

Wymagania Bezpieczeństwa Informatycznego w Jednostkach Administracji Publicznej

Wersja 1.0 – 27 lutego 2007 r.

beta

Spis treści

Wstęp	3
Poruszanie się po dokumencie.....	4
Objaśnienia	4
Wymagania bezpieczeństwa – część I	5
W 1 -Opracowanie polityki bezpieczeństwa	6
W 2 -Opracowanie instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.....	7
W 3 -Kontrola dostępu do obiektów i pomieszczeń, w których zainstalowane serwery przetwarzające dane osobowe	8
W 4 -Sprzętowy moduł bezpieczeństwa HSM (Hardware Security Module)	9
W 5 -Wyposażenie w instalację alarmową klasy SA3	10
W 6 -Ochrona przed awariami zasilania	11
W 7 -Ochrona przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego	12
W 8 -Kopie zapasowe	13
W 9 -Ochrona przed zagrożeniami pochodzącymi z sieci publicznej	14
W 10 -Ochrona kryptograficzna przy udostępnianiu danych w sieci publicznej	15
W 11 -Wysoki poziom bezpieczeństwa	16
Źródła wymogów – część II	17
1 Dz. U. 2004 nr 100 poz. 1024	18
2 Dz. U. 2005 nr 212 poz. 1766	19
3 Dz. U. 2005 nr 200 poz. 1766	19
4 Dz. U. 2005 nr 200 poz. 1651	19
5 Dz. U. 2004 nr 100 poz. 1024	20
6 PN-ISO/IEC 17799:2003 Technika Informatyczna. Praktyczne zasady zarządzania bezpieczeństwem informacji.....	20
7 Dz. U. 2004 nr 100 poz. 1024	21
8 Dz. U. 2004 nr 100 poz. 1024	21
9 Dz. U. 2004 nr 100 poz. 1024	21
10 Dz. U. 2004 nr 100 poz. 1024	22
11 Dz. U. 2004 nr 100 poz. 1024	23
12 Dz. U. 2004 nr 100 poz. 1024	24
Wykaz ustaw i rozporządzeń	27

Wstęp

Szanowni Państwo!

Oddajemy w Wasze ręce opracowanie, które ma być pomocnym przewodnikiem wskazującym, jakie wymagania techniczne i organizacyjne w dziedzinie informatyzacji Waszych urzędów powinniście spełnić, aby być w zgodzie z obowiązującym prawem.

Założeniem prezentowanego opracowania jest zebranie w pigułce wszystkich wymogów prawnych dotyczących stosowania informatyki w administracji publicznej. Doskonale wiemy jak trudno jest się przedrzeć przez gąszcz przepisów i regulacji prawnych. Postawiliśmy sobie za cel opracowanie dokumentu, który ułatwi Państwu zorientowanie się, czy w swoich urzędach spełniacie wszystkie wymogi a jeśli nie, to jak je spełnić.

Dokument ten nie tylko przedstawia wymagania prawne, ale również podpowiada jak praktycznie spełnić te wymogi.

Dla kogo?

Dokument kierowany jest do kadry zarządzającej oraz do osób bezpośrednio zajmujących się informatyką w urzędach.

Co ja tu znajdę?

Dla każdego wymagania znajdziecie Państwo:

- **podstawę prawną** (*odwołania do uchwał i rozporządzeń, polskich norm, oraz innych dokumentów*),
- **proponowane sposoby na spełnienie wymogów** (*wskazówki i przykłady rozwiązań, przykłady dokumentów, rozwiązań sprzętowych, programowych i organizacyjnych*),
- **inne wymagania, które należy spełnić – w zależności od wybranego rozwiązania,**
- **koszty** (*informacje o cenach urządzeń i cenach innych rozwiązań, jeśli ofertę danego produktu lub usługi można znaleźć na rynku*),

Przytoczone w dokumencie nazwy rozwiązań, urządzeń i oprogramowania, podane zostały, jako przykładowe i nie wyczerpują dostępnych rozwiązań.

Uwagi, pytania, komentarze, kolejne wersje dokumentu.

To pierwsza wersja tego opracowania – chcielibyśmy, aby jego zawartość była wyjściem do publicznej dyskusji, w wyniku której, powstaną kolejne wersje tego dokumentu. Liczymy na komentarze i uwagi wskazujące, co jeszcze powinno znaleźć się w tym dokumencie.

Zachęcamy wszystkich do zadawania pytań i dzielenia się spostrzeżeniami – macie Państwo szansę uzyskać odpowiedzi na nurtujące Was pytania.

W sprawie dokumentu, wszelkich uwag i propozycji tematów, które Państwa zdaniem powinny znaleźć się w kolejnych jego wersjach prosimy o kontakt mailowy:

biuro@podpiselektroniczny.pl

Postaramy się odpowiedzieć na wszelkie pytania.

Jeśli chcielibyście Państwo być powiadomieni o wydaniu kolejnej wersji dokumentu, prosimy na podany wyżej adres przesłać email pt: „**WBIJAP**”.

Publiczna dyskusja

Zapraszamy również do publicznej dyskusji na naszym forum dyskusyjnym w dziale:

Spełnienie wymogów nałożonych przez różne ustawy <http://forum.podpiselektroniczny.pl/forum/index.php?c=7>

Po zapoznaniu się z dokumentem zapraszamy do wypełnienia krótkiej ankiety: <http://forum.podpiselektroniczny.pl/forum/ankieta.aspx>

Poruszanie się po dokumencie

Poszczególne wymogi zostały zamknięte w tabelę mieszczące się na stronie A4.

Każda tabela (wymóg) została podzielona na **3 sekcje**:

Sekcja A – identyfikacja, zawiera:

- nr wymogu, np.: W1,
- nazwę wymogu,
- informację czy wymóg jest obligatoryjny.

