ZARZĄDZENIE Nr 26/2012
Wójta Gminy Jastrząb
z dnia 27 kwietnia 2012r.

w sprawie: wprowadzenia Polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy w Jastrzębiu.

Na podstawie § 5 rozporządzenia Prezesa Rady Ministrów z dnia 25 sierpnia 2005 roku w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz. U. Nr 171 poz. 1433), § 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)., art. 31 ustawy z dnia 8 marca 1990r. o samorządzie gminnym (Dz. U. z 2001 r. Nr 142, poz. 1591 z późn. zm.) – **zarządzam co następuje:**

§1

Wprowadzam **Politykę bezpieczeństwa i instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy w Jastrzębiu** stanowiącą załącznik do niniejszego zarządzenia.

§2

Nadzór nad wykonaniem niniejszego zarządzenia powierza się Administratorowi Bezpieczeństwa Informacji danych zawartych w systemach informatycznych Urzędu.

§ 3

Traci moc Zarządzenie Wójta Gminy Jastrząb Nr 50/2007 z dnia 15 października 2007r.

§ 4

Zarządzenie wchodzi w życie z dniem podpisania.

WÓJT GMINY
mgr Zofia Kosno

Załącznik
do Zarządzenia Nr 26/2012
Wójta Gminy Jastrząb
z dnia 27.04.2012r.

Polityka bezpieczeństwa

i

instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych

w URZĘDZIE GMINY W JASTRZĘBIU

SPIS TREŚCI:

Wprowadzenie 3

Rozdział 1. Opis zdarzeń naruszających ochronę danych osobowych 5

Rozdział 2. Zabezpieczenie danych osobowych 7

Rozdział 3. Kontrola przestrzegania zasad zabezpieczenia danych osobowych 10

Rozdział 4. Postępowanie w przypadku naruszenia ochrony danych osobowych 11

Rozdział 5. Monitorowanie zabezpieczeń 13

Rozdział 6. Szkolenia 13

Rozdział 7. Niszczenie wydruków i zapisów na nośnikach magnetycznych 13

Rozdział 8. Archiwizacja danych 14

Rozdział 9. Postanowienia końcowe 14

Załącznik nr 1 – Granice obszarów oraz osoby i wydziały, które przetwarzają dane osobowe 16

Załącznik nr 2 – Opis struktur zbiorów danych 21

Załącznik nr 3 – Raport z naruszenia bezpieczeństwa systemu informatycznego w Urzędzie Gminy w Jastrzębiu 24

Załącznik nr 4 – Wykaz osób, które zostały zapoznane z Polityką Bezpieczeństwa. 25

Załącznik nr 5 – Oświadczenie 26

Załącznik nr 6 – Upoważnienie 27

WPROWADZENIE

Niniejszy dokument opisuje reguły dotyczące bezpieczeństwa danych osobowych zawartych w systemach informatycznych w Urzędzie Gminy w Jastrzębiu. 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 w Jastrzębiu", 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 roku 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 w Jastrzębiu.

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.

Niniejszy dokument jest zgodny z następującymi aktami prawnymi:

1) **Ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.)**

2) **Ustawą o ochronie informacji niejawnych z dnia 22 stycznia 1999 r. (tekst jednolity Dz. U. z 2005 r. Nr 196, poz. 1631 z późn. zm.)**

3) **Rozporządzeniem Prezesa Rady Ministrów z dnia 25 sierpnia 2005 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz. U. Nr 171 poz. 1433)**

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 w Jastrzębiu 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),
   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 w Jastrzębiu i ich zabezpieczeń zawiera **załącznik nr 1 i 2** do niniejszego dokumentu.

7. W celu ochrony przed utratą danych stosowane są następujące zabezpieczenia:

   1) odrębne zasilanie sprzętu komputerowego,
   2) ochrona serwerów przed zanikiem zasilania poprzez stosowanie zasilaczy zapasowych UPS,
   3) ochrona przed utratą zgromadzonych danych przez robienie kopii zapasowych na dyskach twardych, z których w przypadku awarii odtwarzane są dane i system operacyjny,
   4) ochrona przed awarią podsystemu dyskowego przez używanie macierzy dyskowych. Uszkodzenie jakiegokolwiek z dysków zestawu nie spowoduje utraty danych, a nawet zatrzymania pracy systemu (zastosowanie elementów hotswap i hotspare).

