Załącznik nr 1
do Zarządzenia nr 7/2013
Przewodniczącego Zarządu Związku Gmin Krajny w Złotowie
z dnia 21sierpnia 2013r.

Polityka bezpieczeństwa w zakresie zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Związku Gmin Krajny w Złotowie.

Rozdział I

Postanowienia ogólne

1. Polityka bezpieczeństwa w zakresie zarządzania systemem informatycznym służącym do przetwarzania danych osobowych określa reguły postępowania i praktyczne doświadczenia dotyczące zarządzania, ochrony i dystrybucji informacji podlegającej ochronie (danych osobowych) w Związku Gmin Krajny w Złotowie. Dokument zwraca uwagę na konsekwencje jakie mogą ponosić osoby przekraczające określone granice oraz procedury postępowania dla zapobiegania i minimalizowania skutków zagrożeń.

2. Celem polityki bezpieczeństwa, o której mowa w pkt. 1, jest wskazanie działań, jakie należy podejmować oraz ustanowienie zasad, jakie należy stosować, aby prawidłowo były realizowane obowiązki administratora danych w zakresie zabezpieczenia danych osobowych. Polityka wskazuje sposób postępowania w sytuacji naruszenia bezpieczeństwa danych osobowych w systemach informatycznych i przeznaczony jest dla osób zatrudnionych przy przetwarzaniu tych danych.

3. Polityka określa tryb postępowania w przypadku, gdy:
   a) stwierdzono naruszenie zabezpieczenia systemu informatycznego,
   b) 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.

4. Obowiązkiem osób zatrudnionych przy przetwarzaniu danych osobowych jest przestrzeganie postanowień niniejszej polityki.

5. Realizacja postanowień tego dokumentu ma zapewnić ochronę danych osobowych, właściwą ocenę i udokumentowanie przypadków naruszenia bezpieczeństwa systemów oraz zapewnić właściwy tryb działania w celu przywrócenia bezpieczeństwa danych przetwarzanych w systemach informatycznym w Związku Gmin Krajny.

6. Związek Gmin Krajny w Złotowie stosuje odpowiednie środki informatyczne, techniczne i organizacyjne w celu zabezpieczenia danych osobowych przed ich udostępnianiem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszenie ustawy o ochronie danych osobowych, nieautoryzowaną zmianą, utratą, uszkodzeniem lub zniszczeniem.

7. Sprawne realizowanie misji i celów Związku Gmin Krajny w Złotowie w wielu obszarach jest silnie uzależnione od niezakłóconej pracy jego systemów informacyjnych i bezpieczeństwa przetwarzanych w nich informacji.

8. Utrzymanie bezpieczeństwa przetwarzanych przez Związek informacji rozumiane jest jako zapewnienie ich poufności, integralności i dostępności na odpowiednim poziomie.

Stwierdzam prawidłowość niniejszej Polityki bezpieczeństwa pod względem formalnoprawnym. Karta [illegible] niniejszego dokumentu została podpisana

RADCA PRAWNY
BdP - 209
Radosław Kilar

Miarą bezpieczeństwa jest wielkość ryzyka związanego z zasobem stanowiącym przedmiot niniejszej Polityki.

9. Cele Związku Gmin Krajny w dziedzinie bezpieczeństwa informacji:
   a) ochrona zasobów informacyjnych Związku i zapewnienie ciągłości działania procesów Związku,
   b) ochrona wizerunku Związku,
   c) zapewnienie zgodności z prawem podejmowanych działań,
   d) uzyskanie i utrzymanie odpowiednio wysokiego poziomu bezpieczeństwa zasobów Związku rozumiane jako zapewnienie poufności, integralności i dostępności zasobów oraz zapewnienie rozliczalności podejmowanych działań,
   e) wyznaczenie ogólnych kierunków rozwoju systemu informacyjnego,
   f) podnoszenie kultury informatycznej i tworzenie bezpiecznego społeczeństwa informacyjnego.