Sekcja B – źródła wymogu, przedstawia:

- rodzaj źródła wymogu (akt prawny, norma, wytyczne),
- jego identyfikator, np.: (Dz. U. 2004 nr 100 poz. 1024),
- lokalizację w źródle np.: (§ 4),
- cyfrowy odnośnik do fragmentu znajdującego się w II części niniejszego opracowania,
- nazwę pliku zawierającego pełną treść źródła, (pliki umieszczone są w archiwum zip)
- adres URL dokumentu w Internecie,

Sekcja C – rozwiązania, przedstawia:

- proponowane rozwiązania: minimum oraz zalecane,
- listę innych wymogów, które należy spełnić wybierając dane rozwiązanie (inne wymogi przedstawione w postaci odnośników np.: W2)
- praktyczne rozwiązanie w postaci dokumentu, przykładowego rozwiązania technicznego, organizacyjnego lub programowego wraz z ewentualnymi cenami.

CZĘŚĆ I

WYMAGANIA BEZPIECZEŃSTWA

Sekcja A identyfikacja	Nr karty	Typ wymogu	Nazwa wymogu
	W1	OBLIGATORYJNY	Opracowanie polityki bezpieczeństwa

Sekcja B źródła wymogu	Rodzaj źródła wymogu	Identyfikator źródła	Lokalizacja w źródle	Fragment źródła w części II oprac.	Nazwa pliku zawierającego treść źródła (folder „źródła”)	Adres strony internetowej zawierającej treść źródła
	Akt prawny	Dz. U. 2004 nr 100 poz. 1024	§ 4	5	DZ_U_2004_nr_100_poz_1024.pdf	http://isip.sejm.gov.pl/servlet/Search?todo=open&id=WDU20041001024
	Akt prawny	Dz. U. 2005 nr 212 poz. 1766	§ 3	2	DZ_U_2005_nr_212_poz_1766.pdf	http://isip.sejm.gov.pl/servlet/Search?todo=open&id=WDU20052121766
	Norma ISO	PN-ISO/IEC 17799:2003	3.1.1	6	Brak pliku	Niedostępne publicznie
	Inne	Wytyczne GIODO	-	-	wytyczne_giodo_pb.pdf	http://www.giodo.gov.pl/plik/id_p/778/t/pdf/j/pl/

Sekcja C rozwiązania	Proponowane rozwiązania		Inne wymogi, który należy spełnić	Przykładowe opracowanie, komentarz		
	Minimum	Zalecane		Nr zał.	Nazwa pliku (folder „załączniki”)	Komentarz
	Minimum	<p>Administrator danych obowiązany jest do opracowania w formie pisemnej i wdrożenia polityki bezpieczeństwa.</p> <p>Polityka bezpieczeństwa, zawiera w szczególności:</p> <ul style="list-style-type: none"> wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe; wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych; opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi; sposób przepływu danych pomiędzy poszczególnymi systemami; określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych. <p>Najobszerniejszym źródłem w tym temacie są Wytyczne GIODO. Na ich podstawie powstała przykładowa polityka bezpieczeństwa, będąca załącznikiem nr 3 do tego dokumentu.</p>	<p>Politykę bezpieczeństwa z pozycji minimum można rozszerzyć posiłkując się Polską Normą PN-ISO/IEC 17799:2003 - Technika informatyczna. Praktyczne zasady zarządzania bezpieczeństwem informacji.</p> <p>Koszt zakupu PN: ~ 122 zł PN można jednorazowo przeczytać za pomocą serwisów internetowych – koszt 20% ceny normy. PN w Internecie: http://www.google.pl/search?q=polskie+normy</p>	<p>Lista wspólnych wymogów dla rozwiązania minimum i zalecane:</p> <p>W2 W3 W6 W7 W8 W9 W10 W11</p>	3	zal_1_pb.pdf

Sekcja A identyfikacja	Nr karty	Typ wymogu	Nazwa wymogu
	W2	OBLIGATORYJNY	Opracowanie instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych

Sekcja B źródła wymogu	Rodzaj źródła wymogu	Identyfikator źródła	Lokalizacja w źródle	Fragment źródła w części II oprac.	Nazwa pliku zawierającego treść źródła (folder „źródła”)	Adres strony internetowej zawierającej treść źródła
	Akt prawny	Dz. U. 2004 nr 100 poz. 1024	§ 3, § 5	1	DZ_U_2004_nr_100_poz_1024.pdf	http://isip.sejm.gov.pl/servlet/Search?todo=open&id=VDU20041001024
	Inne	Wytyczne GIODO	-	-	wytyczne_giodo_izsi.pdf	http://www.giodo.gov.pl/plik/id_p/550/t/pdf/fj/pl/

Sekcja C rozwiązania	Proponowane rozwiązania		Inne wymogi, który należy spełnić	Przykładowe opracowanie, komentarz		
	Minimum	<p>W instrukcji, powinny być wskazane systemy informatyczne, których ona dotyczy, ich lokalizacje, stosowane metody dostępu. Powinna obejmować zagadnienia bezpieczeństwa informacji, a w szczególności:</p> <ul style="list-style-type: none"> procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania sposób, miejsce i okres przechowywania: elektronicznych nośników informacji zawierających dane osobowe, kopii zapasowych sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych. <p>W odniesieniu do każdego z wymienionych wyżej punktów, powinno być wskazane odpowiednie dla stosowanych systemów informatycznych zasady postępowania.</p> <p>Najobszerniejszym źródłem w tym temacie są Wytyczne GIODO. Na ich podstawie powstała przykładowa instrukcja zarządzania systemem informatycznym, będąca załącznikiem nr 4 do tego dokumentu.</p>	<p>Lista wymogów dla rozwiązania:</p> <p>W1 W3 W6 W7 W8 W11</p>	Nr zał.	Nazwa pliku (folder „załączniki”)	Komentarz
				4	zal_2_izsi.pdf	Załącznik przedstawia przykładową instrukcję zarządzania systemem informatycznym opracowaną w oparciu o podane akty prawne oraz wytyczne GIODO.

