WÓJT GMINY SOMONINO
83-314 SOMONINO
ul. Ceynowy 21

Zarządzenie Nr 26/2012

Wójta Gminy Somonino

z dnia 20.04.2012 r.

w sprawie wprowadzenia „Polityki bezpieczeństwa" i „instrukcji zarządzania systemem informatycznym" służącym do przetwarzania danych osobowych w Urzędzie Gminy w Somoninie

Na podstawie art. 36 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.) 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. z 2004 r. Nr 100, poz. 1024) zarządzam, co następuje:

§ 1

Dla zapewnienia ochrony przetwarzanych danych osobowych w Urzędzie Gminy w Somoninie wprowadza się :Politykę bezpieczeństwa" i „instrukcję zarządzania systemem informatycznym" w brzmieniu jak w załączniku do niniejszego zarządzenia.

§ 2

Dokument, o którym mowa w § 1 ma zastosowanie na wszystkich stanowiskach pracy urzędu, gdzie przetwarzane są dane osobowe lub praca odbywa się w systemie informatycznym.

§ 3

Tracą moc zarządzenia: nr 7/99 Wójta Gminy Somonino z dnia 01.10.1999 r. w sprawie sposobu zarządzania systemem informatycznym służącym do przetwarzania danych osobowych i nr 15/2007 Wójta Gminy Somonino z dnia 14.03.2007 r. w sprawie wprowadzenia „Polityki Bezpieczeństwa" przy przetwarzaniu danych osobowych w Urzędzie Gminy w Somoninie.

§ 4

Zarządzenie wchodzi w życie z dniem podpisania.

WÓJT
mgr Marian Kryszewski

Załącznik
do Zarządzenia Nr 26/2012
Wójta Gminy Somonino
z dnia 20.04.2012 .

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

w Urzędzie Gminy w Somoninie

Opracował:

1) **Marcin Singer – insp. ds. obsługi informatycznej**
2) **Sabina Recław – Drewa – sekretarz gminy**

Zatwierdził:

Marian Kryszewski
Wójt Gminy Somonino
Administrator Bezpieczeństwa Informacji

WÓJT
mgr Marian Kryszewski

SPIS TREŚCI:

WPROWADZENIE

Niniejszy dokument opisuje reguły dotyczące bezpieczeństwa danych osobowych zawartych w systemach informatycznych w Urzędzie Gminy w Somoninie. 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", 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 § 3 rozporządzenia Prezesa Rady Ministrów z dnia 25 lutego 1999 roku w sprawie podstawowych wymagań bezpieczeństwa systemów i sieci teleinformatycznych (Dz.U. Nr 18 poz. 162) 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 Somoninie
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 Gminy spełnia jednocześnie funkcję Administratora Bezpieczeństwa Informacji (ABI) danych zawartych w systemach informatycznych Urzędu, zwanego dalej "Administratorem Bezpieczeństwa", zastępstwo w razie potrzeby pełni Zastępca Wójta Gminy.

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) zapobieganie naruszeniom przepisów ustawy o ochronie danych osobowych,
4) nadzoru 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.: 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
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 Somoninie 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 biurowych
2) zabezpieczenie wejścia do pomieszczeń, o których mowa w pkt. 1,

3) szczególne zabezpieczenie centrum przetwarzania danych (komputer centralny, serwerownia) poprzez wyposażenie pomieszczeń w szafy dające gwarancję bezpieczeństwa dokumentacji, w tym szafy posiadające zamki.

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 Urzędzie Gminy w Somoninie" 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 Somoninie i ich zabezpieczeń zawiera załącznik **nr 1** do niniejszego dokumentu.

7. W celu ochrony przed utratą danych w Urzędzie Gminy w Somoninie 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 zewnętrznym nośniku, z których w przypadku awarii odtwarzane są dane i system operacyjny
4) ochrona przed awarią podsystemu dyskowego przez używanie RAID

Uszkodzenie jakiegokolwiek z dysków zestawu nie spowoduje utraty danych.