10. Cele osiągane są przez:
   a) właściwą organizację systemu informatycznego,
   b) zarządzanie ryzykiem w celu ograniczania go do akceptowanego poziomu,
   c) właściwą ochronę informacji, a w szczególności informacji prawnie chronionych,
   d) zapewnienie odpowiedniego poziomu dostępności informacji i niezawodności systemów informatycznych,
   e) właściwą ochronę informacji związanych z zawartymi umowami,
   f) wdrażanie i rozwój systemów informacyjnych z zachowaniem zasad bezpieczeństwa,
   g) eksploatowanie systemów informatycznych zgodnie z zasadami bezpieczeństwa,
   h) stałą edukację użytkowników systemu informacyjnego.

11. W systemie informacyjnym Związku przetwarzane są informacje służące do wykonywania zadań z zakresu administracji publicznej i rozwoju instytucjonalnego.

12. Informacje te są przetwarzane i składowane zarówno w postaci manualnej jak i elektronicznej.

13. Przetwarzane w Związku informacje są miedzy innymi informacjami dotyczącymi:
   a) informacji publicznych,
   b) danych osobowych,
   c) informacji stanowiących tajemnice Związku,
   d) i innych informacji prawnie chronionych.

14. Informacje niejawne nie są objętym zakresem niniejszej polityki.

15. Administrator danych, którym jest Przewodniczący Zarządu Związku Gmin Krajny w Złotowie, wyznacza Administratora Bezpieczeństwa Informacji (ABI) oraz osobę upoważnioną do zastępowania Administratora.

16. Administrator Bezpieczeństwa Informacji realizuje zadania w zakresie ochrony danych, a w szczególności:
   a) ochrony i bezpieczeństwa danych osobowych zawartych w zbiorach systemów informatycznych Związku,
   b) podejmowania stosownych działań w przypadku wykrycia nieuprawnionego dostępu do bazy danych lub naruszenia zabezpieczenia danych,

RADCA PRAWNY
Radosław Kilar

c) niezwłocznego informowania Administratora danych lub osoby przez niego upoważnionej o przypadkach naruszenia przepisów ustawy o ochronie danych osobowych,
d) podejmuje stosowne działania zgodnie z niniejszą polityką w przypadku otrzymania informacji o naruszeniu zabezpieczeń systemu informatycznego lub informacji o zmianach w sposobie działania programu lub urządzeń, a także w przypadku wykrycia nieuprawnionego dostępu do bazy danych lub naruszenia zabezpieczenia danych wskazujących na naruszenie bezpieczeństwa danych,
e) nadzoru i kontroli systemów informatycznych służących do przetwarzania danych osobowych i osób przy nim zatrudnionych,
f) nadzoruje funkcjonowanie mechanizmów uwierzytelniania użytkowników w systemie informatycznym przetwarzającym dane osobowe oraz kontroli dostępu do danych osobowych,
g) nadzoruje wykonywanie kopii awaryjnych, ich przechowywanie oraz okresowe sprawdzanie pod katem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu,
h) nadzoruje przeglądy, konserwacje oraz uaktualnienia systemu informatycznego służącego do przetwarzania danych osobowych,
i) fizycznego zabezpieczenia danych osobowych oraz obiektów, w których są gromadzone i przetwarzane, prowadzi rejestr osób upoważnionych do przetwarzania danych osobowych,
j) przegląda niniejszą politykę pod kątem aktualności i stosowalności nie rzadziej niż raz w roku.

17.Osoba zastępująca Administratora Bezpieczeństwa Informacji powyższe zadania realizuje w przypadku nieobecności Administratora Bezpieczeństwa.

