ZARZĄDZENIE NR 3 /11
KIEROWNIKA URZĘDU - WÓJTA GMINY SŁAWNO
z dnia 1 lutego 2011 roku

w sprawie : wprowadzenia zasad ochrony danych osobowych przetwarzanych w Urzędzie Gminy w Sławnie

Na podstawie art. 36 ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych / Dz. U. 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 / Dz. U. Nr 100, poz. 1024/ zarządzam co następuje :

§ 1. Dla zapewnienia ochrony przetwarzania danych osobowych wprowadza się „ Politykę bezpieczeństwa w zakresie przetwarzania danych osobowych " w Urzędzie Gminy w Sławnie stanowiącą załącznik Nr 1 do zarządzenia.

§ 2. „ Polityka bezpieczeństwa w zakresie przetwarzania danych osobowych " ma zastosowanie na wszystkich stanowiskach pracy, gdzie przetwarzane są dane osobowe lub praca odbywa się w systemach informatycznych będących w ewidencji urzędu.

§ 3. Dla zapewnienia ochrony przetwarzania danych osobowych wprowadza się „Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych " w Urzędzie Gminy w Sławnie stanowiąca załącznik Nr 2 do zarządzenia.

§ 4. „Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych " w Urzędzie Gminy w Sławnie ma zastosowanie na wszystkich stanowiskach pracy, gdzie przetwarzane są dane osobowe lub praca odbywa się w systemach informatycznych będących w ewidencji urzędu.

§ 5. Administratorem danych osobowych w Urzędzie Gminy w rozumieniu ustawy o ochronie danych osobowych jest Wójt Gminy.

§ 6. 1. W celu organizacji zasad ochrony, zabezpieczenia i kontroli przetwarzania danych osobowych w zbiorach danych osobowych Urzędu Gminy powołuje się Administratora bezpieczeństwa informacji.

2. Obowiązki Administratora bezpieczeństwa informacji powierza się Sekretarzowi Gminy

3. Zadania Administratora bezpieczeństwa informacji, określa załącznik nr 3 do niniejszego zarządzenia.

§ 7. 1. Do przetwarzania danych osobowych mogą być dopuszczone wyłącznie osoby posiadające specjalne upoważnienie, wydane przez Administratora danych osobowych.
Wzór upoważnienia określa załącznik nr 4.

2. Ewidencję osób upoważnionych do przetwarzania danych osobowych prowadzi Administrator bezpieczeństwa informacji.
Wzór rejestru określa załącznik nr 5.

3. Pracownik właściwy do spraw kadrowych jest zobowiązany do uzupełnienia zakresu obowiązków pracowników o odpowiedzialność za ochronę tych danych, zgodnie z przydzielonymi zadaniami.

4. Osoba dopuszczona do przetwarzania danych osobowych podpisuje oświadczenie, które dołącza się do jej akt osobowych.
Wzór oświadczenia określa załącznik nr 6.

§ 8. 1. Powołuje się Administratora systemów informatycznych w celu sprawowania nadzoru nad funkcjonowaniem systemów i programów informatycznych przetwarzających dane osobowe.

2. Obowiązki Administratora systemów informatycznych powierza się informatykowi zatrudnionemu w Urzędzie

3. Zakres obowiązków Administratora systemów informatycznych określa załącznik nr 7.

§ 9. 1. Integralną częścią powyższego zarządzenia jest:

a) Polityka Bezpieczeństwa dla Zbioru Podsystemu Monitorowania Europejskiego Funduszu Społecznego 2007 w Urzędzie Gminy w Sławnie,
b) Instrukcja Zarządzania Systemem Informatycznym dla Podsystemu Monitorowania Europejskiego Funduszu Społecznego 2007 w Urzędzie Gminy w Sławnie.

§ 10. Zobowiązuję wszystkich pracowników zajmujących się przetwarzaniem danych osobowych lub pracujących w systemach informatycznych do zapoznania się z treścią wytycznych określonych w załączniku Nr 1 i 2.

§ 11. Powyższe zasady mają zastosowanie do przetwarzania danych osobowych lub pracujących w systemach informatycznych w Gminnym Zespole Ekonomiczno-Administracyjnego Szkół w Sławnie ze względu na wspólny serwer bazy danych osobowych tj. dla Urzędu Gminy w Sławnie oraz Gminnego Zespołu Ekonomiczno-Administracyjnego Szkół w Sławnie.

§ 12. Zarządzenie wchodzi w życie z dniem podpisania.

WÓJT GMINY
mgr Tadeusz Wojciechowski

ZATWIERDZAM:

WÓJT GMINY
mgr Tadeusz Wojciechowski

Załącznik nr 1
do Zarządzenia Nr 3/11
Kierownika Urzędu –
Wójta Gminy Sławno
z dnia 1 lutego 2011

Polityka bezpieczeństwa przetwarzania danych osobowych

w Urzędzie Gminy w Sławnie

2011

SPIS TREŚCI

1. PODSTAWY OPRACOWANIA

1. Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych
   (t.j. Dz.U. z 2001 r. Nr 101, poz. 926 z późn. zm.)
2. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. 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),
3. Rozporządzenie Prezesa Rady ministrów z dnia 25 lutego 1999 roku w sprawie podstawowych wymagań bezpieczeństwa systemów i sieci teleinformatycznych
   (Dz. U. z 1999 r. Nr 18 poz.162)
4. Rozporządzenie Rady Ministrów z 11 października 2005 w sprawie minimalnych wymagań dla systemów teleinformatycznych
   (Dz. U. 2005r. (Dz. U. nr 212, poz. 1766)
5. Wytyczne GIODO w zakresie opracowania i wdrożenia polityki bezpieczeństwa.

2. TERMINOLOGIA

Ustawa – Ustawa z dnia 29 sierpnia 1997 r o ochronie danych osobowych

Urząd – Urząd Gminy

Administrator danych – Wójt Gminy Sławno

Administrator bezpieczeństwa – Administrator bezpieczeństwa informacji wyznaczony przez Wójta Gminy

Administrator systemu – Administrator systemu informatycznego

Użytkownicy systemu – osoby upoważnione do przetwarzania danych osobowych

System informatyczny – zespół współpracujących ze sobą lub pracujących autonomicznie urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych

Dane osobowe – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne

Zbiór danych osobowych – posiadający strukturę zestaw danych o charakterze osobowym

Przetwarzanie danych osobowych – jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie

Użytkownik - osoba posiadająca upoważnienie wydane przez administratora danych osobowych i dopuszczona do przetwarzania danych osobowych w zakresie wskazanym w upoważnieniu

Nazwa użytkownika – jednoznacznie przypisany jednej osobie identyfikator składający się z liter i cyfr, określający użytkownika w systemie informatycznym

Hasło – ciąg znaków, stanowiący tajemnicę użytkownika, w połączeniu z nazwą użytkownika umożliwiający uwierzytelnienie w systemie informatycznym

3. POLITYKA BEZPIECZEŃSTWA INFORMACJI – CELE REALIZACJI

Polityka bezpieczeństwa informacji to zespół ogólnych zasad i podstawowych wymagań określających, w jaki sposób są zarządzane, udostępniane i chronione przed nieupoważnionym wykorzystaniem zniszczeniem lub nieautoryzowanymi zmianami materialne i zapisane w postaci elektronicznej zbiory danych osobowych.

Polityka bezpieczeństwa informacji jest zbiorem zasad, określających metody ochrony oraz zapewnienia bezpieczeństwa informacji w Urzędzie Gminy, jest zbiorem spójnych, precyzyjnych i zgodnych z obowiązującym prawem przepisów, reguł i procedur, według których instytucja buduje, zarządza i udostępnia zasoby oraz systemy informacyjne i informatyczne.

W polityce bezpieczeństwa informacji zdefiniowano zasoby, które powinny być chronione, określono zasady ochrony grup informacji dotyczące sposobów ich przetwarzania i przechowywania z uwzględnieniem nie tylko zagadnień bezpieczeństwa i komunikacji przetwarzanych informacji, sprzętu i oprogramowania, za pomocą których są przetwarzane informacje, lecz również ludzi, którzy te informacje przetwarzają.

Celem działań w zakresie ochrony i zapewnienia bezpieczeństwa informacji w Urzędzie Gminy jest osiągnięcie takiego poziomu organizacyjnego i technicznego, który:

- zagwarantuje zachowanie poufności informacji chronionych;
- zapewni integralność informacji oraz dostępność do nich;
- zagwarantuje wymagany poziom bezpieczeństwa przetwarzanych informacji;
- maksymalnie ograniczy występowanie zagrożeń dla bezpieczeństwa informacji;
- zapewni poprawne i bezpieczne funkcjonowanie systemów przetwarzania informacji;
- zapewni gotowość do podejmowania działań w sytuacjach kryzysowych.