Sekcja A identyfikacja	Nr karty	Typ wymogu	Nazwa wymogu
	W3	OBLIGATORYJNY	Kontrola dostępu do obiektów i pomieszczeń, w których zainstalowane serwery przetwarzające dane osobowe

Sekcja B źródła wymogu	Rodzaj źródła wymogu	Identyfikator źródła	Lokalizacja w źródle	Fragment źródła w części II oprac.	Nazwa pliku zawierającego treść źródła (folder „źródła”)	Adres strony internetowej zawierającej treść źródła
	Akt prawny	Dz. U. 2004 nr 100 poz. 1024	§ 6	12	DZ_U_2004_nr_100_poz_1024.pdf	http://isip.sejm.gov.pl/servlet/Search?todo=open&id=WDU20041001024

Sekcja C rozwiązania	Proponowane rozwiązania		Inne wymogi, który należy spełnić	Przykładowe opracowanie, sprzęt, komentarz		
	Minimum	Rejestr wejść i wyjść – prowadzony w formie papierowej Dostęp do serwerowni mogą mieć tylko osoby upoważnione Upoważnienie powinno być w formie papierowej. Wzmocnione drzwi wejściowe do serwerowni.		W1 W2	Nr zał.	Nazwa pliku (folder „załączniki”)
			5		zal_3_rw.pdf	Przykładowy rejestr wejść i wyjść
	Zalecane	Elektroniczny system rejestracji wejść (karty zbliżeniowe) Dostęp do serwerowni mogą mieć tylko osoby upoważnione Drzwi antywłamaniowe Żaluzje antywłamaniowe	W1 W2	Koszty		Komentarz
System oparty o czytnik Prox 402 Cena: ~ 3000 zł				Dostęp do "serwerowni" przez system kart zbliżeniowych Założenia: <ul style="list-style-type: none"> ▪ kontrolowane wejście i wyjście dla 20 osób, ▪ zapis czasu zdarzeń, ▪ automatyczne domykanie drzwi. 		

Sekcja A identyfikacja	Nr karty	Typ wymogu	Nazwa wymogu
	W4	OBLIGATORYJNY	Sprzętowy moduł bezpieczeństwa HSM (Hardware Security Module)

Sekcja B źródła wymogu	Rodzaj źródła wymogu	Identyfikator źródła	Lokalizacja w źródle	Fragment źródła w części II oprac.	Nazwa pliku zawierającego treść źródła (folder „źródła”)	Adres strony internetowej zawierającej treść źródła
	Akt prawny	Dz. U. 2005 nr 200 poz. 1651	§ 6	3	DZ_U_2005_nr_200_poz_1651.pdf	http://isip.sejm.gov.pl/servlet/Search?todo=open&id=WDU20052001651

Sekcja C rozwiązania	Proponowane rozwiązania		Inne wymogi, który należy spełnić	Przykładowe opracowanie, sprzęt, komentarz,	
	Minimum	<p>Podpisanie umowy z zewnętrzną firmą posiadającą HSM która będzie świadczyć usługę dla urzędu na zasadzie outsourcingu.</p> <p><i>Podpisanie umowy z zewnętrzną firmą jest wygodnym rozwiązaniem. Z urzędu spada obowiązek zapewnienia szczególnych warunków i wymagań, jakie musi spełnić np. pomieszczenie, w którym urządzenie HSM miałyby być zainstalowane. (W5)</i></p>		-	Firma/Koszty
			EC2 Sp. z o.o. / bd		Cena negocjowana indywidualnie
	Zalecane	<p>Zakup własnego HSM (Hardware Security Module).</p> <p><i>Sam zakup urządzenia to nie wszystko. Urząd musi zapewnić dla urządzenia odpowiednie środowisko pracy, wdrożyć procedury i instrukcje zarządzania kluczami, przechowywanymi w module, ponadto należy uzupełnić politykę bezpieczeństwa.</i></p>	W5	Firma/Koszty	Komentarz
Sputnik Software € 3 300 – € 6 500					

Sekcja A identyfikacja	Nr karty	Typ wymogu	Nazwa wymogu
	W5	WARUNKOWY Wymóg ten będzie obligatoryjny, gdy w wymaganiu nr W4 przyjęte zostanie rozwiązanie w wersji zalecanej.	Wyposażenie w instalację alarmową klasy SA3

Sekcja B źródła wymogu	Rodzaj źródła wymogu	Identyfikator źródła	Lokalizacja w źródle	Fragment źródła w części II oprac.	Nazwa pliku zawierającego treść źródła (folder „źródła”)	Adres strony internetowej zawierającej treść źródła
	Akt prawny	Dz. U. 2005 nr 200 poz. 1651	załącznik pkt. 4	4	DZ_U_2005_nr_200_poz_1651.pdf	http://isip.sejm.gov.pl/servlet/Search?todo=open&id=WDU20052001651

Sekcja C rozwiązania	Proponowane rozwiązania		Inne wymogi, który należy spełnić	Przykładowe opracowanie, sprzęt, komentarz,	
	Minimum	Wyposażenie serwerowni w wymaganą instalację alarmową klasy SA3.		-	Firma/Koszty
	Zalecane	Wyposażenie serwerowni w wymaganą instalację alarmową klasy SA3 Wyposażenie serwerowni w drzwi oraz żaluzje antywłamaniowe	-	Firma/Koszty	Komentarz
				Wycena wg firmy Alarm Serwis System alarmowy: 2 500 zł	Centrala alarmowa DSC 5020 klawiatura LCD akumulator 7 Ah sygnalizator akustyczno-optyczny czujki ruchu (PIR), czujka dualna (PIR+MW) kontaktron boczny czujka dymu
			Wycena wg firmy Alarm Serwis System alarmowy: 2 500 zł Drzwi: 2500 zł	Centrala alarmowa DSC 5020 klawiatura LCD akumulator 7 Ah sygnalizator akustyczno-optyczny czujki ruchu (PIR), czujka dualna (PIR+MW) kontaktron boczny czujka dymu	

Sekcja A identyfikacja	Nr karty	Typ wymogu	Nazwa wymogu
	W6	OBLIGATORYJNY	Ochrona przed awariami zasilania