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

Rozdział II

Identyfikacja zasobów systemu informatycznego

1. Struktura teleinformatyczna Związku składa się z sieci lokalnej połączonej do sieci Internet poprzez system firewall. W ramach tej infrastruktury funkcjonuje system informatyczny służący do rejestrowania i przetwarzania danych osobowych. Informacje przetwarzane w tym systemie są jawne, ale podlegają ochronie, zgodnie z przepisami ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.

2. W ramach tej infrastruktury funkcjonuje także system finansowo-kadrowy oraz inne systemy usług sieciowych. Zawierają one dane podlegające ochronie ze względu na powyższą ustawę oraz są strategicznie ważne dla ciągłości pracy Związku.

3. Podstawowym systemem informatycznym Związku Gmin Krajny w Złotowie jest system służący do zbierania, rejestrowania i przetwarzania danych o osobach zamieszkałych na terenie miasta Złotowa. Do zbierania i wprowadzania danych do systemu są wykorzystywane stacjonarne komputery, stanowiące wyposażenie pracowników Związku.

RADCA PRAWNY
DdP - 209
Radosław Kitar

4. Zapewnienie właściwej ochrony systemu informatycznego Związku, ze względu na różnorodność przetwarzanych systemów oraz fakt połączenia z siecią INTERNET, jest zagadnieniem złożonym. Wprowadzanie efektywnej ochrony systemu informatycznego Związku, ze względu na znaczne koszty, jest procesem długotrwałym i musi być rozłożony na etapy.

Rozdział III

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, pogorszenie jakości sprzętu i oprogramowania) - może dojść do zniszczenia danych, może zostać zakłócona ciągłość pracy systemu, może nastąpić naruszenie poufności danych.

3) Zagrożenia zamierzone - świadome i celowe działania powodujące 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,
- nieuprawnione przekazanie danych,
- bezpośrednie zagrożenie materialnych składników systemu (np. kradzież sprzętu).

2. Naruszenie lub podejrzenie naruszenia systemu informatycznego, w którym przetwarzane są dane osobowe następuje w sytuacji:

a) losowego lub nieprzewidzianego oddziaływania czynników zewnętrznych na zasoby systemu jak np.: wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, itp.,
b) niewłaściwych parametrów środowiska, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy lub wibracje pochodzące od urządzeń przemysłowych,
c) awarii sprzętu lub oprogramowania, które wyraźnie wskazuje na umyślne działanie w kierunku naruszenia ochrony danych,
d) pojawienia się odpowiedniego komunikatu alarmowego,
e) podejrzenia nieuprawnionej modyfikacji danych w systemie lub innego odstępstwa od stanu oczekiwanego,
f) naruszenia lub próby naruszenia integralności systemu lub bazy danych w tym systemie,
g) pracy w systemie wykazującej odstępstwa uzasadniające podejrzenie przełamania lub zaniechania ochrony danych osobowych - np. praca osoby, która nie jest formalnie dopuszczona do obsługi systemu,

RADCA PRAWNY
WOP - 209
Radosław Kilar

h) ujawnienia nieautoryzowanych kont dostępu do systemu,
i) naruszenia dyscypliny pracy w zakresie przestrzegania procedur bezpieczeństwa informacji (np. nie wylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych osobowych w drukarce lub na ksero, nie zamknięcie pomieszczenia z komputerem, pracę na danych osobowych w celach prywatnych, itp.).

3. Za naruszenie ochrony danych uważa się również stwierdzone nieprawidłowości w zakresie zabezpieczenia fizycznego miejsc przechowywania i przetwarzania danych osobowych np.:

- niezabezpieczone pomieszczenia,
- nienadzorowane, otwarte szafy, biurka, regały,
- niezabezpieczone urządzenia archiwizujące,
- pozostawianie danych w nieodpowiednich miejscach – kosze, stoły itp.

4. W przypadku stwierdzenia naruszenia ochrony danych osobowych, stosuje się instrukcję postępowania, stanowiącą załącznik nr 4 do niniejszej polityki.