4. *Zabezpieczenia przed nieautoryzowanym dostępem do baz danych Urzędu:*

1) *wszystkie gniazdka lokalnej sieci komputerowej są galwanicznie oddzielone od szkieletu sieci komputerowej. Podłączenie danego użytkownika do sieci komputerowej dokonuje Administrator Systemów Informatycznych (ASI)*
2) *w systemie informatycznym Urzędu zastosowano podwójną autoryzację użytkownika. Pierwszej autoryzacji należy dokonać w momencie uzyskania dostępu do serwera Urzędu, 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 Urzędu.*

3. *Zabezpieczenia przed nieautoryzowanym dostępem do baz danych Urzędu poprzez internet.*

W zakresie dostępu z sieci wewnętrznej Urzędu do sieci rozległej Internet zastosowano środki ochrony przed podsłuchiwaniem, penetrowaniem i atakiem z zewnątrz. Zastosowano firewall, który ma za zadanie uwierzytelnianie źródła przychodzących wiadomości oraz filtrowanie pakietów w oparciu o adres IP, numer portu i inne parametry. Ściana ogniowa składa się z bezpiecznego systemu operacyjnego i filtra pakietów. Ruch pakietów, który firewall przepuszcza jest określony przez administratora.

Firewall zapisuje do logu fakt zaistnienia wyjątkowych zdarzeń i śledzi ruch pakietów przechodzących przez nią. Dostęp do sieci jest ustalony indywidualnie dla każdego użytkownika na podstawie wniosku.

Oprócz filtra pakietów (firewall) zastosowano również system wykrywający obecność wirusów w poczcie elektronicznej.

W efekcie zapewnione jest:

1) *zabezpieczenie sieci przed atakiem z zewnątrz poprzez blokowanie wybranych portów,*
2) *filtrowanie pakietów i blokowanie niektórych usług,*
3) *objęcie ochroną antywirusową wszystkich danych ściąganych z Internetu oraz routerze na stacjach lokalnych,*
4) *zapisywanie logów połączeń użytkowników z siecią Internet*

4. *Postanowienia końcowe.*

1) *do pomieszczeń w których następuje przetwarzanie danych osobowych mają dostęp tylko uprawnione osoby bezpośrednio związane z nadzorem nad serwerami lub aplikacjami.*
2) *zabezpieczenie przed nieuprawnionym dostępem do danych, prowadzone jest przez Administratora Bezpieczeństwa zgodnie z przyjętymi procedurami wydawania upoważnień do przetwarzania danych osobowych*
3) *osoby mające dostęp do danych powinny oświadczyć, że przebyły szkolenie z zakresu ustawy o ochronie danych osobowych i znane są im stosowne w tym zakresie przepisy prawa.*

4) *w pomieszczeniach w których znajdują się serwery jest 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

Administrator danych, która jest jednocześnie „Administrator Bezpieczeństwa Informacji" sprawuje nadzór nad przestrzeganiem zasad ochrony danych osobowych wynikających z ustawy o ochronie danych osobowych oraz zasad ustanowionych w niniejszym dokumencie.

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 lub Administratora Systemów Informatycznych

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 ASI

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

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) nawiązuje bezpośredni kontakt, jeżeli zachodzi taka potrzeba, ze specjalistami spoza Urzędu.

5. ABI lub ASI 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 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, jeżeli wykonywał to ASI niezwłocznie przekazuje Administratorowi Danych (Wójtowi), a w przypadku jego nieobecności osobie uprawnionej.

7. Po wyczerpaniu niezbędnych środków doraźnych po zaistniałym naruszeniu ABI lub ASI 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 Systemów Informatycznych, 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, jako ABI
   b) Administrator Systemów Informatycznych (ASI)

2. W ramach kontroli należy zwracać szczególna uwagę na:
   a) okresowe sprawdzanie kopii bezpieczeństwa pod względem przydatności do 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 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 Administrator Bezpieczeństwa Informacji,
4. Na koniec danego miesiąca wykonywane są kopie bezpieczeństwa z całego programu przetwarzającego dane. Nośniki z kopiami bezpieczeństwa przechowywane są w (kasa Urzędu)

5. Kopie awaryjne przechowywane są w *(kasa pancerna, szafa metalowa - w wyznaczonym pomieszczeniu lub instytucji , z którą podpisano stosowne porozumienie),*
6. Nośniki , 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 lub Administratora Systemów Informatycznych

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) 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), 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 w Somoninie" wchodzi w życie z dniem jej podpisania przez Wójta.*

Załącznik Nr 1
do Polityki Bezpieczeństwa
przetwarzania danych osobowych
i instrukcji zarządzania systemem
informatycznym stanowiącej załącznik
do Zarządzenia Nr 26/2012
Wójta Gminy Somonino
z dnia 20.04.2012 r.