Te nadrzędne cele realizowane są poprzez:

1. Kształtowanie kultury bezpieczeństwa, promującej świadomość i postawy ukierunkowane na wykrywanie, ujawnianie i eliminację zagrożeń.
2. Wdrażanie spójnej, pro aktywnej i formalnie wyodrębnionej polityki zarządzania bezpieczeństwem, opartej na zaangażowaniu wszystkich pracowników oraz na odpowiednich narzędziach organizacyjnych i ciągłym monitoringu poziomu bezpieczeństwa.
3. Precyzyjne określenie zakresów kompetencji i odpowiedzialności pracowników oraz osób funkcyjnych w zakresie bezpieczeństwa.
4. Zapewnienie systemu szkoleń zmierzający do podnoszenia kwalifikacji i świadomości bezpieczeństwa wśród wszystkich pracowników.
5. Wydzielanie zasobów odpowiednich dla realizacji przedsięwzięć mających na celu podnoszenie poziomu bezpieczeństwa.

Utrzymanie bezpieczeństwa przetwarzanych przez Urząd Gminy informacji rozumiane jest jako zapewnienie ich poufności, integralności i dostępności na odpowiednim poziomie. Miarą bezpieczeństwa jest wielkość ryzyka związanego z zasobem stanowiącym przedmiot Polityki bezpieczeństwa informacji.

Pojęcia użyte powyżej w odniesieniu do informacji i aplikacji oznaczają:

1. poufność informacji – właściwość zapewniająca, że informacja nie jest udostępniana lub ujawniana nieautoryzowanym osobom, podmiotom lub procesom
2. integralność danych – właściwość zapewniająca, że dane nie zostały zmienione bądź zniszczone w sposób nieautoryzowany,
3. dostępność informacji – właściwość bycia dostępnym i możliwym do wykorzystania na żądanie w założonym czasie przez kogoś lub coś, kto/co m do tego prawo
4. autentyczność – właściwość zapewniająca, że tożsamość podmiotu lub zasobu jest taka, jak deklarowana, dotyczy użytkowników, procesów, systemów lub nawet instytucji, autentyczność związana jest z badaniem czy ktoś lub coś jest tym /czym za kogo/co się podaje,

5. integralność systemu – właściwość polegająca na tym, że system realizuje swoją zamierzoną funkcję w nienaruszony sposób, wolny od nieautoryzowanej manipulacji, celowej bądź przypadkowej,
6. rozliczność – właściwość zapewniająca, ze działania podmiotu (np. użytkownika) mogą być jednoznacznie przypisane temu podmiotowi,
7. niezawodność – właściwość oznaczająca spójne, zamierzone działanie, zachowanie i skutki
8. zarządzanie ryzykiem – proces identyfikowania, kontrolowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa.

4. INTENCJE KIEROWNICTWA

Kierownictwo Urzędu Gminy w Sławnie świadome wagi problemów związanych z ochroną prawa do prywatności, w tym w szczególności prawa osób fizycznych, których dane osobowe przetwarzane są w Urzędzie, dla właściwej i skutecznej ochrony tych danych deklaruje:

1. Podejmowanie wszystkich działań niezbędnych dla ochrony praw i usprawiedliwionych interesów jednostki związanych z bezpieczeństwem danych osobowych.

2. Stałe podnoszenie świadomości oraz kwalifikacji osób przetwarzających dane osobowe w Urzędzie w zakresie problematyki bezpieczeństwa tych danych.

3. Traktowanie obowiązków osób zatrudnionych przy przetwarzaniu danych osobowych jako należących do kategorii podstawowych obowiązków pracowniczych oraz stanowczego egzekwowania ich wykonania przez zatrudnione osoby.

4. Zamiar podejmowania w niezbędnym zakresie współpracy z instytucjami powołanymi do ochrony danych osobowych.

Kierownictwo świadome jest zagrożeń związanych z przetwarzaniem przez Urząd Gminy danych osobowych – w tym, w szczególności, zagrożeń wynikających z dynamicznego rozwoju metod i technik przetwarzania tych danych w systemach informatycznych oraz sieciach telekomunikacyjnych.

Jednoczesnym zamiarem jest doskonalenie i rozwijanie nowoczesnych metod przetwarzania danych, przy założeniu, że będą stale doskonalone i rozwijane organizacyjne, techniczne oraz informatyczne środki ochrony danych osobowych przetwarzanych zarówno metodami tradycyjnymi jak i elektronicznie tak, aby skutecznie zapobiegać zagrożeniom.

5. OBOWIĄZKI I ODPOWIEDZIALNOŚĆ

1. Realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych wyznaczono osoby odpowiedzialne za bieżącą realizacje tej polityki na terenie Urzędu Gminy. W szczególności wyznaczeni zostali:

    - Administrator bezpieczeństwa informacji
    - Administrator systemów informatycznych

2. Zakresy zadań i odpowiedzialności ww. osób określone zostały w Zarządzeniu nr 3/11 Kierownika Urzędu - Wójta Gminy Sławno z dnia 1 lutego 2011r. w sprawie wprowadzenia zasad ochrony danych osobowych przetwarzanych w Urzędzie Gminy w Sławnie.

3. Do przetwarzania danych w systemie informatycznym i tradycyjnym dopuszcza się wyłącznie osoby posiadające upoważnienie nadane przez Administratora bezpieczeństwa.

4. Zapewnia się kontrolę nad dostępem do zbiorów danych osobowych. Kontrola ta w szczególności realizowana jest poprzez ewidencjonowanie osób przetwarzających dane osobowe oraz wdrożenie procedur udzielania dostępu do tych danych.

5. Administrator bezpieczeństwa przeprowadza kontrole oraz dokonuje ocen stanu bezpieczeństwa danych osobowych.

6. Osoby upoważnione do dostępu i przetwarzania danych osobowych zostały zaznajomione z powszechnie obowiązującymi przepisami prawa, uregulowaniami wewnętrznymi, a także technikami i środkami ochrony tych danych stosowanymi w Urzędzie.

7. Każdy pracownik biorący udział w przetwarzaniu danych osobowych jest odpowiedzialny za bezpieczeństwo tych danych.

5.1 ODPOWIEDZIALNOŚĆ ZA NARUSZENIE USTAWY

Naruszenia ustawy o ochronie danych osobowych zagrożone jest odpowiedzialnością administracyjną, cywilna oraz karną.

Postępowanie administracyjne toczy się przed GIODO, który może wydać decyzje nakazującą przywrócenie stanu zgodnego z przepisami ustawy, usunięcie uchybień, uaktualnienie, uzupełnienie, udostępnienie danych, usunięcie.

Postępowanie cywilne może być prowadzone niezależnie od administracyjnego. Następuje w sytuacji wszczęcia go przez osobę, której dane zostały naruszone. Podstawą roszczeń z tego tytułu jest art. 23 – 24 Kodeksu Cywilnego. Na podstawie powołanych przepisów osoba poszkodowana może żądać nie tylko zaniechania i usunięcia skutków naruszenia ale także zadośćuczynienia pieniężnego za doznaną krzywdę. W przypadku gdy wskutek naruszenia ustawy ucierpią interesy majątkowe odpowiedzialność wobec sprawcy może być egzekwowana na podstawowe art. 415 kodeku cywilnego.

Niezależnie od powyższego za naruszenie bezpieczeństwa danych osobowych następuje odpowiedzialność karna, o której mowa w art. 49 i art.52 Ustawy.

Art. 49

Kto przetwarza w zbiorze dane osobowe, choć ich przetwarzanie nie jest dopuszczalne, albo do których przetwarzania nie jest uprawniony, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

Art 52:

Kto administrując danymi narusza choćby nieumyślnie obowiązek zabezpieczenia ich przed zabraniem przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

W Urzędzie Gminy naruszanie przez osoby upoważnione do dostępu i przetwarzania danych osobowych, zasad bezpiecznego i zgodnego z prawem ich przetwarzania, traktowane będzie jako naruszenie podstawowych obowiązków pracowniczych z wszystkimi wynikającymi stąd konsekwencjami.

Każdy pracownik, który powezmie informację bądź podejrzenie o możliwości naruszenia bezpieczeństwa danych osobowych przetwarzanych w Urzędzie Gminy jest zobowiązany do natychmiastowego poinformowania o powyższym Administratora bezpieczeństwa.

6. NARUSZENIE BEZPIECZEŃSTWA DANYCH

Naruszenie ochrony danych osobowych może być skutkiem różnych czynników w tym:

- szkodliwego wpływu środowiska na system przetwarzania danych osobowych,
- zewnętrznych zdarzeń losowych dotyczących systemu przetwarzania danych osobowych,
- zamierzonych lub niezamierzonych czynności użytkowników dopuszczonych do przetwarzania danych osobowych,
- nieuprawnionych działań osób nieupoważnionych do dostępu do danych osobowych.