Rozdział IV

Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe

1. Przetwarzaniem danych osobowych jest wykonywanie jakichkolwiek operacji na danych osobowych, takich jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza takich, które wykonuje się w systemach informatycznych.

2. Biorąc pod uwagę przepisy ustawy, nakazujące jej stosowanie także w przypadkach przetwarzania danych poza zbiorem danych, przetwarzanie danych osobowych może wystąpić w większości pomieszczeń Związku.

3. Ze względu jednak na nagromadzenie danych osobowych, szczególnie chronione powinny być pomieszczenia serwerowni, pomieszczenia, w których przechowuje się i składuje kopie zapasowe, pomieszczenia archiwów zakładowych oraz pomieszczenia komórek finansowo-księgowych i kadrowych.

4. Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar w Związku Gmin Krajny w Złotowie obszar, w którym przetwarzane są dane osobowe stanowi załącznik A do niniejszego załącznika.

RADCA PRAWNY
BDP - 209
Radosław Kilar

Rozdział V

Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych, struktury zbiorów wskazujące zwartość poszczególnych pól i przepływ danych pomiędzy poszczególnymi programami w Związku Gmin Krajny w Złotowie

Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych, struktury zbiorów wskazujące zwartość poszczególnych pól oraz przepływ danych pomiędzy poszczególnymi systemami w Związku Gmin Krajny w Złotowie stanowi załącznik B do niniejszego załącznika.

Rozdział VI

Środki techniczne i organizacyjne służące zapewnieniu poufności, integralności i rozliczalności przetwarzania danych

System informatyczny Związku, ze względu na połączenie z siecią publiczną, musi zapewniać środki bezpieczeństwa określone dla wysokiego poziomu bezpieczeństwa (§6 ust. 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).

I. Bezpieczeństwo fizyczne

1. Gwarancją zapewnienia bezpieczeństwa systemu informatycznego Związku oraz przetwarzanych i przechowywanych danych jest zapewnienie bezpieczeństwa fizycznego:

a) kontrola dostępu – pomieszczenia, w których znajdują się stacje robocze, serwery i węzły sieci LAN oraz te, w których przechowywane są i składowane dane, są zamykane na klucz, a dostęp do nich posiadają tylko upoważnione osoby,

b) dane osobowe przechowywane w wersji tradycyjnej (papierowej) lub elektronicznej (pendrive, płyta CD/DVD, dyskietka) po zakończeniu pracy są przechowywane w zamykanych na klucz meblach biurowych. Klucze do szafek należy zabezpieczyć przed dostępem osób nieupoważnionych do przetwarzania danych osobowych,

c) nieaktualne lub błędne wydruki zawierające dane osobowe niszczone są w niszczarce.

2. Obowiązkiem osoby użytkującej komputer przenośny zawierający dane osobowe jest zachowanie szczególnej ostrożności podczas jego transportu, przechowywania i użytkowania poza pomieszczeniami tworzącymi obszar, w którym przetwarzane są dane osobowe. Należy dążyć do powszechnego stosowania ochrony kryptograficznej w takich przypadkach.

Radosław Kilar

3. Wszystkie komputery są zabezpieczone hasłem na BIOS przed uruchomieniem komputera przez osoby nieuprawnione.

II. Wykorzystanie mechanizmów systemu operacyjnego

1. System operacyjny Microsoft Windows XP posiada wbudowane mechanizmy nadawania uprawnień i praw dostępu. Dla pełnego wykorzystania tych mechanizmów stosowany jest system plików NTFS.

2. Wszyscy użytkownicy systemów informatycznych posiadają swój indywidualny login i hasło w usłudze katalogowej Novell, w przypadku użytkowników niepodłączonych do systemu Novell login i pierwsze hasło ustala administrator sieci. Są oni rozróżniani i identyfikowani w systemie na podstawie swoich loginów. Przydział uprawnień jest możliwy po zalogowaniu się użytkownika do systemu Novell/Windows.

