Zarządzenie Nr 13
Wojewody Dolnośląskiego
z dnia 8 stycznia 2010 roku

w sprawie: wprowadzenia **Dokumentu Programowego** Polityki Bezpieczeństwa Informacji Dolnośląskiego Urzędu Wojewódzkiego we Wrocławiu

Na podstawie art. 17 ustawy z 23 stycznia 2009r. o wojewodzie i administracji rządowej w województwie (Dz.U. Nr 31, poz. 206) w związku z art. 36 ust. 2 ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz.U. z 2002r. Nr 101, poz. 926 i Nr 153, poz. 1271, z 2004r. Nr 25, poz. 219 i Nr 33, poz. 285, z 2006r. Nr 104, poz. 708 i 711 oraz z 2007r. Nr 165, poz. 1170 i Nr 176, poz. 1238) i rozporządzeniem 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) oraz art.61 ustawy z dnia 22 stycznia 1999r. o ochronie informacji niejawnych (Dz. U. z 2005 r. Nr 196, poz. 1631, z 2006r. Nr 104, poz. 708 i 711, Nr 149, poz. 1078, Nr 218, poz. 1592 i Nr 220, poz. 1600 oraz z 2008r. Nr 171, poz. 1056) i § 8 Regulaminu Dolnośląskiego Urzędu Wojewódzkiego we Wrocławiu zarządza się co następuje:

§ 1

Wprowadzam Dokument Programowy Polityki Bezpieczeństwa Informacji Dolnośląskiego Urzędu Wojewódzkiego we Wrocławiu w brzmieniu stanowiącym załącznik do niniejszego zarządzenia.

§ 2

Przygotowanie Polityk Bezpieczeństwa Grup Informacji oraz procedur, instrukcji i regulaminów, o których mowa w pkt 3 załącznika do niniejszego zarządzenia, stanowiących szczegółowe dokumenty Polityki Bezpieczeństwa Informacji, powierzam Administratorom zasobów informacji wyznaczanym w sposób określony w pkt 2 załącznika do niniejszego zarządzenia.

§ 3

1. Administratorzy zasobów informacji przedstawią przygotowane dokumenty, o których mowa w § 2 zarządzenia w terminie do dnia 30.04.2010r., do zweryfikowania i uzgodnienia Zespołowi ds. opracowania Polityki Bezpieczeństwa Informacji Dolnośląskiego Urzędu Wojewódzkiego we Wrocławiu.
2. Zespół ds. opracowania Polityki Bezpieczeństwa Informacji Dolnośląskiego Urzędu Wojewódzkiego we Wrocławiu w terminie do dnia 30.06.2010r. przedstawi uzgodnione dokumenty do akceptacji Dyrektorowi Generalnemu Dolnośląskiego Urzędu Wojewódzkiego we Wrocławiu.

§ 4

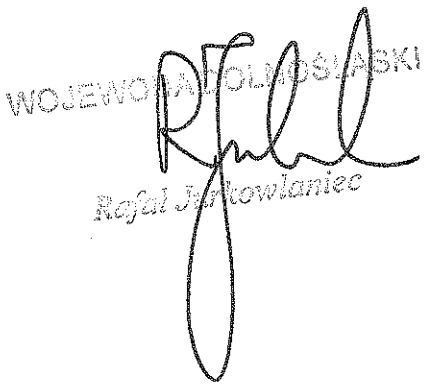
Dokumenty Polityki Bezpieczeństwa Informacji, będą po ich przygotowaniu w sposób wymieniony w paragrafach poprzedzających i akceptacji przez Dyrektora Generalnego Dolnośląskiego Urzędu Wojewódzkiego we Wrocławiu wprowadzane w życie na podstawie zarządzeń Wojewody Dolnośląskiego.

§5

Nadzór nad realizacją niniejszego zarządzenia powierzam Dyrektorowi Generalnemu Dolnośląskiego Urzędu Wojewódzkiego we Wrocławiu.

§ 6

Zarządzenie wchodzi w życie z dniem podpisania.



Załącznik
do Zarządzenia Nr 13
Wojewody Dolnośląskiego
z dnia 8 stycznia 2010 r.