Sekcja B źródła wymogu	Rodzaj źródła wymogu	Identyfikator źródła	Lokalizacja w źródle	Fragment źródła w części II oprac.	Nazwa pliku zawierającego treść źródła (folder „źródła”)	Adres strony internetowej zawierającej treść źródła
	Akt prawny	Dz. U. 2004 nr 100 poz. 1024	załącznik pkt. III.2	7	DZ_U_2004_nr_100_poz_1024.pdf	http://isip.sejm.gov.pl/servlet/Search?todo=open&id=WDU20041001024

Sekcja C rozwiązania	Proponowane rozwiązania		Inne wymogi, który należy spełnić	Przykładowe opracowanie, sprzęt, komentarz,	
	Minimum	Zasilacz awaryjny (UPS) o mocy właściwie dobranej do zasilanego serwera. Zabezpieczenie tylko poprawnego wyłączenia serwera.		Produkt/Koszty	Komentarz
				APC Back-UPS RS 1500VA (BR1500I)	Automatyczną regulacją napięcia na wyjściu (AVR), komunikacja z komputerem poprzez USB. Moc rzeczywista: 865 Wat
				1 200 zł	
	Zalecane	Zasilacze redundantne w serwerze Zasilacz awaryjny (UPS) o mocy tak dobranej do zasilanego serwera, aby podtrzymał pracę serwera i urządzeń sieciowych zachowując ciągłość pracy przez 30 min a następnie w przypadku ciągłego braku zasilania wyłączył serwer.		Ever Eco 1200 Pro CDS Sinus	Kształt napięcia wyjściowego sinusoidalny.
				750 zł	
Produkt/Koszty			Komentarz		
APC Smart-UPS 2200 (SUA2200I)					
3 100 zł					
UPS Ares 3000 RACK	Wersja RACK, przeznaczona do montażu w szafie serwerowej.				
1 700 zł					

Sekcja A identyfikacja	Nr karty	Typ wymogu	Nazwa wymogu
	W7	OBLIGATORYJNY	Ochrona przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego

Sekcja B źródła wymogu	Rodzaj źródła wymogu	Identyfikator źródła	Lokalizacja w źródle	Fragment źródła w części II oprac.	Nazwa pliku zawierającego treść źródła (folder „źródła”)	Adres strony internetowej zawierającej treść źródła
	Akt prawny	Dz. U. 2004 nr 100 poz. 1024	załącznik pkt. III.9	8	DZ_U_2004_nr_100_poz_1024.pdf	http://isip.sejm.gov.pl/servlet/Search?todo=open&id=WDU20041001024

Sekcja C rozwiązania	Proponowane rozwiązania		Inne wymogi, który należy spełnić	Przykładowe opracowanie, sprzęt, komentarz	
	Minimum	<p>Wykluczenie niekontrolowanych źródeł w/w oprogramowania przez:</p> <ul style="list-style-type: none"> zablokowanie dostępu do napędów optycznych i magnetycznych dla wszystkich pracowników. zablokowanie możliwości instalacji i korzystania z pamięci USB (PenDrive) ograniczenie dostępu do Internetu i poczty internetowej tylko do osób które muszą taki dostęp posiadać kontrola antywirusowa poczty elektronicznej na serwerze oprogramowanie antywirusowe na stacjach roboczych i serwerach mających dostęp do Internetu. 		W1 W2	Produkt/Koszty
			NOD32 BOX - licencja 3-letnia 310 zł / licencja		Jeden z najszybszych programów antywirusowych na rynku, chroniący przed wirusami, spyware, adware i phishingiem. Zdobywca rekordowej ilości nagród VB100%. NOD32 przeznaczony jest do ochrony systemów Linux, Windows 95/98/Me/NT/2000/XP/Vista/2003
	Zalecane	<p>Wszystkie warunki wymienione w minimum oraz:</p> <ul style="list-style-type: none"> oprogramowanie antywirusowe (z centralnym zarządzaniem konfiguracją) i personal firewall na wszystkich stacjach roboczych częsta aktualizacja poprawek do systemu operacyjnego ograniczenie zbędnych praw dla użytkowników systemu, przy wykorzystaniu systemów 2000/XP i pracujących w domenie, można w zasadach grup Active Directory ustalić listę dozwolonych plików .exe oraz zablokować dostęp do napędów optycznych i magnetycznych. oprogramowanie antywirusowe na wszystkich serwerach serwery chronione firewallem działającym na poziomie aplikacji można też zastosować sprzętowy system antywirusowy. 	W1 W2	Kaspersky AntiVirus Business 1 200 zł/ licencja	Kaspersky™ Anti-Virus for Windows Server jest kompleksowym systemem ochrony antywirusowej przeznaczonym dla serwerów plików i serwerów aplikacji pracujących pod kontrolą systemu operacyjnego Windows Server.
McAfee VirusScan SMB Edition + (25 użyt.) 3 500 zł				Active VirusScan Small Business Edition chroni zarówno stacje robocze jak i serwery. Protection Pilot - centralne zarządzanie konfiguracją i aktualizacją pakietu.	
			ZyWALL 70 + Karta Turbo dla ZyWall 35 i 70 + subskrybcja AV/IDP na 1 rok 5 600 zł	Filtrowanie pakietów; Stateful Packet Inspection: FTP, SMTP, HTTP, Telnet, SSL, DNS; Wykrywanie i zapobieganie atakom (DoS) dla: Ping of Death, SYN flood, LAND, Teardrop, Smurf, SMTP Blokowanie dostępu do URL/Java/ActiveX/Cookie/Proxy Funkcje dodatkowe: Anti-Virus, IDP, Anti-Spam, Firewall, VPN, Load Balancing, Bandwidth Management, Content Filtering.	