GRANICE OBSZARÓW w budynku Urzędu Gminy w Somoninie wraz z WYKAZEM ZBIORÓW DANYCH OSOBOWYCH w nich przetwarzanych i wskazaniem programów zastosowanych do ich przetwarzania

Lp.	Nr pomieszczenia, w którym przetwarzane są dane osobowe	Nazwa zbioru przetwarzanych danych osobowych	Programy zastosowane do przetwarzania danych osobowych
1	2	3	4
1.	1	Akta Stanu Cywilnego	forma papierowa
2.	1	Ewidencja ludności i dowody osobiste	ELUD
3.	10	Świadczenia rodzinne	EZAR
4.	10	Zaliczka alimentacyjna Fundusz alimentacyjny	EZAR
5.	10	Zarządzanie, kryzysowe, informacje niejawne, kwalifikacja wojskowa	forma papierowa + komputer certyfikowany
6.	12	Podatki i opłaty lokalne	WIP, POST, POGRUN
7.	13	Zamówienia publiczne	Zamówienia publiczne
8.	13	Ochrona środowiska, rolnictwa, gospodarka odpadami	forma papierowa
9.	14	Oświadczenia majątkowe radnych	forma papierowa
10.	14	Działalność gospodarcza, ewidencja usług turystycznych, rejestr zezwoleń na sprzedaż napojów alkoholowych	CEIDG forma papierowa forma papierowa
11.	15	Przelewy (wpłaty, wypłaty) Wpłaty, wypłaty gotówkowe	HOME BANK KASA
12.	16	Pomoc stypendialna	Program STYPENDIA
13.	16	Wyprawka szkolna	forma papierowa
14.	16	Dodatki mieszkaniowe	forma papierowa
15.	16	Płace Składki na ZUS	PŁACE PŁATNIK

16.	16	Kadry Informacja oświatowa	KADRY Program ministerialny - SIO
17.	16a	Płace Składki na ZUS Pracownicy młodociani Arkusze organizacyjne	PŁACE PŁATNIK forma papierowa ProgMan
18.	17	Budownictwo i planowanie przestrzenne	forma papierowa
19.	17	Ewidencja gruntów i budynków	zadanie Starostwa Powiatowego- urząd gminy ma możliwość korzystania z programu Starostwa
20.	17	Najem lokali, dzierżawy	forma papierowa
21.	17	Gospodarka nieruchomościami i mieszkaniowym zasobem gminy	forma papierowa
22.	19	Dane uczniów i nauczycieli będących uczestnikami projektów edukacyjnych realizowanych w ramach „Programu Operacyjnego Kapitał Ludzki 2007 ÷ 2013”	formularze w formacie MS Excel, zależne od rodzaju projektów
23.	Pomieszczenie sekretarza i radcy prawnego	Oświadczenia majątkowe kierowników jednostek i kierownictwa urzędu	forma papierowa
24.	23	Skargi i wnioski Wybory Referenda Spisy powszechne	Forma papierowa Forma papierowa + platforma udostępniana przez Krajowe Biuro Wyborcze forma papierowa forma papierowa + urządzenia do przesyłu dla rachmistrzów

Załącznik nr 2
do Polityki Bezpieczeństwa i „instrukcji zarządzania systemem informatycznym" służącym do przetwarzania danych osobowych w Urzędzie Gminy w Somoninie stanowiącej załącznik do Zarządzenia Nr ..26/2012 Wójta Gminy Somonino z dnia .20.04.2012r.

Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informatycznych i powiązania między nimi

Lp.	Nazwa zbioru danych osobowych	Zawartość pól informacyjnych	Powiązania między polami informatycznymi
1	2	3	4
1.	Budownictwo i planowanie przestrzenne	nazwiska i imiona, imiona rodziców, data urodzenia, adres zamieszkania lub pobytu, nr ewidencyjny PESEL, zawód, wykształcenie, seria i nr dowodu osobistego, nr, położenie, powierzchnia, wartość i przeznaczenie nieruchomości, nr i data aktu notarialnego, nr i data pozwolenia na budowę, typ projektu, nr i data uprawnień budowlanych	
2.	Ewidencja gruntów i budynków	nazwiska i imiona, imiona rodziców, adres zamieszkania lub pobytu, seria i nr dowodu osobistego, nr księgi wieczystej, nr działki, nr rej. gruntów, pow. gruntów, klasy i rodzaj gruntów, nr dowodu zmiany	
3.	Powszechny obowiązek obrony	nazwiska i imiona, imiona rodziców, data urodzenia, adres zamieszkania lub pobytu, nr ewidencyjny PESEL, miejsce pracy, zawód, wykształcenie, seria i nr dowodu osobistego, nr książeczki wojskowej, kategorie zdrowia, stan zdrowia, nałogi	
4.	Najem lokali	nazwiska i imiona, data urodzenia, adres zamieszkania lub pobytu, miejsce pracy, zawód	
5.	Dodatki mieszkaniowe	nazwiska i imiona, nazwisko i imię członków rodziny, daty urodzenia, adres zamieszkania lub pobytu, miejsce pracy, zawód, uzyskiwany dochód osoby ubiegającej się o dodatek mieszkaniowy oraz członków rodziny, ponoszone wydatki mieszkaniowe,	