O naruszeniu ochrony danych osobowych mogą świadczyć min. następujące symptomy:

- ślady włamania lub prób włamania do obszaru, w którym przetwarzane są dane osobowe,
- ślady włamania lub prób włamania do pomieszczeń, w których odbywa się przetwarzanie danych osobowych, w szczególności do serwerowni oraz do pomieszczeń, w których przechowywane są nośniki kopii zapasowych,
- włamanie lub próby włamania do szaf i biurek, w których przechowywane są – w postaci elektronicznej lub papierowej – nośniki danych osobowych,
- zagubienie bądź kradzież nośnika danych osobowych,
- zagubienie bądź kradzież nośnika materiału kryptograficznego (karty mikroprocesorowej, pamięci typu flash itp.),
- kradzież sprzętu informatycznego, w którym przechowywane są dane osobowe,
- fizyczne zniszczenie lub podejrzenie zniszczenia elementów systemu informatycznego przetwarzającego dane osobowe na skutek przypadkowych lub celowych działań albo zaistnienia działania siły wyższej,

W stosunku do danych przetwarzanych w aplikacjach komputerowych mogą być to ponadto:

- brak możliwości uruchomienia przez użytkownika aplikacji pozwalającej na dostęp do danych osobowych,
- brak możliwości zalogowania się do tej aplikacji,
- ograniczone, w stosunku do normalnej sytuacji, uprawnienia użytkownika w aplikacji (na przykład brak możliwości wykonania pewnych operacji normalnie dostępnych użytkownikowi) lub uprawnienia poszerzone w stosunku do normalnej sytuacji,
- wygląd aplikacji inny niż normalnie,
- inny zakres danych niż normalnie dostępny dla użytkownika – dużo więcej lub dużo mniej danych,
- znaczne spowolnienie działania systemu informatycznego,
- pojawienie się niestandardowych komunikatów generowanych przez system informatyczny,
- informacja z systemu antywirusowego o zainfekowaniu systemu informatycznego wirusami,
- podejrzenie nieautoryzowanej modyfikacji danych osobowych przetwarzanych w systemie informatycznym.

6.1. PROCEDURA POSTĘPOWANIA

Po otrzymaniu zgłoszenia o podejrzeniu bądź stwierdzeniu zaistnienia naruszenia bezpieczeństwa danych osobowych Administrator bezpieczeństwa, we współpracy z Administratorem systemu, jest zobowiązany do podjęcia kroków w celu:

1. Wyjaśnienia zdarzenia, a w szczególności czy miało miejsce naruszenie ochrony danych osobowych.
2. Wyjaśnienia przyczyn naruszenia bezpieczeństwa danych osobowych i zebrania ewentualnych dowodów, w szczególności, gdy zdarzenie było związane z celowym działaniem pracownika bądź osób trzecich.
3. Rozważenia konieczności natychmiastowej wymiany technicznych środków zabezpieczeń.

Jeżeli naruszenie dotyczy zbiorów danych w postaci elektronicznej Administrator bezpieczeństwa we współpracy z Administratorem systemu podejmują dodatkowe działania zmierzające do:

1. Zabezpieczenia systemu informatycznego przed dalszym rozprzestrzenianiem się zagrożenia.
2. Zabezpieczenia danych przetwarzanych w systemie informatycznym, w szczególności danych konfiguracyjnych tego systemu.
3. Przeprowadzenia analizy danych osobowych przetwarzanych w systemie informatycznym.
4. Przeprowadzenia analizy poprawności funkcjonowania systemu informatycznego.
5. Usunięcia skutków incydentu i przywróceniu pierwotnego stanu systemu informatycznego (to jest stanu sprzed incydentu).
6. Wprowadzenia zmian w dostępie do zbioru danych zgromadzonych w komputerze.

Administrator bezpieczeństwa określa na podstawie zebranych informacji przyczyny i skutki zaistniałego incydentu. Jeżeli incydent był spowodowany działaniem celowym, jest zobowiązany do powiadomienia Administratora danych, który zgłasza ten fakt organom ścigania, oraz:

1. Nakazuje zabezpieczenie miejsca ewentualnego przestępstwa do czasu dokonania ustaleń przez organy ścigania.
2. Sporządza natychmiast komisyjny, szczegółowy protokół ze stanu faktycznego naruszenia bezpieczeństwa, w którym ustala ewentualne osoby odpowiedzialne za zaistnienie zdarzenia.
3. Inwentaryzuje stan zbiorów danych, w celu ustalenia faktycznego zakresu naruszenia bezpieczeństwa danych.

System informatyczny, którego prawidłowe działanie zostało odtworzone powinien zostać poddany szczegółowej obserwacji w celu stwierdzenia całkowitego usunięcia symptomów incydentu.

Administrator bezpieczeństwa prowadzi ewidencję interwencji związanych z zaistniałymi incydentami w zakresie bezpieczeństwa danych osobowych.

Ewidencja taka obejmuje następujące informacje:

- imię i nazwisko osoby zgłaszającej incydent,
- imię i nazwisko osoby przyjmującej zgłoszenie incydentu,
- datę zgłoszenia incydentu,
- przeprowadzone działania wyjaśniające przyczyny zaistnienia incydentu,
- wyniki przeprowadzonych działań,
- podjęte akcje naprawcze i ich skuteczność.

Administrator bezpieczeństwa informacji odpowiedzialny jest za przeprowadzenie przynajmniej raz w roku analizy zaistniałych incydentów w celu:

- określenia skuteczności podejmowanych działań wyjaśniających i naprawczych,
- określenie wymaganych działań zwiększających bezpieczeństwo systemu informatycznego i minimalizujących ryzyko zaistnienia incydentów,
- określenie potrzeb w zakresie szkoleń Administratora systemu i użytkowników systemu informatycznego przetwarzającego dane osobowe.

7. WYKAZ BUDYNKÓW I POMIESZCZEŃ TWORZĄCYCH OBSZAR, W KTÓRYM PRZETWARZANE SĄ DANE OSOBOWE

Wykaz budynków, w których przetwarzane są dane osobowe:

Budynek Urzędu Gminy w Sławnie zlokalizowany przy
ul. Marszałka Józefa Piłsudskiego 31

Wykaz pomieszczeń:

W budynku zajmowanym przez Urząd Gminy pomieszczenia:

1. na parterze pomieszczenia Urzędu Stanu Cywilnego-Referatu Spraw Obywatelskich, pomieszczenia Gminnego Zespołu Ekonomiczno-Administracyjnego Szkół
2. na II piętrze pomieszczenia oznaczone numerami: 2, 3, 4, 5, 7, 8, 11, 16 i Sekretariat
3. w północnej części budynku na parterze pomieszczania Referatu Ochrony Środowiska i Rolnictwa

8. WYKAZ ZBIORÓW DANYCH OSOBOWYCH

Wykaz zbiorów danych osobowych przetwarzanych w Urzędzie wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych stanowi Załącznik nr 1 do niniejszej Polityki bezpieczeństwa.

9. OPIS STRUKTURY ZBIORÓW DANYCH

Opis struktury zbiorów danych stanowi Załącznik nr 2 do niniejszej Polityki bezpieczeństwa.

10. POGRAMY WYKORZYSTYWANE DO PRZETWARZANIA DANYCH OSOBOWYCH

Lp.	Nazwa programu	Producent	Miejsce dostępu
1.	ZUS Płatnik	Asseco Poland S.A.	pokój nr 3, 4
2.	Program płacowo-kadrowo,	INFO SYSTEM	pokój nr 2, 3, 4
3.	Program księgowo-podatkowy	INFO SYSTEM	pokój nr 3, 16
4.	Program „Woda"	INFO SYSTEM	Referat Ochrony Środowiska i Rolnictwa
5.	EGB	GEOBAZA Sp.z o.o.	pokój nr 11 pokój nr 16
6.	Selwin	Q100 Computers	Urząd Stanu Cywilnego
7.	USC WIN	Q100 Computers	Urząd Stanu Cywilnego
8.	System Informacji Oświatowej	MEN	pokój nr 8
9.	Podsystem monitorowania EFS 2007	Microsoft	pokój nr 4

11. STRUKTURA ZBIORÓW, SPOSÓB PRZEPŁYWU DANYCH POMIĘDZY ZBIORAMI

Część zbiorów przetwarzanych w Urzędzie posiada strukturę złożoną. Zbiór główny składa się kilku podzbiorów. Ich strukturę oraz przepływ danych pomiędzy zbiorami ilustrują zamieszczone poniżej diagramy.