Sekcja A identyfikacja	Nr karty	Typ wymogu	Nazwa wymogu
	W8	OBLIGATORYJNY	Kopie zapasowe

Sekcja B źródła wymogu	Rodzaj źródła wymogu	Identyfikator źródła	Lokalizacja w źródle	Fragment źródła w części II oprac.	Nazwa pliku zawierającego treść źródła (folder „źródła”)	Adres strony internetowej zawierającej treść źródła
	Akt prawny	Dz. U. 2004 nr 100 poz. 1024	§ 5 pkt. 4,5 załącznik IV pkt. 3,4	9	DZ_U_2004_nr_100_poz_1024.pdf	http://isip.sejm.gov.pl/servlet/Search?todo=open&id=WDU20041001024

Sekcja C rozwiązania	Proponowane rozwiązania		Inne wymogi, który należy spełnić	Przykładowe opracowanie, sprzęt, komentarz	
	Minimum	<p>Kopie zapasowe zapisujemy na tanich nośnikach DVD DVD/RW i przechowujemy w innym pomieszczeniu w sejfie (zabezpieczonym przed nieuprawnionym dostępem) lub tworzymy kopie poprzez odosobnioną sieć na serwer w innym bezpiecznym (zabezpieczonym przed nieuprawnionym dostępem) pomieszczeniu.</p> <p>W polityce bezpieczeństwa opisano sposób wykonywania cyklicznych kopii.</p>		W1 W2	Produkt/Koszty
			Nagrywarka DVD/RW 200 zł		Najtańszy napęd i tanie nośnik. Podstawowa wada to mała pojemność 4,7 GB
	Zalecane	<p>Streamer + taśmy (odpowiedniej do potrzeb pojemności) Do robienia kopii używamy oprogramowania umożliwiającego szyfrowanie danych. Taśmy z danymi są przechowywane w innym pomieszczeniu najlepiej w innym budynku. Pomieszczenie do przechowywania kopii powinno być zabezpieczone przed nieuprawnionym dostępem</p> <p>W polityce bezpieczeństwa opisano sposób wykonywania cyklicznych kopii.</p>	W1 W2	Dysk twardej USB 500 GB 1 200 zł	Duża pojemność, łatwo można zautomatyzować backup. Podstawowa wada to cały backup na jednym nośniku (zalecane co jakiś czas zrobić kopię na DVD)
Produkt/Koszty				Komentarz	
				Quantum DAT72 32/72GB SCSI 3 000 zł + 400 zł (10 taśm)	Streamer zewnętrzny interfejs SCSI, pojemność nośników z kompresją 72 GB. Wymagany kontroler SCSI
				HP StorageWorks DAT72 USB Ext Drive 2 500 zł + 400 zł (10 taśm)	Streamer zewnętrzny interfejs USB, pojemność nośników z kompresją 72 GB. Wymagany wolny port USB 2.0

Sekcja A identyfikacja	Nr karty	Typ wymogu	Nazwa wymogu
	W9	OBLIGATORYJNY	Ochrona przed zagrożeniami pochodzącymi z sieci publicznej

Sekcja B źródła wymogu	Rodzaj źródła wymogu	Identyfikator źródła	Lokalizacja w źródle	Fragment źródła w części II oprac.	Nazwa pliku zawierającego treść źródła (folder „źródła”)	Adres strony internetowej zawierającej treść źródła
	Akt prawny	Dz. U. 2004 nr 100 poz. 1024	Zał. C XII 1,2	10	DZ_U_2004_nr_100_poz_1024.pdf	http://isip.sejm.gov.pl/servlet/Search?todo=open&id=WDU20041001024

Sekcja C rozwiązania	Proponowane rozwiązania		Inne wymogi, który należy spełnić	Przykładowe opracowanie, sprzęt, komentarz	
	Minimum	Odpowiednio skonfigurowany router/firewall.	W1	Produkt/Koszty	Komentarz
				Linksys BEFSX41 EtherFast Firewall Router 270 zł	Niedrogi firewall z podstawowymi funkcjami : blokowanie ataków: Ping of Death, SYN Flood, Land Attacks, IP Spoofing i innych ataków typu DoS, dwa kanały VPN szyfrowane DES/3DES, filtry URL (blokują dostęp do adresów zawierających określony tekst), filtry Web (blokowanie proxy, apletów Javy, ActiveX oraz cookies), filtry czasowe (blokowanie dostępu do LAN/WAN w określonych przedziałach czasowych), logi aktywności routera, VPN i firewalla, DMZ
	Zalecane	Odpowiednio skonfigurowany firewall z funkcjami zaawansowanej ochrony lub bardziej zaawansowany sprzęt działający w warstwie aplikacji. Można również zastosować odpowiednio skonfigurowany serwer Proxy.	W1	3COM OfficeConnect Secure VPN Router (3CR860-95) 480 zł	Firewall SPI (Stateful Packet Inspection), zabezpieczenie przed atakami typu DoS, filtrowanie URL, Virtual Server
Produkt/Koszty				Komentarz	
Linksys RV042 700 zł	Router Linksys z obsługą dwóch złączy WAN, firewallem oraz 4-portowym przełącznikiem 10/100. Specyfikacja: Smart Link Backup - użytkownik definiuje łącze główne, drugie staje się łączem zapasowym w momencie awarii pierwszego, priorytetyzacja ruchu na każdym porcie (normalny / wysoki), firewall wykorzystuje mechanizm SPI (Stateful Packet Inspection) śledzący pakiety przechodzące przez router, wykrywa ataki typu DoS (Denial of Service), możliwość definiowania polityk dostępu (Access rules) dla różnych portów TCP/IP w zależności od interfejsu źródłowego oraz adresów IP źródła i celu wraz z możliwością określenia czasu działania danej reguły, blokada dostępu do zabronionych domen w określonym czasie, VPN IPSec DES/3DES, przepuszczanie ruchu szyfrowanego (VPN Pass-thru): IPSec, PPTP, L2TP, tworzenie logów systemowych: w pamięci routera (System / Access / Firewall / VPN), wysyłanie logów na serwer syslog, wysyłanie alarmów na podany adres e-mail, statystyki on-line dla każdego portu: typ, interfejs, status, priorytet.				
ZyWALL 5 Firewall 1 050 zł	Firewall z funkcją serwer/klient VPN. Umożliwia obsługę do 10 bezpiecznych połączeń IPSec VPN (szyfrowanie DES/3DES/AES). Chroni przed atakami typu DoS oraz DDoS. Pozwala na zarządzanie pasmem. Nowością jest możliwość pracy w trybie przezroczystego firewall'a (Transparent Firewall - bridge mode). Umożliwia filtrowanie dostępu do stron WWW w oparciu o zewnętrzną, bazę danych ze zbiorem informacji o stronach.				