8. Zabezpieczenia przed nieautoryzowanym dostępem do baz danych Urzędu:

   1) wszystkie gniazda lokalnej sieci komputerowej są galwanicznie oddzielone od szkieletu sieci komputerowej. Podłączenie (zkrosowanie) danego użytkownika do sieci komputerowej dokonuje Administrator Bezpieczeństwa Informacji,
   2) aby uzyskać dostęp do zasobów sieci, należy zwrócić się do Administratora Bezpieczeństwa z odpowiednim wnioskiem, w którym podane będą dane nowego użytkownika oraz zasoby jakie ma on mieć udostępnione,
   3) w systemie informatycznym Urzędu zastosowano podwójną autoryzację użytkownika. Pierwszej autoryzacji należy dokonać w momencie uzyskania dostępu do komputera, podając login użytkownika i hasło. Drugiej autoryzacji należy dokonać uruchamiając program użytkowy, podając login użytkownika i hasło. Dostęp do wybranej bazy danych Urzędu uzyskuje się dopiero po poprawnym podwójnym zalogowaniu się do systemu informatycznego.

9. Postanowienia końcowe.

   1) do pomieszczeń w których następuje przetwarzanie danych osobowych mają dostęp tylko uprawnione osoby bezpośrednio związane z nadzorem nąd serwerami lub aplikacjami.
   2) zabezpieczenie przed nieuprawnionym dostępem do danych, prowadzone jest przez Administratora Bezpieczeństwa zgodnie z przyjętymi procedurami nadawania uprawnień do systemu informatycznego,
   3) osoby mające dostęp do danych powinny posiadać zaświadczenie o przebytym szkoleniu z zakresu ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997r. (tekst jednolity Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.),
   4) w pomieszczeniach w których znajdują się serwery powinna być zamontowana klimatyzacja, która zapewnia właściwą temperaturę i wilgotność powietrza dla sprzętu komputerowego,
   5) w pobliżu wejścia do pomieszczenia z serwerami i innym urządzeniami znajduje się gaśnica, która okresowo jest napełniana i kontrolowana przez specjalistę,
   6) większość urządzeń w serwerowni umieszczona jest w szafach serwerowych i sieciowych.

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 Gminy,
   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 Gminy.

5. Administrator Bezpieczeństwa dokumentuje zaistniały przypadek naruszenia oraz sporządza raport wg wzoru stanowiącego **załącznik nr 3**, który powinien zawierać w szczególności:

1) wskazanie osoby powiadamiającej o naruszeniu oraz innych osób zaangażowanych lub odpytanych w związku z naruszeniem,
2) określenie czasu, 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:
   a) Administrator Danych,
   b) Administrator Bezpieczeństwa Informacji.

2. W ramach kontroli należy zwracać szczególna uwagę na:
   a) okresowe sprawdzanie kopii bezpieczeństwa pod względem przydatności o możliwości odtwarzania danych,
   b) kontrola ewidencji nośników magnetycznych,
   c) kontrola właściwej częstotliwości zmiany haseł.

ROZDZIAŁ 6

SZKOLENIA

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

ROZDZIAŁ 7

NISZCZENIE WYDRUKÓW I ZAPISÓW NA NOŚNIKACH DANYCH

1. Nośniki danych 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 danych powinna być sprawdzona przez Administratora Bezpieczeństwa Informacji.
4. Uszkodzone nośniki danych 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 Administrator Bezpieczeństwa Informacji.
4. Na koniec danego miesiąca wykonywane są kopie bezpieczeństwa z całego programu przetwarzającego dane. Nośniki z kopiami bezpieczeństwa przechowywane są w kasie Urzędu.
5. Kopie awaryjne przechowywane są w szafie metalowej w pokoju Nr 8 Urzędu Gminy w Jastrzębiu.
6. Dyskietki, 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 4** 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 późn. zm.) 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 późn. zm.), 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 zabezpieczania 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 w Jastrzębiu" wchodzi w życie z dniem jej podpisania przez Wójta.