Zbiór „Dowody osobiste" składa się z dwóch podzbiorów

Zbiór „Rejestr mieszkańców, realizacja obowiązku meldunkowego" składa się z sześciu podzbiorów

Zbiór „Księgi stanu cywilnego" składa się z trzech podzbiorów

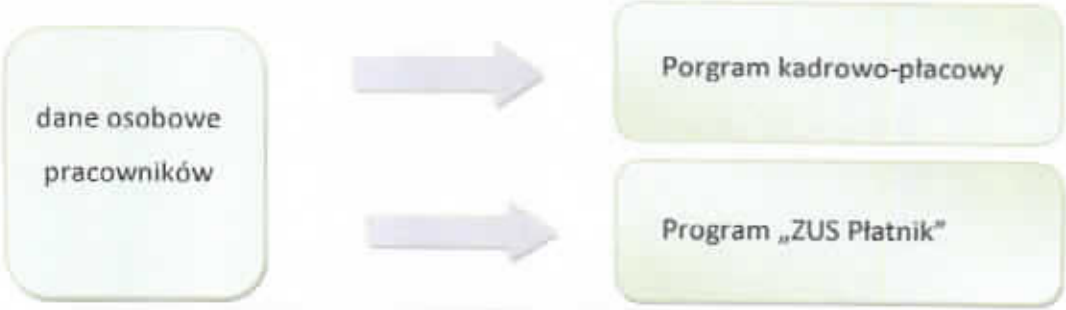
Zbiór „Pobór, kwalifikacja wojskowa" składa się z pięciu podzbiorów

Zbiór „Formacje OC" składa się z dwóch podzbiorów

Zbiór „Podatki i opłaty lokalne" składa się z pięciu podzbiorów

Zbiór „Zwrot podatku od oleju napędowego" składa się z dwóch podzbiorów

Przepływ danych pomiędzy zbiorami: dane ze zbioru dane osobowe pracowników przekazywane są do programów Kadrowo-płacowego i ZUS Płatnik



12. ŚRODKI NIEZBĘDNE DLA ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZY PRZETWARZANIU DANYCH

12.1. OKREŚLENIE POZIOMU BEZPIECZEŃSTWA PRZETWARZANIA DANYCH

Dane osobowe przetwarzane w Urzędzie Gminy w Sławnie w systemach informatycznych winny mieć zagwarantowany wysoki poziom bezpieczeństwa w rozumieniu § 6 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

Powyższe wynika z faktu połączenia komputerów wykorzystywanych do przetwarzania danych osobowych z publiczną siecią informatyczną Internet

12.2. ŚRODKI TECHNICZNE

Antywłamaniowe zabezpieczenie budynków

1. Po godzinach pracy wejście do budynku Urzędu Gminy jest skutecznie zabezpieczone przed dostaniem się osób postronnych. Powyższe jest realizowane poprzez zamykanie drzwi wejściowych dwoma zamkami patentowymi.
2. Zastosowano podwójne drzwi zewnętrzne.
3. Budynek wyposażony jest w systemy alarmowy przeciwwłamaniowy.

Zabezpieczenie pomieszczeń i dokumentacji

1. Każde z pomieszczeń, w których przetwarzane są dane osobowe posiada drzwi zamykane, na co najmniej jeden zamek patentowy.
2. Okna pomieszczeń zlokalizowanych na parterze zabezpieczone są metalowymi kratami.
3. Zbiory danych w postaci dokumentów papierowych w teczkach, zeszytów, ksiąg, kartotek itp. po zakończeniu pracy odbywa się w szafach i biurkach zamykanych na zamki.

12.3. Środki organizacyjne

1. W Urzędzie wyznaczono Administratora bezpieczeństwa informacji, który wnioskuje o przyznanie uprawnień do przetwarzania danych osobowych w formie pisemnego upoważnienia przez Administratora danych.
2. Osoby upoważnione do przetwarzania danych osobowych, przed dopuszczeniem do pracy z tymi danymi, szkoli się w zakresie obwiązujących przepisów o ochronie danych osobowych, procedur przetwarzania danych oraz informuje o podstawowych zagrożeniach związanych z przetwarzaniem danych w systemie informatycznym.
3. Prowadzona jest ewidencja osób upoważnionych do przetwarzaniu danych osobowych.
4. Wprowadzono Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.
5. Zdefiniowano procedury postępowania w sytuacji naruszenia ochrony danych osobowych.
6. Określono sposób postępowania z nośnikami informacji.
7. Osoby, o których mowa w pkt. 2 zostały przeszkolone, w zakresie bezpiecznej obsługi urządzeń i programów związanych z przetwarzaniem i ochroną danych osobowych.
8. Przebywanie osób trzecich w pomieszczeniach, gdzie przetwarzane są dane osobowe dopuszczalne jest tylko w obecności osoby upoważnionej do przetwarzania tych danych lub za zgodą Administratora danych.
9. Pomieszczenia, o których mowa w pkt.8 zamykane są na czas nieobecności osoby zatrudnionej przy przetwarzaniu danych, w sposób uniemożliwiający dostęp do nich osób trzecich.
10. W przypadku przebywania osób trzecich w pomieszczeniach, o których mowa wyżej, monitory stanowisk komputerowych, na których przetwarzane są dane osobowe ustawione w taki sposób, aby uniemożliwiać tym osobom wgląd w dane.

11. Urządzenia przetwarzające dane zostały umieszczone w taki sposób, by zminimalizować niepożądany dostęp do obszarów roboczych oraz ograniczyć do minimum brak nadzoru podczas ich używania.
12. Po zakończonej pracy nośniki danych zabezpiecza się w zamykanych szafach.
13. Każdorazowe odejście od komputerowego stanowiska pracy zostaje poprzedzone zablokowaniem klawiatury i włączeniem wygaszacza ekranu zabezpieczonego hasłem.
14. Na zakończenie pracy aktywne sesje są zamykane.
15. Do faksów, kserokopiarek i drukarek nie mają dostępu osoby postronne. Jeśli jest to możliwe, urządzenia te są zablokowane poza normalnymi godzinami pracy. Niezwłocznie po skopiowaniu lub wydrukowaniu dokumentów są one zabierane z podajnika urządzenia.
16. Z wszelkich nośników wielokrotnego użytku, które mają być wyniesione z Urzędu, wymazania jest poprzedniej zawartości, o ile nie będzie już potrzebna.
17. Klucze do szaf i biurek, w których przechowywane są dokumenty z danymi osobowymi posiadają tylko osoby upoważnione do przetwarzania danych osobowych; komplety kluczy zapasowych przechowywany jest w bezpieczny sposób przez Administratora bezpieczeństwa informacji,
18. Zabrania się przechowywania kluczy w sposób umożliwiający dostęp do nich osób nieuprawnionych.
19. Każdy dokument papierowy zawierający dane osobowe, który jest przeznaczony do wyrzucenia jest uprzednio niszczony w sposób uniemożliwiający jego odczytanie (przy pomocy niszczarki dokumentów).

12.4. Zabezpieczenie KOMPUTERÓW

1. Komputery posiadają zasilacze awaryjne zabezpieczające je przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci elektrycznej.
2. Poczta elektroniczna wpływającą do Urzędu skanowana jest programem antywirusowym podczas odbioru z serwera pocztowego.
3. Komputery połączone są z publiczną siecią Internet za pośrednictwa serwera, który posiada zabezpieczenia przed nieuprawnionym dostępem z zewnątrz.
4. Zdefiniowano użytkowników i ich prawa dostępu do danych osobowych na poziomie aplikacji (unikalny identyfikator i hasło).
5. Komputery, z których możliwy jest dostęp do danych osobowych zabezpieczone są hasłem uruchomieniowym.
6. Na poziomie aplikacji służącej do przetwarzania danych osobowych, do której dostęp mają co najmniej dwie osoby winny zastosowano: identyfikator i hasło dostępu dla każdego upoważnionego pracownika
7. System informatyczny zapewnia rejestrację dostępu do aplikacji w których przetwarzane są dane osobowe przez poszczególnych użytkowników.

12.5. ZABEZPIECZENIE ZBIORÓW DANYCH OSOBOWYCH PRZED SZKODLIWYM WPŁYWEM ZEWNĘTRZNYCH CZYNNIKÓW ŚRODOWISKOWYCH

Fizyczna ochrona danych osobowych powinna przeciwdziałać zagrożeniu nieupoważnionego dostępu do informacji, ale również niebezpiecznym czynnikom środowiskowym, które mogłyby wpłynąć na działanie urządzeń przetwarzających dane osobowe, a także na ich uszkodzenie bądź zniszczenie.

Podczas normalnego funkcjonowania w budynku Urzędu nie występują czynniki środowiskowe mogące w destrukcyjny sposób wpływać na przetwarzane i przechowywane zbiory danych osobowych. Nie mniej jednak należy założyć wystąpienie sytuacji szczególnych, kiedy w wyniku nietypowych, czy nadzwyczajnych zdarzeń takich jak poważne awarie infrastruktury technicznej budynku, naruszenie konstrukcji budynku, powstanie pożaru czy wreszcie celowe działanie o charakterze terrorystycznym wystąpią szkodliwe czynniki środowiskowe o znacznym nasileniu, które w efekcie będą miały negatywny wpływ na zbiory danych osobowych.