Sekcja A identyfikacja	Nr karty	Typ wymogu	Nazwa wymogu
	W10	OBLIGATORYJNY	Ochrona kryptograficzna dla danych wykorzystywanych do uwierzytelniania przy przesyłaniu danych w sieci publicznej

Sekcja B źródła wymogu	Rodzaj źródła wymogu	Identyfikator źródła	Lokalizacja w źródle	Fragment źródła w części II oprac.	Nazwa pliku zawierającego treść źródła (folder „źródła”)	Adres strony internetowej zawierającej treść źródła
	Akt prawny	Dz. U. 2004 nr 100 poz. 1024	zał. pkt. C XIII	11	DZ_U_2004_nr_100_poz_1024.pdf	http://isip.sejm.gov.pl/servlet/Search?todo=open&id=WDU20041001024

Sekcja C rozwiązania	Proponowane rozwiązania		Inne wymogi, który należy spełnić	Przykładowe opracowanie, sprzęt, komentarz	
	Minimum	Połączenie z serwerem z sieci publicznej szyfrowane HTTPS (SSL)		-	Produkt/Koszty
	Zalecane	Połączenie z serwerem z sieci publicznej szyfrowane HTTPS (SSL) Firewall skonfigurowany tak aby odrzucał wszystkie połączenia na porcie 443 niezgodne z HTTPS (SSL)	-	Produkt/Koszty	Komentarz

Sekcja A identyfikacja	Nr karty	Typ wymogu	Nazwa wymogu
	W11	OBLIGATORYJNY	Wysoki poziom bezpieczeństwa

Sekcja B źródła wymogu	Rodzaj źródła wymogu	Identyfikator źródła	Lokalizacja w źródle	Fragment źródła w części II oprac.	Nazwa pliku zawierającego treść źródła (folder „źródła”)	Adres strony internetowej zawierającej treść źródła
	Akt prawny	Dz. U. 2004 nr 100 poz. 1024	§ 6	12	DZ_U_2004_nr_100_poz_1024.pdf	http://isip.sejm.gov.pl/servlet/Search?todo=open&id=WDU20041001024

Sekcja C rozwiązania	Proponowane rozwiązania		Inne wymogi, który należy spełnić	Przykładowe opracowanie, sprzęt, komentarz			
	Minimum	<p>Środki bezpieczeństwa na poziomie wysokim obejmują:</p> <ul style="list-style-type: none"> ▪ Kontrolę przepływu informacji pomiędzy systemem informatycznym administratora danych a siecią publiczną. ▪ Kontrolę działań inicjowanych z sieci publicznej i systemu informatycznego administratora danych. ▪ Środki kryptograficznej ochrony wobec danych wykorzystywanych do uwierzytelnienia, które są przesyłane w sieci publicznej. ▪ Do uwierzytelniania użytkowników używa się hasła, składa się ono co najmniej z 8 znaków. ▪ Zabezpieczenie przed dostępem osób nieuprawnionych. ▪ W systemie informatycznym służącym do przetwarzania danych osobowych stosuje się mechanizmy kontroli dostępu do tych danych. ▪ Dostęp do danych był możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia. ▪ Zabezpieczenia przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego. ▪ Zabezpieczenia przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej. ▪ Zmiana haseł następuje nie rzadziej niż co 30 dni. ▪ Zabezpieczenie się przez wykonywanie kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych. ▪ Kopie zapasowe przechowywane w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem <p>Administrator danych monitoruje wdrożone zabezpieczenia systemu informatycznego</p>		<p>W1 W2 W6 W7 W8 W9 W10</p>	<p>Komentarz</p> <p>Spełnienie postulatów tego wymogu możliwe jest poprzez zastosowanie się do innych wymogów.</p>		
		Zalecane	<p>Wszystkie wytyczne zawarte w „minimum” rozszerzone o wymagania z tabeli W7 „zalecane”.</p> <p>Dodatkowo można również zamiast standardowych haseł zastosować e-tokeny/karty chipowe lub czytniki linii papilarnych.</p>		<table border="1"> <tr> <td>Produkt/Koszty</td> <td>Komentarz</td> </tr> <tr> <td>e-Token USB od 100 do 250 zł /szt.</td> <td>Autoryzacja podczas logowania do systemu.</td> </tr> </table>	Produkt/Koszty	Komentarz
	Produkt/Koszty	Komentarz					
e-Token USB od 100 do 250 zł /szt.	Autoryzacja podczas logowania do systemu.						

CZĘŚĆ II

ŹRÓDŁA WYMOGÓW

1 Dz.U. 2004 nr 100 poz. 1024

<http://isip.sejm.gov.pl/servlet/Search?todo=open&id=WDU20041001024>

§ 3

1. Na dokumentację, o której mowa w § 1 pkt 1, składa się polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, zwana dalej „instrukcją”.
2. Dokumentację, o której mowa w § 1 pkt 1, prowadzi się w formie pisemnej.
3. Dokumentację, o której mowa w § 1 pkt 1, wdraża administrator danych.