III. Zarządzanie oprogramowaniem

1. Najwyższe uprawnienia w systemie informatycznym posiada administrator systemu. Tylko administrator jest osobą uprawnioną do instalowania i usuwania oprogramowania systemowego i narzędziowego.

2. Dopuszcza się instalowanie tylko legalnie pozyskanych programów, niezbędnych do wykonywania ustawowych zadań Związku i posiadających ważną licencję użytkowania komercyjnego lub GPL.

IV. Uwierzytelnianie użytkowników

1. Dostęp do systemu informatycznego służącego do przetwarzania danych osobowych, może uzyskać wyłącznie osoba (użytkownik) zarejestrowana w tym systemie przez administratora systemu.

2. Dostęp do systemów operacyjnych serwerów i stacji roboczych jest chroniony przez nazwę użytkownika i hasło. System Novell ma wbudowane mechanizmy ograniczające liczbę błędnych prób logowania oraz umożliwia wskazanie stacji roboczych, na których dany użytkownik może pracować. Zastosowane są blokady konta użytkownika na 6 prób logowania. Po blokadzie konta użytkownika odblokowanie jest możliwe tylko przez administratora systemu informatycznego.

3. Identyfikator użytkownika składa się z co najmniej sześciu znaków. W identyfikatorze pomija się polskie znaki diakrytyczne.

4. Hasło składa się z unikalnego zestawu co najmniej ośmiu znaków, zawiera małe i wielkie litery oraz cyfry lub znaki specjalne. Hasło nie może być identyczne z identyfikatorem użytkownika, ani z jego imieniem lub nazwiskiem. Wymuszenie zmiany haseł w systemie Novell następuje automatycznie co 30 dni. Zastosowana jest również historia pamiętania kilku ostatnich haseł tzn. użytkownicy nie mogą zastosować tego samego hasła podczas próby wymuszenia zmiany hasła.

5. Użytkownikom systemu nie wolno udostępniać swojego hasła innym osobom.

V. Redundancja sprzętowa i programowa

1. Dla zapewnienia wysokiej niezawodności systemu administrator sytemu wyznacza komputery na serwery zapasowe.

RADCA PRAWNY
WdP - 209
Radosław Kitar

2. Nośniki zawierające kopie baz danych i pełnych systemów operacyjnych są przechowywane i odpowiednio zabezpieczone fizycznie w szafie pancernej w pomieszczeniu administratora sieci (informatyka).

VI. Zapewnienie stałego zasilania energią

Podtrzymywanie zasilania serwerom i komputerom stacjonarnym zapewniają zasilacze awaryjne UPS-Y.

VII. Procedury przeciwpożarowe

Pomieszczenia, w których systemy komputerowe pracują bez nadzoru, szczególnie pomieszczenie serwerowni pracującej w systemie pracy ciągłej są wyposażone w gaśnice ppoż.

VIII. Procedury awaryjne i procedury na wypadek klęsk żywiołowych i ewakuacji

Zapewnieniu ciągłej dostępności informacji służą komputery przewidywane na awaryjne serwery. Powinny one stać w pomieszczeniach innych niż serwery bieżąco eksploatowane. W przypadku gdyby doszło do ewakuacji należy w pierwszej kolejności zapewnić bezpieczeństwo danym.

IX. Procedury tworzenia kopii zapasowych ich przechowywania i ochrony

1. Wszystkie bazy danych aplikacji krytycznych: USC, Księgowość, Ewidencja Ludności, Kadry, Elektroniczny Obieg Dokumentów znajdują się na osobnych serwerach.

2. Dla krytycznych baz danych kopie bezpieczeństwa wykonuje się od poniedziałku do piątku. Składowane są tylko kopie wykonane w piątek lub na wniosek użytkownika.

3. Kopie zapasowe przechowuje się w szafie pancernej w pomieszczeniu innym, niż dane przetwarzane na bieżąco - w pomieszczeniu administratora sieci (informatyka).