Podstawowe kategorie takich zagrożeń środowiskowych, to:

- pożar
- zalanie w wyniku awarii wewnętrznej instalacji wod-kan. czy CO
- pył, dym, kurz
- interferencje ze źródeł zasilania, promieniowanie elektromagnetyczne
- naruszenie konstrukcji, zerwanie, zawalenie dachu budynku w wystąpienia silnych wiatrów czy obfitych opadów śniegu

Najgroźniejszym zdarzeniem z punktu widzenia rozmiaru powodowanych szkód i zniszczeń pozostaje pożar. Wynika to min. z faktu, że posiada on dużą zdolność do gwałtownego niekontrolowanego rozprzestrzeniania się w środowisku, gdzie występuje duże nagromadzenie materiałów palnych, jak to ma miejsce w pomieszczeniach biurowych. Towarzyszące mu takie szkodliwe czynniki jak wysoka temperatura, oraz występowanie w jego atmosferze dużych ilości dymu

i gazów pożarowych często agresywnie oddziałujących na otoczenie, mogą spowodować całkowite zniszczenie wyposażenia pomieszczeń, a w konsekwencji również przechowywanych w nich dokumentacji i urządzeń komputerowych. Konsekwencją wystąpienia pożaru jest prowadzenie akcji ratowniczo-gaśniczej, która powoduje kolejne szkody w otoczeniu. W sytuacji, gdy pożar osiągnie znaczne rozmiary koniecznym staje się używanie jako środka gaśniczego wody, która częściowo odparowuje, jednak w większości pozostaje na podłożu oraz przedostaje się na niższe kondygnacje powodując zalania pomieszczeń tam zlokalizowanych.

W budynku występują instalacje użytkowe, w których przesyłana jest pod ciśnieniem woda. Jest to instalacja wodna oraz instalacja centralnego ogrzewania. Są one również potencjalnymi źródłami mogącymi spowodować szkody w dokumentacji papierowej oraz zalania i awarie komputerów. Nawet niezbyt duże rozszczelnienia w sieci bądź armaturze spowodowane np. ich korozją, a powstałe w porze nocnej lub w dni wolne od pracy i w porę niezauważone mogą powodować wydostanie się znacznych ilości wody oraz zalania zarówno pomieszczeń, w którym wystąpiły jak i sąsiednich czy zlokalizowanych na niższych kondygnacjach.

Następnym potencjalnym zagrożeniem dla budynku jest naruszenie jego konstrukcji, zerwanie, zawalenie dachu budynku w wystąpienia silnych wiatrów czy obfitych opadów śniegu. Jak pokazały przykłady z ubiegłych lat takie anomalia pogodowe mogą coraz częściej występować w naszym klimacie. Mimo, iż budynki projektowane są przy założeniu konieczności przenoszenia takich obciążeń to w ekstremalnych przypadkach ich wytrzymałość i nośność okazują się zbyt małe. Dochodzi wówczas do naruszenia konstrukcji dachu, ale często również ścian nośnych. Zerwanie czy załamanie się dachu do wnętrza budynku powoduje znaczne zniszczenie pomieszczeń znajdujących się na najwyższej kondygnacji.

Urządzenia komputerowe wykorzystywane do administrowania danymi wrażliwe są na niektóre czynniki środowiskowe mogące powodować ich uszkodzenia, bądź utratę zgromadzonych danych. W jednostkach centralnych komputerów w procesie ich eksploatacji gromadzą się znaczne ilości kurzu i pyłów. Osiadają one min. na radiatorach i wentylatorach zapewniających właściwe odprowadzanie ciepła

z nagrzewających się w czasie pracy mikroprocesorów. Tym samym zaburzają odpowiednie chłodzenie, powodując ich przegrzewanie i awarie. Podobnie w wyniku niedostatecznego odprowadzania ciepła uszkodzeniom ulegać mogą dyski twarde.

Urządzenia komputerowe wrażliwe są również na interferencje i przepięcia pochodzące ze źródeł zasilania. Na magnetyczne nośniki danych w destrukcyjny sposób działają pola elektromagnetyczne.

W większości przypadków dokumenty z danymi osobowymi przechowywane są w typowych szafach biurowych wykonanych z okleinowanej płyty wiórowej. Szafy tego typu nie stanowią dostatecznego zabezpieczenia przed działaniem zewnętrznych czynników środowiskowych o destrukcyjnych charakterze, wobec czego przechowywane w nich dokumenty narażone są na zniszczenie bądź uszkodzenie.

Komputery służące do przechowywania danych osobowych również zagrożone są utratą danych wskutek oddziaływania takich czynników. W przypadku, gdy są one ustawione na podłodze pomieszczeń pojawienie się na niej wody spowoduje ich zalanie i uszkodzenie.

W stosunku do danych gromadzonych w postaci dokumentacji papierowej przyjęto zasady:

- szafy z danymi lokalizować w pomieszczeniach w jak największej możliwej odległości od instalacji wodnej i CO,
- nie przechowywania dokumentów na najniższych półkach szaf, a co najmniej na półkach znajdujących się 0,2 m nad poziomem podłogi,
- umieszczenia duplikatów kluczy do szaf w miejscu skąd mogą zostać użyte w razie potrzeby.

W stosunku do urządzeń komputerowych przyjęto zasady:

- jednostek centralnych komputerów nie umieszczać bezpośrednio na podłodze, a na półkach biurek lub innych podwyższeniach,
- lokalizowania w pomieszczeniach stanowisk pracy z komputerami w maksymalnie największej odległości od instalacji wodociągowej i CO,
- zlokalizowania serwerów w wydzielonym pomieszczeniu posiadającym podwyższoną odporność pożarową i na włamanie oraz zapewniającym urządzeniom odpowiedni komfort pracy.
- Zabezpieczenia serwerów i komputerów urządzeniami „UPS"
- Wydzielenia oddzielnego obwodu elektrycznego do przeznaczonego wyłącznie do zasilania wszystkich komputerów.

W przypadku wystąpienia sytuacji kryzysowej, tj. zaistnienia zdarzenia, któremu towarzyszą szkodliwe czynniki środowiskowe mogące destrukcyjnie wpłynąć na zbiory danych osobowych należy przystąpić do ich fizycznej ewakuacji.

Pod tym pojęciem należy rozumieć wszelkie działania prowadzone zarówno przez pracowników jak ich służby ratownicze, polegające na fizycznym przemieszczeniu nośników danych z miejsca ich dotychczasowego przechowywania do miejsca gdzie mogą być czasowo bezpiecznie przechowane. Tym docelowym miejscem mogą być inne pomieszczenia w budynku niezagrożone w konkretnym zdarzeniu i posiadające odpowiednie zabezpieczenia, a w przypadku dużej skali zdarzenia nośniki danych należy ewakuować do innych bezpiecznych budynków.

Prowadzenie ewakuacji, aby odbywało się sprawnie, musi być właściwie przygotowane tym bardziej, że będzie realizowane często w warunkach zagrożenia.

Na powyższe składają się takie czynniki jak:

- opracowanie systemu uruchamiania ewakuacji
- przeszkolenie pracowników w zakresie prowadzenia ewakuacji
- przydział konkretnych zadań
- wyposażenie w niezbędny sprzęt ewakuacyjny

System uruchamiania ewakuacji obejmuje wykrycie i zlokalizowanie zagrożenia wraz z określeniem jego skali. Przekazanie informacji do osoby upoważnionej do zarządzenia ewakuacji, a następnie rozgłoszenie komunikatu o jej rozpoczęciu z podaniem docelowego miejsca przemieszczenia ewakuowanego mienia.

Pracownicy zostali przeszkoleni w zakresie sposobów postępowania w przypadku zaistnienia sytuacji nadzwyczajnych, w tym w szczególności ze sposobami i środkami prowadzenia ewakuacji mienia, ze szczególnym uwzględnieniem zbiorów danych osobowych, jako informacji szczególnie chronionych.

Poszczególnym pracownikom, w tym w pierwszej kolejności zatrudnionym w komórkach organizacyjnych przetwarzających dane osobowe przydzielono konkretne zadania do realizacji.

Kolejność podejmowanych czynności w przypadku powstania zagrożenia w godzinach pracy Urzędu:

1. Osoba, która pierwsza zauważyła zdarzenie natychmiast powiadamia bezpośredniego przełożonego i osoby z kierownictwa Urzędu.
2. Do czasu zapoznania się ze zdarzeniem przez osobę z kierownictwa, kompetentną do podejmowania decyzji o dalszym sposobie postępowania, pracownicy w marę możliwości podejmują czynności zmierzające do zatrzymania rozwoju zagrożenia i ograniczenia jego skutków.
3. Przybyła na miejsce zdarzenia osoba z kierownictwa Urzędu ocenia jego rozmiar i podejmuje decyzję w zakresie konieczności wezwania na pomoc służb interwencyjnych oraz polecenia pracownikom wykonywania niezbędnych czynności w tym ograniczenia rozwoju zagrożenia, zabezpieczenia mienia, ewakuacji mienia.