§ 5

Instrukcja, o której mowa w § 3 ust. 1, zawiera w szczególności:

- 1) procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności;
 - 2) stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem;
 - 3) procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu;
 - 4) procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania;
 - 5) sposób, miejsce i okres przechowywania:
 - a) elektronicznych nośników informacji zawierających dane osobowe,
 - b) kopii zapasowych, o których mowa w pkt 4,
 - 6) sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, o którym mowa w pkt III ppkt 1 załącznika do rozporządzenia;
 - 7) sposób realizacji wymogów, o których mowa w § 7 ust. 1 pkt 4;
 - 8) procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.
-

2 [Dz.U. 2005 nr 212 poz. 1766](#)

<http://isip.sejm.gov.pl/servlet/Search?todo=open&id=WDU20052121766>

§ 3

1. Podmiot publiczny opracowuje, modyfikuje w zależności od potrzeb oraz wdraża politykę bezpieczeństwa dla systemów teleinformatycznych używanych przez ten podmiot do realizacji zadań publicznych.
2. Przy opracowywaniu polityki bezpieczeństwa, o której mowa w ust. 1, podmiot publiczny powinien uwzględniać postanowienia Polskich Norm z zakresu bezpieczeństwa informacji.

3 [Dz.U. 2005 nr 200 poz. 1651](#)

<http://isip.sejm.gov.pl/servlet/Search?todo=open&id=WDU20052001651>

§ 6

4. System teleinformatyczny wykorzystywany przez podmiot publiczny do wytworzenia urzędowego poświadczenia odbioru powinien spełniać wymagania techniczne i organizacyjne określone w załączniku do rozporządzenia.

Załącznik do rozporządzenia prezesa rady ministrów z dnia 29 września 2005 r. w sprawie warunków organizacyjno-technicznych doręczania dokumentów elektronicznych podmiotom publicznym

1. System teleinformatyczny wykorzystywany przez podmiot publiczny do wytworzenia urzędowego poświadczenia odbioru:
 - 1) zawiera sprzętowy moduł bezpieczeństwa (Hardware Security Module), zwany dalej „HSM” spełniający wymagania normy FIPS 140-2 (*security Requirements for Cryptographic Modules*) poziom 3 lub wyższy, wydanej przez National Institute of Standards and Technology (NIST);

4 [Dz.U. 2005 nr 200 poz. 1651](#)

<http://isip.sejm.gov.pl/servlet/Search?todo=open&id=WDU20052001651>

Załącznika do rozporządzenia Prezesa Rady ministrów z dnia 29 września 2005 r. (poz. 1651)

4. HSM powinno się znajdować w pomieszczeniu zabezpieczonym systemem kontroli dostępu klasy SA3 lub wyższym, zgodnie z Polską Normą.

5 Dz.U. 2004 nr 100 poz. 1024

<http://isip.sejm.gov.pl/servlet/Search?todo=open&id=WDU20041001024>

§ 4

Polityka bezpieczeństwa, o której mowa w § 3 ust. 1, zawiera w szczególności:

- 1) wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe;
- 2) wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych;
- 3) opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi;
- 4) sposób przepływu danych pomiędzy poszczególnymi systemami;
- 5) określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

6 PN-ISO/IEC 17799:2003 Technika Informatyczna. Praktyczne zasady zarządzania bezpieczeństwem informacji

3.1.1 Dokument polityki bezpieczeństwa informacji

7 [Dz.U. 2004 nr 100 poz. 1024](#) <http://isip.sejm.gov.pl/servlet/Search?todo=open&id=WDU20041001024>

Załącznik do rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. (poz. 1024)

III

System informatyczny służący do przetwarzania danych osobowych zabezpiecza się, w szczególności przed:
2) utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej

8 [Dz.U. 2004 nr 100 poz. 1024](#) <http://isip.sejm.gov.pl/servlet/Search?todo=open&id=WDU20041001024>

Załącznik do rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. (poz. 1024)

A. Środki bezpieczeństwa na poziomie podstawowym

III

System informatyczny służący do przetwarzania danych osobowych zabezpiecza się, w szczególności przed:
9.działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego;

9 [Dz.U. 2004 nr 100 poz. 1024](#) <http://isip.sejm.gov.pl/servlet/Search?todo=open&id=WDU20041001024>

§ 5

- 4) procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania;
- 5) sposób, miejsce i okres przechowywania:
 - a) elektronicznych nośników informacji zawierających dane osobowe,
 - b) kopii zapasowych, o których mowa w pkt 4,

Załącznik do rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. (poz. 1024)

IV

3. Dane osobowe przetwarzane w systemie informatycznym zabezpiecza się przez wykonywanie kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych.
4. Kopie zapasowe:
 - a) przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem;
 - b) usuwa się niezwłocznie po ustaniu ich użyteczności.

10 [Dz.U. 2004 nr 100 poz. 1024](#)

<http://isip.sejm.gov.pl/servlet/Search?todo=open&id=WDU20041001024>

Załącznik do rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. (poz. 1024)

C. Środki bezpieczeństwa na poziomie wysokim

XII

1. System informatyczny służący do przetwarzania danych osobowych chroni się przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych lub logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem.
2. W przypadku zastosowania logicznych zabezpieczeń, o których mowa w ust. 1, obejmują one:
 - a) kontrolę przepływu informacji pomiędzy systemem informatycznym administratora danych a siecią publiczną;
 - b) kontrolę działań inicjowanych z sieci publicznej i systemu informatycznego administratora danych.

[Dz.U. 2004 nr 100 poz. 1024](#)

§ 1.

Rozporządzenie określa:

- 1) sposób prowadzenia i zakres dokumentacji opisującej sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną;
- 2) podstawowe warunki techniczne i organizacyjne, jakim powinny odpowiadać urzędnicy i systemy informatyczne służące do przetwarzania danych osobowych;
- 3) wymagania w zakresie odnotowywania udostępniania danych osobowych i bezpieczeństwa przetwarzania danych osobowych.

11 [Dz.U. 2004 nr 100 poz. 1024](#)

<http://isip.sejm.gov.pl/servlet/Search?todo=open&id=WDU20041001024>

Załącznik do rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. (poz. 1024)

XIII

Administrator danych stosuje środki kryptograficznej ochrony wobec danych wykorzystywanych do uwierzytelnienia, które są przesyłane w sieci publicznej.