		powierzchnia mieszkania, wyposażenie mieszkania w instalacje, wysokość czynszu, wysokość dodatku mieszkaniowego	
6.	Akta Stanu Cywilnego	nazwiska i imiona, imiona rodziców, data urodzenia, adres zamieszkania lub pobytu, nr ewidencyjny PESEL, zawód, wykształcenie, seria i nr dowodu osobistego, nazwisko panieńskie, nazwisko z poprzedniego małżeństwa, nazwisko rodowe, miejsce i godz. urodzenia, data i nr aktu zgonu, data i nr aktu małżeństwa, data i nr urodzenia, imię i nazwisko ojca, imię i nazwisko matki, imię i nazwisko współmałżonka, płeć, stan cywilny, data i miejsce zawarcia małżeństwa, miejsce wystawienia i nr aktu urodzenia żony, męża, data, godzina, miejsce zgonu, odnalezienia zwłok, data zgonu męża, matki, nazwisko, imię i adres osoby zgłaszającej zgony, nr aktu zgonu żony, męża, nazwisko rodowe matki i ojca mężczyzny, nazwisko rodowe matki i ojca kobiety, adnotacje o rozwodzie, nazwisko po zawarciu małżeństwa mężczyzny, kobiety, nr dowodu i miejsce wydania dowodu kobiety, mężczyzny, pesel, data unieważnienia aktu małżeństwa, urodzenia, zgonu, imię nadane z urzędu, data i nr orzeczenia sądu ustalającego ojcostwo, zaprzeczającego ojcostwo, przysposabiającego dziecko, imię i nazwisko osoby przysposabiającej dziecko, zmiana nazwiska dziecka, data rozwiązania poprzedniego małżeństwa, orzekającego separację, rozwodu	
7.	Ewidencja ludności i dowody osobiste	nazwiska i imiona, imiona rodziców, data urodzenia, adres zamieszkania lub pobytu, nr ewidencyjny PESEL, miejsce pracy, zawód, wykształcenie, seria i nr dowodu osobistego, nazwisko rodowe, nazwisko z poprzedniego małżeństwa, data i nr aktu urodzenia, małżeństwa, zgonu, imię i nazwisko ojca, imię i nazwisko matki, imię i nazwisko współmałżonka, płeć, kolor oczy, wzrost i wizerunek twarzy, miejsce urodzenia, zgonu, małżeństwa; data zgonu i zawarcia bądź	

		rozwiązania małżeństwa, nazwa i nr wojskowych dokumentów osobistych, obywatelstwo; rysopis; grupa krwi i czynnik RH, data i przyczyna utraty dowodu, rodzaj zameldowania	
8.	Podatki i opłaty lokalne	nazwiska i imiona, imiona rodziców, data urodzenia, adres zamieszkania lub pobytu, nr ewidencyjny PESEL, NIP, powierzchnia gruntów, nr działek i ich lokalizacja, nr budynków, wysokość podatku, wpłaty, zaległości, nadpłaty	ściąganie danych z programu ELUD, wymiana danych między programami WIP a POST i POGRUN
9.	Gospodarka nieruchomościami i mieszkaniowym zasobem gminy	Nazwiska i imiona, imiona rodziców, data urodzenia, adres zamieszkania lub pobytu, nr ewidencyjny PESEL, seria i nr dowodu osobistego, nr działki, powierzchnia nieruchomości i jej położenie, opłaty za użytkowanie wieczyste, nr KW, opłaty za dzierżawę i najem nieruchomości	
10.	Świadczenia rodzinne	nazwiska i imiona, imiona rodziców, data urodzenia, miejsce urodzenia, płeć, adres zamieszkania lub pobytu, nr ewidencyjny PESEL, seria i nr dowodu osobistego, nr telefonu, stan zdrowia, stan cywilny	Współpraca z programem ELUD
11.	Zaliczka alimentacyjna	nazwiska i imiona, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, nr ewidencyjny PESEL, seria i nr dowodu osobistego, nr telefonu, orzeczeń o karaniu, innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym	Czerpanie danych z programu ELUD
12.	Pomoc stypendialna	nazwiska i imiona, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, nr ewidencyjny PESEL, seria i nr dowodu osobistego, nr telefonu, nazwa i adres szkoły (kolegium), klasa, stan zdrowia, nałogi, inne orzeczenia wydawane w postępowaniu sadowym lub administracyjnym	
13.	Oświadczenia majątkowe radnych	nazwiska i imiona, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, seria i nr dowodu osobistego, stan majątkowy w tym informacje	