4. W przypadku przystąpienia do ewakuacji mienia należy doraźnie wyznaczyć docelowe miejsce gromadzenia ewakuowanej dokumentacji.

W przypadku konieczności prowadzenia ewakuacji po godzinach pracy Urzędu przybyła na miejsce osoba z kierownictwa Urzędu udostępnia w razie potrzeby kierującemu akcją ratowniczą dostęp do kopii zbiorów danych osobowych, wskazuje lokalizację dokumentacji z danymi osobowymi zgromadzonymi w formie papierowej. Zabezpiecza następnie ewakuowane dokumenty.

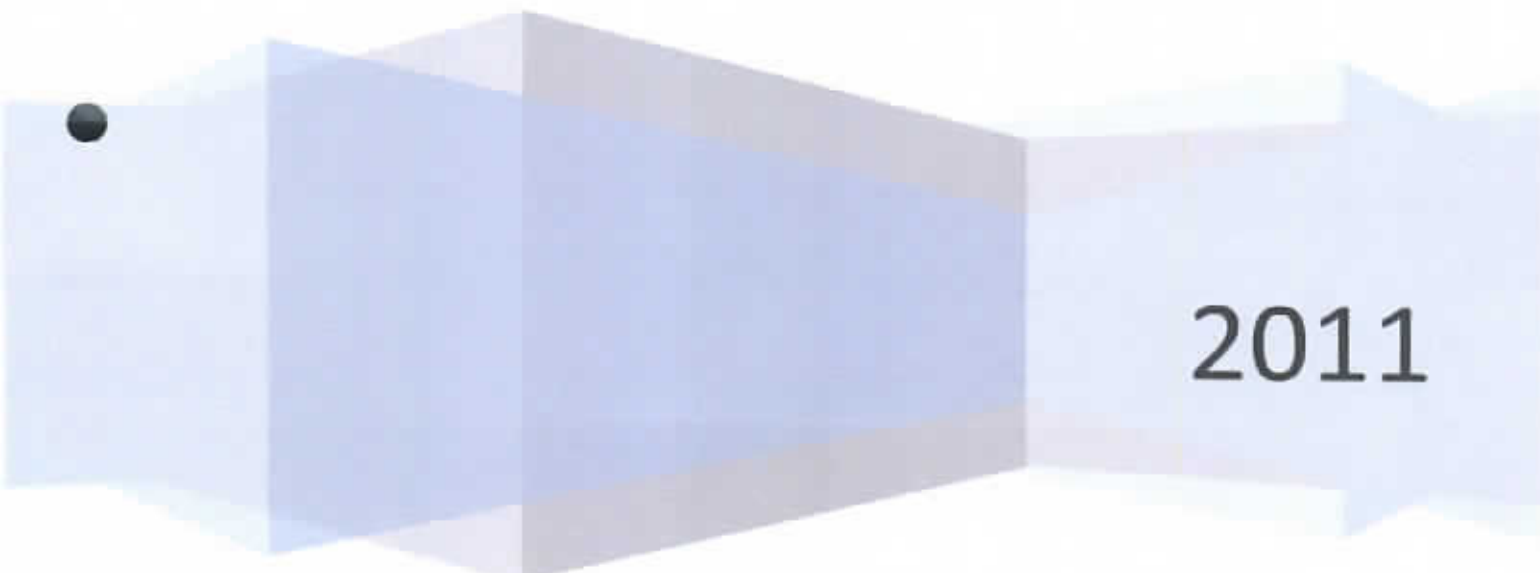
ZATWIERDZAM:

WÓJT GMINY
mgr Tadeusz Wojciechowski

Załącznik nr 2
do Zarządzenia Nr 3/11
Kierownika Urzędu –
Wójta Gminy Sławno
z dnia 1 lutego 2011

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych

w Urzędzie Gminy w Sławnie



2011

Spis treści

1. TERMINOLOGIA

Zbiór danych osobowych - każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.

Administrator danych osobowych – Wójt Gminy

Administrator bezpieczeństwa informacji –osoba wyznaczona przez Administratora danych osobowych, odpowiedzialna za bezpieczeństwo danych osobowych przetwarzanych w Urzędzie Gminy

Administrator systemów informatycznych - osoba odpowiedzialna za sprawność, konserwację oraz wdrażanie technicznych zabezpieczeń systemu informatycznego do przetwarzania danych osobowych w Urzędzie Gminy

System informatyczny - zespół współpracujących ze sobą lub pracujących autonomicznie urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

Stacja robocza – stacjonarny lub przenośny komputer wchodzący w skład systemu informatycznego umożliwiający użytkownikom systemu dostęp do danych osobowych znajdujących się w systemie.

Bezpieczeństwo systemu informatycznego - wdrożenie przez administratora danych osobowych lub osobę przez niego uprawnioną środków organizacyjnych i technicznych w celu zabezpieczenia oraz ochrony danych przed dostępem, modyfikacją, ujawnieniem, pozyskaniem lub zniszczeniem.

Przetwarzanie danych osobowych - wykonywanie jakichkolwiek operacji na danych osobowych, takich jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i ich usuwanie

Użytkownik - osoba posiadająca upoważnienie wydane przez administratora danych osobowych i dopuszczona do przetwarzania danych osobowych w zakresie wskazanym w upoważnieniu

Identyfikator użytkownika (login) - ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym

Hasło - ciąg znaków literowych, cyfrowych lub innych, przypisany do identyfikatora użytkownika, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.

2. PROCEDURA NADAWANIA UPRAWNIEŃ DO PRZETWARZANIA DANYCH I REJESTROWANIA TYCH UPRAWNIEŃ W SYSTEMIE INFORMATYCZNYM

1. Przetwarzać dane osobowe w systemach informatycznych może wyłącznie osoba posiadająca pisemne upoważnienie do przetwarzania danych osobowych (wzór upoważnienia stanowi załącznik nr 4 do Zarządzenia Nr 3/11 Kierownika Urzędu - Wójta Gminy Sławno w sprawie wprowadzenia zasad ochrony danych osobowych przetwarzanych w Urzędzie Gminy w Sławnie.

2. Identyfikator i hasło do systemu operacyjnego komputera, na którym przetwarzane są dane osobowe są przydzielane użytkownikowi tylko w przypadku, gdy posiada on pisemne upoważnienie do przetwarzania danych osobowych wydane przez Administratora danych osobowych.

3. Administrator bezpieczeństwa informacji sprawdza przed wydaniem upoważnienia do przetwarzania danych osobowych czy użytkownik spełnia warunki dopuszczenia do przetwarzania danych osobowych, a w szczególności:
   a. czy zna przepisy z zakresu bezpieczeństwa informacji, w tym ochrony danych osobowych,
   b. czy stanowisko pracy użytkownika, w tym system informatyczny, spełnia warunki dopuszczenia do przetwarzania danych osobowych,
   c. czy użytkownik podpisał oświadczenie o poufności, według wzoru w załączniku nr 5 do Zarządzenia Nr 3/11 Kierownika Urzędu - Wójta Gminy Sławno w sprawie wprowadzenia zasad ochrony danych osobowych przetwarzanych w Urzędzie Gminy w Sławnie.

4. Za przydzielenie identyfikatora i hasła użytkownikowi, który pierwszy raz będzie przetwarzał dane osobowe w systemie informatycznym odpowiada Administrator systemów informatycznych.

5. Identyfikator i hasło użytkownikowi przydzielane są na wniosek Administratora bezpieczeństwa informacji.

6. Odebranie uprawnień użytkownika do przetwarzania danych realizuje Administrator systemów informatycznych na wniosek Administratora bezpieczeństwa informacji.

7. Administrator systemów informatycznych rejestruje wykonane czynności związane z przydzielaniem i odbieraniem identyfikatorów i haseł w dzienniku pracy systemu.

3. STOSOWANE METODY I ŚRODKI UWIERZYTELNIENIA ORAZ PROCEDURY ZWIĄZANE Z ICH ZARZĄDZANIEM I UŻYTKOWANIEM

1. W systemach służących do przetwarzania danych osobowych stosowane jest uwierzytelnianie użytkownika przy pomocy jego identyfikatora i hasła.
2. Dostęp do danych osobowych przetwarzanych w systemie informatycznym możliwy jest wyłącznie po podaniu identyfikatora i właściwego hasła.
3. Każdy użytkownik systemu przetwarzania posiada swój unikalny identyfikator.
4. Użytkownikom zabrania się używania tych samych identyfikatorów oraz wymieniania się identyfikatorami.
5. Pierwsze hasło przypisane nowemu użytkownikowi Administrator systemów informatycznych przekazuje w formie pisemnej.
6. Użytkownik jest zobowiązany zmienić hasło, przy pierwszym dostępie do systemu.
7. Każdy użytkownik zarządza swoimi hasłami dla wszystkich identyfikatorów, których używa.
8. Hasło użytkownika jest jego własnością; zabronione jest przekazywanie go innym osobom.
9. Hasło użytkownika składa się z minimum 8 znaków i jest zmieniane co 30 dni.
10. Hasło oprócz znaków literowych małych i dużych zawiera znaki alfanumeryczne i specjalne.
11. Użytkownicy są zobowiązani do przestrzegania zasad dotyczących długości i złożoności hasła określonych powyżej.
12. W przypadku, gdy istnieje podejrzenie, że hasło mogła poznać osoba nieuprawniona, użytkownik zobowiązany jest do natychmiastowej zmiany hasła.