Załącznik Nr 1 do „Polityki bezpieczeństwa"

Granice obszarów oraz osoby i wydziały, które przetwarzają dane osobowe w budynku przy pl. Niepodległości 5

POKÓJ NR 15 – II piętro – OBSŁUGA; poczta przychodząca	
Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji	Imię i nazwisko: - Malwina Ziętek

POKÓJ NR 19 – II piętro – OBSŁUGA Wydziału Finansowego – KASA	
Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji	Imię i nazwisko: - Justyna Stępień

POKÓJ NR 20 – II piętro – OBSŁUGA Wydziału Finansowego – program „Podatek rolny, leśny, od nieruchomości i od środków transportowych"	
Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji	Imię i nazwisko: - Elżbieta Gołosz - Aleksandra Burek - Jadwiga Szafrańska

POKÓJ NR 22 – II piętro – OBSŁUGA Wydziału Finansowego – program „Płace", „Płatnika"	
Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji	Imię i nazwisko: - Jadwiga Nowak - Małgorzata Rokosz

POKÓJ NR 23 – II piętro – OBSŁUGA Wydziału Rolnictwa i Gospodarki Wodnej – program „Woda"	
Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji	Imię i nazwisko: - Krystyna Czyżewska

POKÓJ NR 25 – II piętro – OBSŁUGA Wydziału Budownictwa	
Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji	Imię i nazwisko: - Jolanta Gromek

POKÓJ NR 25 – II piętro – OBSŁUGA Wydziału Ochrony Środowiska – program „GOMIG"	
Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji	Imię i nazwisko: - Magdalena Bińkowska - Bogdan Zdon

POKÓJ NR 11 – I piętro – OBSŁUGA USC – programy „PB_USC", „Dowody osobiste"	
Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji	Imię i nazwisko: - Anna Matuszkiewicz

POKÓJ NR 11 – I piętro – OBSŁUGA Ewidencji Ludności – programy „SELWIN", „RWWIN"	
Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji	Imię i nazwisko: - Lilla Grzyb - Milena Wanat

POKÓJ NR 10 – I piętro – OBSŁUGA Kadr	
Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji	Imię i nazwisko: - Daria Sławińska

POKÓJ NR 8 – I piętro – OBSŁUGA Biura rady	
Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji	Imię i nazwisko: - Elżbieta Bodo

Osoby mające prawo wglądu do danych osobowych w kartotekach z uwagi na wykonywane zakresy czynności	
Administrator Danych	Imię i nazwisko: Zofia Kosno
Sekretarz Gminy	Imię i nazwisko: Jan Gula
Administrator Bezpieczeństwa Informacji	Imię i nazwisko: Łukasz Bińkowski
Radca Prawny	Imię i nazwisko: Marek Gordat

Uwaga!

1. Obsługa techniczna urzędu, (sprzątaczki, kierowcy) podpisują oświadczenie, którego wzór stanowi **załącznik nr 5** do „Polityki bezpieczeństwa".
2. Osoby odbywające staż, praktykę mają wgląd do danych osobowych oraz do systemu informatycznego na podstawie upoważnienia (**załącznik nr 6**) nadanego przez Administratora oraz oświadczenia (**załącznik nr 5**).

WÓJT GMINY
mgr Zofia Kosno

Załącznik Nr 2 do „Polityki bezpieczeństwa" – Opis struktur zbiorów danych

Zbiór danych KADRY zawiera następujące pola:

Identyfikacja
• nazwisko aktualne,
• nazwisko rodowe,
• nazwisko rodowe matki,
• pierwsze imię,
• drugie imię,
• imię ojca,
• imię matki,
Urodzenie
• płeć,
• data urodzenia,
• miejsce urodzenia,
Pochodzenie
• obcokrajowiec,
• karta stałego pobytu,
• narodowość,
• obywatelstwo,
Dokument tożsamości
• dowód osobisty (seria i nr),
• wydany przez (organ administracyjny wydający dowód osobisty),
• paszport (nr),
• wydany przez (organ wydający paszport),
Dane ewidencyjne
• numer PESEL,
• numer NIP,
Pozostałe informacje
• Urząd Skarbowy (nazwa właściwego urzędu skarbowego),
• wykształcenie,
• zawód wyuczony,
Pochodzenie danych
• osoba rejestrująca dane,
• data rejestracji,
• źródło pochodzenia informacji.

Załącznik Nr 3 do „Polityki bezpieczeństwa"

Raport
z naruszenia bezpieczeństwa systemu informatycznego w Urzędzie Gminy w Jastrzębiu

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 4 do „Polityki bezpieczeństwa"

Wykaz osób, które zostały zapoznane z „Polityką bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Urzędzie Gminy w Jastrzębiu" 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 5 do „Polityki bezpieczeństwa"

.....
(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 (tekst jednolity Dz.U. z 2002 r. Nr 101, poz.926 z późn. zm.),
   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 6 do „Polityki bezpieczeństwa"

.....
(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 (tekst jednolity Dz.U. z 2002 r. Nr 101 poz.926 z późn.zm.)

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