4. Kopie awaryjne podlegają takiej samej ochronie jak serwery zawierające dane bieżąco przetwarzane.

X. Profilaktyka antywirusowa

1. Wszystkie serwery i stacje robocze posiadają zainstalowany program antywirusowy, z możliwie często aktualizowaną bazą wykrywanych wirusów. Zabronione jest blokowanie pracy tego programu.

2. Dla zapewnienia ochrony przed wirusami i innymi niepożądanymi kodami sprawdza się wszystkie zbiory przychodzące z sieci rozległej i Internetu. Systemy plików poszczególnych serwerów i stacji roboczych sprawdza się, co najmniej raz w miesiącu, całościowym testem antywirusowym.

XI. Monitorowanie serwerów, systemów operacyjnych i prowadzenie dziennika zdarzeń

System operacyjny zawiera dzienniki zdarzeń zawierające opis wszystkich ważniejszych czynności wykonywanych przez użytkowników a także błędów. Są określone zdarzenia,

Radosław Kilar

które muszą być rejestrowane, jak również tryb postępowania z tymi dziennikami (co rejestrować, w jaki sposób, jak często i na jak długo składować). Są stosowane ograniczenia zbytniego rozszerzenia zakresu rejestrowanych czynności ze względu na obciążenie systemu operacyjnego i wielkość generowanych zbiorów zawierających dzienniki zdarzeń.

XII. Przeciwdziałanie nowym technikom łamania zabezpieczeń oraz eliminacja luk wykrytych w zabezpieczeniach systemów

W związku z dynamicznym rozwojem technik służących do atakowania systemów informatycznych administrator systemu na bieżąco śledzi informacje na temat wykrytych luk i wprowadza aktualizacje zalecane tym zabezpieczeniom.

XIII. Procedury postępowania z nośnikami informacji i wydrukami (wytwarzanie, rejestrowanie, kasowanie, niszczenie)

Dla zachowania wysokiego poziomu bezpieczeństwa informacji w systemie informatycznym określa się procedury postępowania z nośnikami (dyskietki, kasety, pamięci masowe, krążki CD, nośniki papierowe) zawierającymi informacje od chwili wytworzenia do chwili skasowania:

a) dane osobowe przechowywane w wersji tradycyjnej (papierowej) lub elektronicznej (pendrive, płyta CD/DVD, dyskietka) po zakończeniu pracy są przechowywane w zamykanych na klucz meblach biurowych. Klucze do szafek należy zabezpieczyć przed dostępem osób nieupoważnionych do przetwarzania danych osobowych,

b) nieaktualne lub błędne wydruki zawierające dane osobowe niszczone są w niszczarce.

Dąży się dla zapewnienia szczelności systemu - aby nośniki były opisane i ewidencjonowane.

XIV. Testy okresowe systemu ochrony

1. System ochrony jest w sposób ciągły nadzorowany i możliwie często aktualizowany.

2. Kontrole i testy obejmują zarówno dostęp do zasobów systemu, jak i profile oraz uprawnienia poszczególnych użytkowników.

3. Zapisy logów systemowych są przeglądane każdorazowo po wykryciu naruszenia zasad bezpieczeństwa.

XV. Zabezpieczanie przetwarzania niejawnych informacji

1. W systemach informatycznych Związku informacje niejawne mogą być przetwarzane tylko na wydzielonych komputerach dopuszczonych przez właściwą służbę ochrony państwa, po uzyskaniu certyfikatu wydanego na podstawie przepisów ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. z 2005r, Nr 196 poz. 1631).

2. Informacje niejawne nie są objętym zakresem niniejszej polityki.

RADCA PRAWNY
Radosław Kilar

XVI. Zabezpieczenia medium transmisyjnego

1. Połączenia z sieci wewnętrznej z siecią zewnętrzną (Internet) są wykonywane tylko za pośrednictwem systemów firewall o odpowiednich zabezpieczeniach i parametrach zainstalowanych w Związku.

