczyn

Pomieszczenie straży gminnej	
1.Rejestry,dokumenty w wersji papierowej**:** ✓ rejestr interwencji, ✓ rejestr nałożonych mandatów karnych, ✓ rejestr spraw o wykroczenia, ✓ notatniki służbowe ✓ kopie wniosków o ukaranie kierowanych do sądu ✓ rejestr kart MRD -5 ✓ rejestr korespondencji wpływającej i wychodzącej	**Komendant Straży,** **Strażnik gminny**

Załącznik Nr 4

Opis struktur zbiorów danych

1. Ewidencja zmarłych pochowanych na cmentarzu
- imiona i nazwiska,
- ostatnie miejsce zamieszkania
- data i miejsce urodzenia
- data i miejsce zgonu

2. Decyzje o nałożeniu zobowiązań do świadczeń rzeczowych i osobistych.
- imiona i nazwiska,
- adres zamieszkania.
- rodzaj świadczenia

3. Dziennik korespondencji wpływającej do urzędu
- data wpływu
- imiona i nazwiska,
- adres zamieszkania.
- znak sprawy
- treść wniosku, podania
- komu przydzielono – podpis odbierającego

4. Rejestr wysyłanej korespondencji
- data przekazania wysyłki do adresatów
- imiona i nazwiska,
- adres zamieszkania.
- treść pism wysyłanych
- kto wysyła - znak pisma

5. Rejestr psów.
- imiona i nazwiska,
- adres zamieszkania.
- kod pocztowy,
- rasa psa

6. Rejestr zezwoleń na wycinkę drzew.
- imiona i nazwiska,
- adres zamieszkania.
- rodzaj zameldowania,
- kod pocztowy,
- nr działki

7. Ewidencja ewidencji zabytków.
- imiona i nazwiska,
- adres zamieszkania.
- kod pocztowy,
- nr działki

8.Rejestr przydomowych oczyszczalni ścieków

- imię i nazwisko,
- adres,
- numer działki

9. Rejestr decyzji o warunków zabudowy i zagospodarowania terenu.

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

10. Rejestr decyzji o ustaleniu celu publicznego.

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

11. Rejestr zaświadczeń z planu i wypisów i wyrysów

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

12. Rejestr wniosków do zmian w planie zagospodarowania przestrzennego.

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

13. Rejestr zaświadczeń – zarobki

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

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
- zaświadczenie o stanie zdrowia
- zdjęcia

16. 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

17. Rejestr decyzji na zajęcie pasa drogowego.

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

18. Rejestr decyzji na wbudowanie urządzenia w drogę.

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

19. Rejestr zamówień publicznych

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

20. Podatki

- imiona i nazwiska,
- imię ojca i matki
- adres zamieszkania.
- rodzaj zameldowania,
- kod pocztowy,

- pesel
- NIP
- data urodzenia
- nr telefonu
- nr działki

21. Pojazdy

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

22. 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

23.Rejestr zaświadczeń

- data wpływu wniosku
- nr zaświadczenia
- data wydania
- imię i nazwisko
- adres, NIP
- treść zaświadczenia
- podpis pracownika
- forma odbioru

24. Rejestr tytułów wykonawczych

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

25.Rejestr upomnień

- Nr ewidencyjny upomnienia,
- Data wystawienia upomnienia,
- Nr konta zobowiązanego,
- Nazwisko i imię lub nazwa zobowiązanego,
- Adres zamieszkania,
- Należność ; rodzaj –okres, kwota, kwota upomnienia, razem , data doręczenia upomnienia

26. Rejestr skarg i wniosków

- imiona i nazwiska,
- adres zamieszkania.
- kod pocztowy,
- przedmiot skargi, zażalenia,
- data zlecenia załatwienia skargi,
- komu zlecono załatwienie,
- termin załatwienia,
- sposób załatwienia,
- data wysłania zawiadomienia,
- kogo zawiadomiono,
- uwagi

27.Rejestr pełnomocnictw, upoważnień

- imię i nazwisko
- data wydania
- data anulowania upoważnienia

28.Rejestr zarządzeń Wójta

- nr zarządzenia,
- data podjęcia,
- treść,
- termin wykonania,
- wykonawca Zarządzenia,
- uwagi

29.Rejestr uchwał Rady Gminy

- nr uchwały,
- data podjęcia,
- treść uchwały,
- termin wykonania
- data przekazania uchwały
- wykonawca uchwały,
- ogłoszenie w Dz.U.

30.Rejestr informacji publicznej

- data wpływu,
- imię i nazwisko,
- adres
- przedmiot wniosku
- załatwiający wniosek
- data załatwienia,

- sposób załatwienia,
- powiadomiono,
- przekazano wg właściwości
- uwagi

31.Rejestr delegacji

- data wystawienia
- nazwisko i imię,
- wyjazd od –do,
- środek lokomocji,
- dokąd
- w jakiej sprawie
- uwagi

32.Rejestr kontroli

- imię i nazwisko ,tytuł służbowy kontrolującego,
- przez kogo delegowany,
- data i nr delegacji służbowej,
- czas trwania czynności kontrolnych,
- wyszczególnienie skontrolowanych działów pracy,
- określenie charakteru czynności oraz wydane zarządzenie doraźne,
- podpisy kontrolującego, kierownika jednostki kontrolowanej,
- protokół z kontroli,
- zarządzenie wydane po kontroli,
- uwagi