13. Hasło użytkownika nie jest pokazywane na ekranie lub wydrukach w postaci otwartego tekstu.

14. Administrator systemów informatycznych nadzoruje funkcjonowanie procedury zmiany haseł przez użytkowników.

15. Jeżeli dane wykorzystywane do uwierzytelniania przesyłane są w sieci publicznej Administrator danych stosuje wobec nich środki ochrony kryptograficznej.

4. PROCEDURY ROZPOCZĘCIA, ZAWIESZENIA I KOŃCZENIA PRACY PRZEZNACZONE DLA UŻYTKOWNIKÓW SYSTEMU

1. Przed rozpoczęciem pracy, w trakcie rozpoczynania pracy z systemem informatycznym oraz w trakcie pracy każdy użytkownik obowiązany jest do zwracania uwagi, czy nie wystąpiły symptomy mogące świadczyć o naruszeniu ochrony danych osobowych. Szczegółowy opis takich symptomów oraz sposób postępowania w przypadku ich wykrycia został opisany w dokumencie „Polityka bezpieczeństwa przetwarzania danych osobowych" rozdział 6.

2. Rozpoczęcie pracy użytkownika w systemie informatycznym obejmuje wprowadzenie identyfikatora i hasła w sposób minimalizujący ryzyko podejrzenia przez osoby nieupoważnione oraz ogólne stwierdzenie poprawności działania systemu.

3. Maksymalna ilość prób wprowadzenia hasła przy logowaniu się do systemu wynosi trzy. Po przekroczeniu tej liczby system blokuje dostęp do zbioru danych na poziomie danego użytkownika. Odblokowania konta dokonuje Administrator systemów informatycznych, który informuje o powyższym Administratora bezpieczeństwa informacji

4. W przypadku bezczynności użytkownika na stacji roboczej przez okres dłuższy niż 15 minut automatycznie włączany jest wygaszacz ekranu. Wygaszacze ekranu są zaopatrzone w hasła zbudowane analogicznie do haseł używanych przez użytkownika przy logowaniu. Hasło jest zmieniane nie rzadziej niż co 30 dni.

5. Zmianę użytkownika stacji roboczej każdorazowo poprzedza wylogowanie się poprzedniego użytkownika.

6. W przypadku, gdy przerwa w pracy na stacji roboczej trwa dłużej niż 60 minut użytkownik wylogowuje się z aplikacji i systemu stacji roboczej na której pracuje oraz sprawdza czy nie zostały pozostawione bez zamknięcia nośniki informacji zawierające dane osobowe.

7. Kończąc pracę użytkownik w systemie informatycznym wylogowanie się z aplikacji.

5. ZABEZPIECZENIE NOŚNIKÓW DANYCH OSOBOWYCH

5.1 PROCEDURY TWORZENIA KOPII ZAPASOWYCH ZBIORÓW DANYCH I PROGRAMÓW SŁUŻĄCYCH DO ICH PRZETWARZANIA ORAZ SPOSOBY ICH PRZECHOWYWANIA

1. Dane osobowe i programy służące do ich przetwarzania w systemie informatycznym zabezpiecza się poprzez tworzenie kopii zapasowych.
2. Za proces tworzenia kopii zapasowych odpowiada Administrator systemów informatycznych; kopie danych mogą wykonywać również przeszkoleni w tym zakresie użytkownicy.
3. Kopie zapasowych danych Administrator systemów informatycznych sporządza na nośniku wymiennym i przechowuje w szafie metalowej w pomieszczeniu informatyka znajdującym się w budynku Urzędu na poziomie 0.
4. Kopie zapasowe danych Administratora bezpieczeństwa informacji sporządzana nie rzadziej niż raz w tygodniu. Może być to realizowane poprzez nadpisywanie ich na nośnikach zapisanych wcześniejszymi kopiami danych.

5.2 POSTĘPOWANIE Z NOŚNIKAMI WYCOFANYMI Z UŻYTKOWANIA

1. Nośniki danych oraz kopii zapasowych, które zostały wycofane z użycia, pozbawia się zapisanych na nich danych za pomocą specjalnego oprogramowania do bezpiecznego usuwania zapisanych danych.
2. W wypadku, gdy nie przewiduje się ich ponownego wykorzystywania do innych celów podlegają fizycznemu zniszczeniu z wykorzystaniem metod adekwatnych do typu nośnika, w sposób uniemożliwiający odczytanie zapisanych na nich danych.

6. SPOSÓB ZABEZPIECZENIA SYSTEMU INFORMATYCZNEGO PRZED INGERENCJĄ ZEWNĘTRZNĄ

6.1. ZABEZPIECZENIE PRZED DZIAŁANIEM SZKODLIWEGO OPROGRAMOWANIA

1. W związku z istnieniem zagrożenia, ze strony wirusów komputerowych oraz innego oprogramowania złośliwego, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego, konieczna jest ochrona przed nimi systemów komputerowych przetwarzających dane osobowe.

2. Wirusy komputerowe mogą infekować systemy informatyczne poprzez: Internet, nośniki informacji takie jak: płyty CD, DVD, dyski przenośne, pamięci typu flash itp.

3. Serwer, za pośrednictwem którego komputery uzyskują dostęp do publicznej sieci Internet jest zabezpieczony urządzeniem „UTM" uniemożliwiającym uzyskanie nieuprawnionego dostępu do zgromadzonych w nim danych.

4. Oprogramowanie urządzenia którym mowa w pkt. 3 jest na bieżąco aktualizowane zgodnie z zaleceniami producenta.

5. Użytkownicy każdorazowo sprawdzają elektroniczne nośniki informacji takie jak dyskietki, dyski przenośne, pamięci typu flash itp. programem antywirusowym przed ich użyciem, po zainstalowaniu w systemie.

6. W przypadku wystąpienia infekcji i braku możliwości automatycznego usunięcia wirusów przez system antywirusowy użytkownik zaprzestaje wszelkich czynności w systemie i informuje Administrator systemów informatycznych

7. Przy korzystaniu z poczty elektronicznej należy zwrócić szczególną uwagę na otrzymywane załączniki dołączane do treści wiadomości. Zabrania się otwierania załączników i wiadomości poczty elektronicznej od „nieznanych" nadawców.

8. Zabrania się użytkownikom, wyłączania, blokowania, odinstalowywania programów zabezpieczających komputer przed złośliwym oprogramowaniem oraz nieautoryzowanym dostępem.

6.2. KONTROLA DZIAŁAŃ I PRZEPŁYWU INFORMACJI Z SIECI PUBLICZNEJ

1. System informatyczny przetwarzający dane osobowe zabezpieczony jest urządzeniem „UTM", które realizuje kontrolę przepływu informacji z siecią publiczną.

2. Kontrolowane są również wszelkie działania inicjowane z sieci publicznej i systemu informatycznego Administratora danych.

7. SPOSÓB REALIZACJI WYMOGÓW W ZAKRESIE EWIDENCJI WPISÓW I UDOSTĘPNIEŃ DANYCH

1. System informatyczny przetwarzający dane osobowe posiada mechanizmy pozwalające na kontrolę dostępu do danych poprzez odnotowanie faktu wykonania operacji takich jak: logowanie konkretnego użytkownika, czas rozpoczęcia i zakończenia przez danego użytkownika pracy.

2. System odnotowuje również nieudane próby dostępu do niego.

3. Jeżeli dostęp do danych przetwarzanych w systemie informatycznym posiadają co najmniej dwie osoby, wówczas system zapewnia:
   a) rejestrowanie w systemie dla każdego użytkownika odrębnego identyfikatora;
   b) dostęp do danych wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia.

4. Odnotowanie informacji, o których mowa w pkt. 1 następuje automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzenia danych.