2. Komputery przenośne podczas połączeń z siecią Internet, wykonywanych poza siecią wewnętrzną Związku, muszą być chronione swoimi autonomicznymi systemami firewall.

3. Zasadą konfigurowania systemów firewall jest blokowanie wszystkich usług, które są zbędne dla działalności pracownika Związku.

XVII. Konserwacja i naprawy sprzętu i oprogramowania

1. Wszelkie naprawy i konserwacje sprzętu i oprogramowania mogą odbywać się tylko w obecności osób uprawnionych.

2. Urządzenia informatyczne służące do przetwarzania danych osobowych mogą być przekazane do naprawy dopiero po uzyskaniu zgody Administratora Bezpieczeństwa informacji.

XVIII. Szkolenia

1. Każdy użytkownik powinien mieć świadomość zagrożeń wpływających na bezpieczeństwo systemu informatycznego, z którego korzysta.

2. Organizacyjną ochronę danych i ich przetwarzania realizuje się poprzez:

a) zapoznanie każdej osoby z przepisami dotyczącymi ochrony osobowych, przed dopuszczeniem jej do pracy przy ich przetwarzaniu,

b) przeszkolenie osób, o których mowa powyżej, w zakresie bezpiecznej obsługi urządzeń i programów związanych z przetwarzaniem i ochroną danych osobowych oraz zabezpieczenia pomieszczeń i budynków. Raz na dwa lata przeprowadza się szkolenia z udziałem wszystkich pracowników Związku, omawiające problematykę bezpieczeństwa teleinformatycznego, ze szczególnym uwzględnieniem nowych uregulowań prawnych. Szkolenie to powinno uzmysłowić pracownikom skalę zagrożeń oraz rangę zabezpieczeń, zwłaszcza stosowanych na poziomie użytkownika.

c) kontrolowanie pomieszczeń, w których są przetwarzane dane osobowe.

Rozdział VII

Postanowienia końcowe

1. Zasady określone przez dokumenty Polityki Bezpieczeństwa Systemu Informacyjnego mają zastosowanie do całego systemu informacyjnego Związku w szczególności do:

a) wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych oraz papierowych, w których przetwarzane są lub będą informacje podlegające ochronie,

RADCA PRAWNY
Radosław Kilar

b) informacji będących własnością Związku, lub klienta Związku, o ile zostały przekazane Związkowi na podstawie umów,

c) wszystkich nośników papierowych, magnetycznych lub optycznych, na których są lub będą znajdować się informacje podlegające ochronie,

d) wszystkich lokalizacji – budynków i pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie.

e) wszystkich pracowników w rozumieniu przepisów Kodeksu Pracy, stażystów i innych osób mających dostęp do informacji podlegających ochronie,

2. Do stosowania zasad określonych przez dokumenty polityki zobowiązani są wszyscy pracownicy w rozumieniu przepisów Kodeksu Pracy, stażyści i inne osoby mające dostęp do informacji podlegającej ochronie.

3. Niniejszy dokument będzie zmieniany, w każdym przypadku zmiany przepisów związanych z polityką.

4. Polityka jest dokumentem nadrzędnym nad wszystkimi dokumentami dotyczącymi bezpieczeństwa informacji w Związku Gmin Krajny w Złotowie.

5. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszej polityki, w szczególności przez osobę, która wobec naruszenia ochrony danych osobowych lub uzasadnionego domniemania takiego naruszenia, nie podjęła działań określonych w niniejszym dokumencie, mogą być potraktowane jako ciężkie naruszenie obowiązków pracowniczych.

6. W sprawach nieuregulowanych niniejszym dokumentem mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (t.j. Dz. U. z 2002 r., Nr 101, poz. 926 z póź. zm.), oraz rozporządzenie 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).

RADCA PRAWNY
BdP - 209
Radosław Kilar