		o zasobach pieniężnych, nieruchomościach, udziałach: akcjach w spółkach prawa handlowego oraz nabyciu od Skarbu Państwa, innej państwowej osoby prawnej, gminy lub związku międzygminnego mienia, które podlegało zbyciu w drodze przetargu, a także dane o prowadzeniu działalności gospodarczej przez siebie lub małżonka oraz dotyczące zajmowania stanowisk w spółkach prawa handlowego i dotyczące majątku objętego wspólnością majątkową małżeńską, dane o zajmowaniu przez małżonka stanowisk (lub ich zmian) w urzędzie gminy lub w jednostkach organizacyjnych gminy, bądź zawartych przez siebie lub małżonka umowach cywilnoprawnych z organami gminy lub jej jednostkami organizacyjnymi	
14.	Oświadczenia majątkowe kadry kierowniczej UG i kierowników jednostek organizacyjnych	nazwiska i imiona, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, seria i nr dowodu osobistego, stan majątkowy w tym informacje o zasobach pieniężnych, nieruchomościach, udziałach: akcjach w spółkach prawa handlowego oraz nabyciu od Skarbu Państwa, innej państwowej osoby prawnej, gminy lub związku międzygminnego mienia, które podlegało zbyciu w drodze przetargu, a także dane o prowadzeniu działalności gospodarczej przez siebie lub małżonka oraz dotyczące zajmowania stanowisk w spółkach prawa handlowego i dotyczące majątku objętego wspólnością majątkową małżeńską, dane o zajmowaniu przez małżonka stanowisk (lub ich zmian) w urzędzie gminy lub w jednostkach organizacyjnych gminy, bądź zawartych przez siebie lub małżonka umowach cywilnoprawnych z organami gminy lub jej jednostkami organizacyjnymi	
15.	Dane uczniów i nauczycieli – uczestników projektów edukacyjnych	nazwisko, imiona, wiek, PESEL, wykształcenie, płeć, adres zamieszkania lub pobytu, adres poczty elektronicznej, nr telefonu komórkowego, nr telefonu stacjonarnego, status osoby na rynku pracy w	

	realizowanych w ramach Programu Operacyjnego Kapitał Ludzki 2007÷2013	chwili przystąpienia do projektu, szczegóły wsparcia, zakończenie udziału osoby we wsparciu zgodnie z zaplanowaną dla niej ścieżką uczestnictwa.	

Załącznik nr 3 do „Polityki bezpieczeństwa" i „instrukcji zarządzania systemem informatycznym" służącym do przetwarzania danych osobowych w Urzędzie Gminy w Somoninie stanowiącej załącznik do zarządzenia nr 26.2012 Wójta Gminy Somonino z dnia 20.04.2012

Raport
z naruszenia bezpieczeństwa systemu informatycznego w Urzędzie.....

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" i „instrukcji zarządzania systemem informatycznym" służącym do przetwarzania danych osobowych w Urzędzie Gminy w Somoninie stanowiącej załącznik do zarządzenia nr 26/2012 Wójta Gminy Somonino z dnia 20.04.2012

Wykaz osób, które zostały zapoznane z „Polityką bezpieczeństwa i obsługi systemów informatycznych służących do przetwarzania danych osobowych w Urzędzie Gminy w Somoninie, 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" i „instrukcji zarządzania systemem informatycznym" służącym do przetwarzania danych osobowych w Urzędzie Gminy w Somoninie stanowiącej załącznik do zarządzenia nr 26/2012 Wójta Gminy Somonino z dnia 20.04.2012

.....
/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 6 do „Polityki bezpieczeństwa" i „instrukcji zarządzania systemem informatycznym" służącym do przetwarzania danych osobowych w Urzędzie Gminy w Somoninie stanowiącej załącznik do zarządzenia nr 26/2012 Wójta Gminy Somonino z dnia 20.04.2012

.....
/miejscowość, data/

U P O W A Ż N I E N I E Nr.....

Na podstawie art.37 ustawy z dnia 29 sierpnia 1999 r. o ochronie danych osobowych (t.j. 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

Załącznik nr 7 do „Polityki bezpieczeństwa" i „instrukcji zarządzania systemem informatycznym" służącym do przetwarzania danych osobowych w Urzędzie Gminy w Somoninie stanowiącej załącznik do zarządzenia nr 16/2012 Wójta Gminy Somonino z dnia 20.04.2012

(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)