§ 6

1. Uwzględniając kategorie przetwarzanych danych oraz zagrożenia wprowadza się poziomy bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym:
 - 1) podstawowy;
 - 2) podwyższony;
 - 3) wysoki.
4. Poziom wysoki stosuje się, gdy przynajmniej jedno urządzenie systemu informatycznego, służącego do przetwarzania danych osobowych, połączone jest z siecią publiczną.
5. Opis środków bezpieczeństwa stosowany na poziomach, o których mowa w ust. 1, określa załącznik do rozporządzenia.

Załącznik do rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. (poz. 1024)

A. Środki bezpieczeństwa na poziomie podstawowym

I

Obszar, o którym mowa w § 4 pkt 1 rozporządzenia, zabezpiecza się przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych.

Przebywanie osób nieuprawnionych w obszarze, o którym mowa w § 4 pkt 1 rozporządzenia, jest dopuszczalne za zgodą administratora danych lub w obecności osoby upoważnionej do przetwarzania danych osobowych.

2.

II

1. W systemie informatycznym służącym do przetwarzania danych osobowych stosuje się mechanizmy kontroli dostępu do tych danych.
2. Jeżeli dostęp do danych przetwarzanych w systemie informatycznym posiadają co najmniej dwie osoby, wówczas zapewnia się, aby:
 - a) w systemie tym rejestrowany był dla każdego użytkownika odrębny identyfikator;
 - b) dostęp do danych był możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia.

III

System informatyczny służący do przetwarzania danych osobowych zabezpiecza się, w szczególności przed:

- 1) działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego;
- 2) utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.

IV

1. Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie może być przydzielony innej osobie.
2. W przypadku gdy do uwierzytelniania użytkowników używa się hasła, jego zmiana następuje nie rzadziej niż co 30 dni. Hasło składa się co najmniej z 6 znaków.
3. Dane osobowe przetwarzane w systemie informatycznym zabezpiecza się przez wykonywanie kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych.

4. Kopie zapasowe:

- a) przechowywane w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem;
- b) usuwane niezwłocznie po ustaniu ich użyteczności.

V

Osoba użytkująca komputer przenośny zawierający dane osobowe zachowuje szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem, o którym mowa w § 4 pkt 1 rozporządzenia, w tym stosuje środki ochrony kryptograficznej wobec przetwarzanych danych osobowych.

VI

Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:

- 1) likwidacji — pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie;
- 2) przekazania podmiotowi nieuprawnionemu do przetwarzania danych — pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie;
- 3) naprawy — pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych.

VII

Administrator danych monitoruje wdrożone zabezpieczenia systemu informatycznego

B. Środki bezpieczeństwa na poziomie podwyższonym

VIII

W przypadku gdy do uwierzytelniania użytkowników używa się hasła, składa się ono co najmniej z 8 znaków, zawiera małe i wielkie litery oraz cyfry lub znaki specjalne.

IX

Urządzenia i nośniki zawierające dane osobowe, o których mowa w art. 27 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, przekazywane poza obszar, o którym mowa w § 4 pkt 1 rozporządzenia, zabezpiecza się w sposób zapewniający poufność i integralność tych danych.

X

Instrukcja zarządzania systemem informatycznym, o której mowa w § 5 rozporządzenia, rozszerza się o sposób stosowania środków, o których mowa w pkt IX załącznika.

XI

Administrator danych stosuje na poziomie podwyższonym środki bezpieczeństwa określone w części A załącznika, o ile zasady zawarte w części B nie stanowią inaczej.

C. Środki bezpieczeństwa na poziomie wysokim

XII

1. System informatyczny służący do przetwarzania danych osobowych chroni się przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych lub logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem.

2. W przypadku zastosowania logicznych zabezpieczeń, o których mowa w ust. 1, obejmują one:

- a) kontrolę przepływu informacji pomiędzy systemem informatycznym administratora danych a siecią publiczną;
- b) kontrolę działań inicjowanych z sieci publicznej i systemu informatycznego administratora danych.

XIII

Administrator danych stosuje środki kryptograficznej ochrony wobec danych wykorzystywanych do uwierzytelnienia, które są przesyłane w sieci publicznej.

XIV

Administrator danych stosuje na poziomie wysokim środki bezpieczeństwa, określone w części A i B załącznika, o ile zasady zawarte w części C nie stanowią inaczej.

Wykaz ustaw i rozporządzeń:

[Dz.U. 2005 nr 171 poz. 1433](#)

Rozporządzenie Prezesa Rady Ministrów z dnia 25 sierpnia 2005 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego

[Dz.U. 1999 nr 18 poz. 162](#)

Rozporządzenie Prezesa Rady Ministrów z dnia 25 lutego 1999 r. w sprawie podstawowych wymagań bezpieczeństwa systemów i sieci teleinformatycznych.

[Dz.U. 2004 nr 100 poz. 1024](#)

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. 2005 nr 212 poz. 1766](#)

Rozporządzenie Rady Ministrów z dnia 11 października 2005 r. w sprawie minimalnych wymagań dla systemów teleinformatycznych

[Dz.U. 2001 nr 100 poz. 1087](#)

Ustawa z dnia 25 sierpnia 2001 r. o zmianie ustawy o ochronie danych osobowych.

[Dz.U. 1997 nr 133 poz. 883](#)

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

[Dz.U. 2001 nr 121 poz. 1306](#)

Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 1 października 2001 r. zmieniające rozporządzenie w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

[Dz.U. 1998 nr 80 poz. 521](#)

Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 3 czerwca 1998 r. w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

[Dz.U. 2006 nr 12 poz. 65](#)

Ustawa z dnia 16 grudnia 2005 r. o zmianie ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne

[Dz.U. 2005 nr 64 poz. 565](#)

Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne

[Dz.U. 2005 nr 200 poz. 1651](#)

Rozporządzenie Prezesa Rady Ministrów z dnia 29 września 2005 r. w sprawie warunków organizacyjno-technicznych doręczania dokumentów elektronicznych podmiotom publicznym