33. Program finansowo-księgowy

- imiona i nazwiska
- adres zamieszkania

34. Rejestr faktur

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

35. 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

36. Rejestr cudzoziemców zameldowanych czasowo do 3 miesięcy

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

37. Lista przedpoborowych i poborowych

- imiona i nazwiska,
- imię ojca
- PESEL
- adres stałego zameldowania

38. Ewidencja działalności gospodarcze

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

39. Rejestr wydanych zezwoleń na sprzedaż napojów alkoholowych

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

40. Rejestr skarg i wniosków

- imiona i nazwiska,
- adres zamieszkania.
- kod pocztowy,
- przedmiot skargi, zażalenia,
- data zlecenia załatwienia skargi,
- komu zlecono załatwienie,
- termin załatwienia,
- sposób załatwienia,
- data wysłania zawiadomienia,
- kogo zawiadomiono,
- uwagi

41.Rejestr wniosków i interpelacji radnych

- imię i nazwisko radnego,
- data zgłoszenia wniosku, interpelacji,
- data udzielenia odpowiedzi,
- treść zgłoszonego wniosku, interpelacji,
- treść udzielonej odpowiedzi,
- uwagi

42.Rejestr oświadczeń majątkowych radnych

- 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

43.Rejestr podjętych uchwał przekazywanych na stanowiska

- data
- nr uchwały
- treść
- imię i nazwisko odbierającego
- data odbioru,
- podpis

44.Rejestr projektów uchwał

- tytuł projektu uchwały,
- projektodawca,
- nr Uchwały
- data

45.Rejestr teczek własnościowych

- nr teczki
- imię i nazwisko

46. Rejestr umów nabycia i zbycia nieruchomości

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

47.Rejestr umów dzierżaw

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

48.Rejestr osób bezrobotnych

- Imię i nazwisko
- Adres zamieszkania
- Kontakt telefoniczny

49.Indeks firm

- nazwa firmy
- adres

50. Rejestr interwencji

- imiona i nazwiska,
- adres zamieszkania.
- nr telefonu
- nr rej pojazdu
- powód interwencji
- nałożony mandat karny

51. Rejestr nałożonych mandatów karnych

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

52. Rejestr spraw o wykroczenia

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

53.Notatniki służbowe

- przebieg służby z podaniem godzin patrolowania danego rejonu
- podjęcia interwencji,
- dane dotyczące osoby legitymowanej(imię i nazwisko, data urodzenia ,miejsce zamieszkania, nr dokumentu tożsamości)
- rodzaju dokumentu lub oświadczenie , które stanowi podstawę do ustalenia tożsamości,
- czasu, miejsca oraz podstawy prawnej i faktycznej podjęcia czynności legitymowania

54. Kopie wniosków o ukaranie kierowanych do sądu

- imię i nazwisko,
- adres zamieszkania,
- imię rodziców,
- data i miejsce urodzenia,
- treść popełnionego wykroczenia

55.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

56.Rejestr korespondencji wpływającej do urzędu

- data wpływu
- imiona i nazwiska,
- adres zamieszkania.
- znak sprawy
- treść wniosku, podania
- komu przydzielono – podpis odbierającego

Załącznik nr 5

W z ó r

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

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 Informa

Załącznik nr 6

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

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

Nazwisko i Imię	Komórka organizacyjna	Data,podpis
Kaszubski Andrzej	Wójt	
Lubert Tadeusz	Z-ca Wójta	
Jolanta Kazberuk	Sekretarz	
Bernadeta Opasińska	Skarbnik	
Ewa Radlińska	Z-ca Skarbnika	
Jolanta Szymańska	Księgowość	
Elżbieta Sznycer	Organizacyjno -administracyjny	
Iwona Lisowska	Księgowość	
Izabela Drąg	Księgowość	
Małgorzata Hoff	Księgowość podatkowa, windykacja	
Izabela Pankiewicz	Wymiar podatków i opłat	
Małgorzata Kopa	Wymiar podatków i opłat	
Łucja Klińska	ds. obywatelskich i społecznych, ewidencja działalności gospodarczej	
Joanna Baszak	Obsługa Rady Gminy	
Elżbieta Sawka	Gospodarka nieruchomościami	
Magdalena Zawadzka	Gospodarka nieruchomościami	

Adam Hendzel	Obsługa informatyczna	
Iwona Wróbel	Gospodarka komunalna	
Adam Kawczyński	Inwestycje	
Edyta Filipowicz	Stanowisko obsługi interesantów	
Marcin Lewicki	Ochrona środowiska	
Hanna Olszewska	Planowanie przestrzenne	
Magdalena Wawrowicz	Planowanie przestrzenne	
Dorota Frąckiewicz	Wynagrodzenia, kadry, oświata	
Beata Domaradzka	Inwestycje	
Zbigniew Sroczyk	Inwestycje	
Irena Staniszewska	Gminne Centrum Informacji	
Robert Sawicki	Komendant Straży	
Robert Kosobucki	Strażnik Gminny	

Załącznik nr 7

……..……
/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 8

.....

/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 9

(imię i nazwisko)	(stanowisko)

Lp.	Data nadania upoważnienia	Data ustania upoważnienia	Zakres upoważnienia	Hasło	Uwagi
1.					
2.					
3.					
4.					

Zakres upoważnienia :

wgląd	D
wprowadzenie	W
Modyfikacja	M
Usuwanie	U

(Administrator Bezpieczeństwa Informacji)

…….
(imię i nazwisko)

…….

(miejscowość, data)