5. System rejestruje dane odbiorców, którym dane osobowe zostały udostępnione, oraz datę i zakres tego udostępnienia.

8. PROCEDURY WYKONYWANIA PRZEGLĄDÓW I KONSERWACJI SYSTEMÓW ORAZ NOŚNIKÓW INFORMACJI SŁUŻĄCYCH DO PRZETWARZANIA DANYCH

1. Wszelkie prace związane z naprawami i konserwacją systemu informatycznego przetwarzającego dane osobowe uwzględniają wymagany poziom zabezpieczenia tych danych przed dostępem do nich osób nieupoważnionych.
2. Przeglądy i konserwacje systemu oraz zbiorów danych wykonuje Administrator systemów informatycznych na bieżąco, lecz nie rzadziej niż dwa razy w roku.
3. Sprawdzeniu podlega:
   a) spójność danych i indeksów,
   b) sprawność warstwy sprzętowej do realizacji wszystkich funkcji niezbędnych z punktu widzenia wykonywanych działań,
   c) poprawność funkcjonowania systemu operacyjnego (m.in. analiza dzienników zdarzeń) oraz poprawność konfiguracji pod względem wydajnościowym jak i zapewnienia bezpieczeństwa,
   d) poprawność funkcjonowania aplikacji przetwarzających dane,
   e) zgodność liczby użytkowników i ich uprawnień ze stanem oczekiwanym,
   f) zabezpieczenia systemu informatycznego ze względu na mogące się pojawić zagrożenia (np. brak zasilania, atak wirusowy, itp.),
4. Konserwacja sprzętu może być prowadzona również przez firmy zewnętrzne na podstawie zawartych umów. Umowa musi bezwzględnie zawierać klauzulę o przestrzeganiu przez pracowników firmy zasad zachowania poufności w stosunku do danych osobowych znajdujących się w konserwowanym systemie.
5. W razie konieczności naprawy urządzeń poza miejscem ich użytkowania, sprzęt komputerowy, przed oddaniem do serwisu, jest odpowiednio przygotowany. Dane są archiwizowane na nośniki informacji, a dyski twarde - gdy jest to tylko możliwe - wymontowywane i zabezpieczyć na czas naprawy.
6. W przypadku niemożności zrealizowania czynności o których mowa w pkt 5 naprawy dokonuje się pod nadzorem Administratora systemów informatycznych.

załącznik nr 3

Zakres działania administratora bezpieczeństwa informacji

1. Administrator bezpieczeństwa informacji podlega bezpośrednio Administratorowi danych osobowych.
2. Administrator bezpieczeństwa informacji sprawuje nadzór nad Administratorem systemów informatycznych w zakresie przetwarzania danych osobowych w systemach informatycznych.
3. Administrator bezpieczeństwa informacji jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych w Urzędzie oraz ich zabezpieczenie przed udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.
4. Administrator bezpieczeństwa informacji jest odpowiedzialny za:
   1) nadzorowanie zasad bezpieczeństwa danych osobowych zgromadzonych i przetwarzanych w Urzędzie;
   2) podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń;
   3) w szczególności jest odpowiedzialny za:
   a) zapewnienie przetwarzania danych osobowych zgodnie z ustawą o ochronie danych osobowych,
   b) nadzór nad przestrzeganiem przez pracowników zasad ochrony danych osobowych obowiązujących w Urzędzie,
   c) dopuszczenie do przetwarzania danych wyłącznie osób upoważnionych,
   d) nadzór nad nadawaniem i odbieraniem uprawnień do korzystania z danych osobowych oraz prowadzenie ewidencji uprawnień,
   e) rejestrowanie zbiorów danych u Generalnego Inspektora Ochrony Danych Osobowych,
   f) prowadzenie ewidencji wniosków o udostępnianie danych osobowych (także w przypadku przekazywania ich do państwa trzeciego zgodnie z rozdziałem 7 ustawy o ochronie danych osobowych)
   g) nadzór nad przeprowadzaniem w bezpieczny sposób napraw i konserwacji sprzętu i oprogramowania służącego do przetwarzania lub będącego nośnikiem danych osobowych,
   h) koordynację procesu reagowania na naruszenia lub próby naruszenia bezpieczeństwa danych osobowych,
   i) organizowanie szkoleń dla osób upoważnionych do korzystania z danych osobowych,
   j) monitorowanie zmian w przepisach prawnych dotyczących sposobu zabezpieczenia danych osobowych i dopasowanie systemu do wymagań prawnych,
   k) monitorowanie zaleceń i interpretacji GIODO w zakresie ochrony danych osobowych i implementowanie ich w Urzędzie.

WÓJT GMINY
mgr Tadeusz Wojciechowski

załącznik nr 4

UPOWAŻNIENIE

do przetwarzania danych osobowych nr .....

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926, z późn. zm.):

upoważniam, Panią/Pana .....
(imię i nazwisko)

zatrudnioną na stanowisku .....

w .....
(nazwa jednostki/komórki organizacyjnej)

do przetwarzania danych osobowych, które obejmuje przetwarzanie danych osobowych w zakresie *

.....

.....

.....
(podpis administratora danych osobowych)

....., dnia.....

* podać sposób przetwarzania danych np. w systemie informatycznym lub/także w kartotekach, skorowidzach, księgach, wykazach i innych zbiorach ewidencyjnych oraz wymienić zbiory danych

załącznik nr 5

.....

(pieczęć nagłówkowa jednostki)

REJESTR OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH w Urzędzie Gminy w Sławnie

Lp.	Nazwa zbioru danych	Nazwisko i imię	Rodzaj uprawnień	Numer upoważnienia	Nazwa Identyfikatora	Data		Lokalizacja	Uwagi
						nadania uprawnień	ustania uprawnień		
1	2	3	4	5	6	7	8	9	10

Legenda:

1) kolumna 4 – wpisać skróty stosowane do określenia uprawnień w systemie informatycznym:

P - pełne prawa do zarządzania bazą danych

W - pełne prawa do edycji danych (w tym drukowania, archiwizowania, usuwania)

N - prawo do zakładania nowych kont

C - prawo do tworzenia nowych danych

M - prawo modyfikacji istniejących danych

O - prawo do odczytu danych

D - prawo do drukowania danych

A - prawo do wykonywania kopii archiwalnych

2) E - skrót stosowany do określenia uprawnień poza systemem informatycznym

załącznik nr 6

....., dnia.....

.....
(imię i nazwisko)

.....
(stanowisko, jednostka organizacyjna)

.....
(nr ewidencyjny)

OŚWIADCZENIE

Ja niżej podpisany oświadczam, że znana mi jest treść przepisów:

1. Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych;
2. Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych;
3. Zarządzenia nr 3/11 Kierownika Urzędu - Wójta Gminy Sławno z dnia 1 lutego 2011 r. w sprawie ochrony danych osobowych przetwarzanych w Urzędzie Gminy i wydanych na jego podstawie:
   1) Polityki bezpieczeństwa ochrony danych osobowych,
   2) Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych

i zobowiązuję się

nie ujawniać nikomu w żaden sposób i nie wykorzystywać informacji związanych z przetwarzanymi danymi osobowymi, z którymi się zapoznałam(em) w związku z wykonywaną pracą, oraz zachować w tajemnicy sposoby ich zabezpieczenia.

.....
(potwierdzenie ważności podpisu,
kierownik jednostki organizacyjnej)

.....
(podpis pracownika)

załącznik nr 7

Zakres działania administratora systemów informatycznych

1. Przeprowadzanie w bezpieczny sposób napraw i konserwacji sprzętu i oprogramowania służącego do przetwarzania lub będącego nośnikiem danych osobowych.
2. Sprawowanie nadzoru nad zapewnieniem awaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych.
3. Sprawowanie nadzoru nad likwidacją urządzeń komputerowych, na których zapisane są dane osobowe.
4. Identyfikowanie i analizowanie zagrożenia oraz ryzyka, na które narażone może być przetwarzanie danych osobowych w systemach informacyjnych Urzędu.
5. Określanie potrzeb w zakresie zabezpieczenia systemów informacyjnych, w których przetwarzane są dane osobowe.
6. Monitorowanie działania zabezpieczeń wdrożonych w celu ochrony danych osobowych w systemach informacyjnych.
7. Sprawowanie nadzoru nad funkcjonowaniem mechanizmów uwierzytelniania użytkowników w systemie informacyjnym przetwarzającym dane oraz kontrolą dostępu do danych.
8. Bieżący monitoring i zapewnienie ciągłości działania systemu informatycznego oraz baz danych.
9. Zarządzanie kopiami awaryjnymi konfiguracji oprogramowania systemowego.
10. Zarządzanie kopiami awaryjnymi danych w tym danych osobowych oraz zasobów umożliwiających ich przetwarzanie.
11. Przeciwdziałanie próbom naruszenia bezpieczeństwa informacji w systemach informatycznych.
12. Przyznawanie na podstawie upoważnienia Administratora danych, ściśle określonych praw dostępu do informacji w danym systemie.
13. Wnioskowanie do Administratora bezpieczeństwa Informacji w sprawie procedur bezpieczeństwa i standardów zabezpieczeń.
14. Zarządzanie licencjami, procedurami ich dotyczącymi, prowadzenie profilaktyki antywirusowej.
15. Uczestniczenie w procedurze realizowanej w sytuacji naruszenia zbiorów danych osobowych.

Funkcjonowanie Administratora systemów informatycznych jest nadzorowane pod względem zachowania bezpieczeństwa danych przez Administratora bezpieczeństwa informacji.