DOKUMENT PROGRAMOWY

POLITYKI BEZPIECZEŃSTWA INFORMACJI DOLNOŚLĄSKIEGO URZĘDU WOJEWÓDZKIEGO WE WROCŁAWIU

Spis treści:

Słownik terminów

Administrator bezpieczeństwa informacji	–	wyznaczona przez administratora danych osoba nadzorująca przestrzeganie zasad ochrony zgodnie z ustawą o ochronie danych osobowych (Dz.U.2002, Nr 101, poz.926, ze zm.).
Administrator zasobu informacji	–	osoba nadzorująca, z upoważnienia Wojewody, przestrzeganie stosowania środków technicznych i organizacyjnych zapewniających ochronę powierzonego mu zasobu informacji, w sposób odpowiedni do zagrożeń oraz kategorii informacji objętej ochroną.
Analiza ryzyka	–	systematyczne wykorzystanie informacji do zidentyfikowania źródeł i oszacowania ryzyka.[1]
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.[2]
Bezpieczeństwo informacji	–	zachowanie poufności, integralności i dostępności informacji.[1]
Dyrektor wydziału	–	należy przez to rozumieć dyrektorów wydziałów i dyrektorów równorzędnych komórek organizacyjnych.[3]
Dostępność	–	właściwość bycia dostępnym i możliwym do wykorzystania na żądanie, w założonym czasie przez kogoś lub coś, kto/co ma do tego prawo.[2]
Incydent związany z bezpieczeństwem informacji	–	jest to pojedyncze zdarzenie lub seria zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo naruszenia obowiązujących procedur wynikających z przyjętej dokumentacji bezpieczeństwa.
Grupa informacji	–	zbiór informacji podlegających ochronie, obejmujących podobne zagadnienia lub dotyczące jednego tematu. Grupa informacji może być określona przepisami prawa.
Integralność	–	integralność danych oraz integralność systemu.[2]
Integralność danych	–	właściwość zapewniająca, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany.[2]
Integralność systemu	–	właściwość polegająca na tym, że system realizuje swoją zamierzoną funkcję w sposób nienaruszony, wolny od nieautoryzowanej manipulacji, celowej lub przypadkowej.[2]
Monitorowanie	–	proces weryfikacji stosowanych metod i zasad bezpieczeństwa oraz kontrola ich przestrzegania.
Naruszenie bezpieczeństwa	–	odstępstwo od obowiązujących procedur postępowania lub bezprawne naruszenie zasobów bez względu na skutki.

Polityka bezpieczeństwa informacji	–	zestaw praw, reguł i praktycznych doświadczeń, regulujących sposób zarządzania, ochrony i dystrybucji informacji wrażliwej wewnątrz określonego systemu, zawartych w „Dokumencie Programowym Polityki Bezpieczeństwa Informacji Dolnośląskiego Urzędu Wojewódzkiego we Wrocławiu", Polityce Bezpieczeństwa Grupy Informacji oraz procedurach, instrukcjach i regulaminach.
Poufność	–	właściwość zapewniająca, że informacja nie jest udostępniana lub ujawniana nieautoryzowanym osobom, podmiotom lub procesom.[2]
Rozliczalność	–	właściwość zapewniająca, że działanie podmiotu (np. użytkownika) mogą być jednoznacznie przypisane tylko temu podmiotowi.[2]
Ryzyko	–	prawdopodobieństwo, że określone zagrożenie w połączeniu z podatnością doprowadzi do utraty, zniszczenia lub ujawnienia zasobów.
Szacowanie ryzyka	–	całościowy proces analizy i oceny ryzyka.[1]
System informatyczny	–	zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
Urząd	–	należy przez to rozumieć Dolnośląski Urząd Wojewódzki we Wrocławiu.[3]
Utrzymanie ciągłości działania	–	zapewnienie, na określonym poziomie, nieprzerwanej realizacji zadań statutowych Urzędu na wypadek wystąpienia incydentu związanego z bezpieczeństwem informacji.
Zagrożenie bezpieczeństwa informacji	–	potencjalna przyczyna niepożądanego incydentu, który może wywołać szkodę w systemie lub organizacji.[1]
Zasób informacji	–	zbiór informacji wytwarzanych, przetwarzanych, przechowywanych i udostępnianych z zastosowaniem infrastruktury Urzędu.

[1] – oznaczono definicje zgodne z Polską Normą PN- ISO/IEC 27001.
[2] – oznaczono definicje zgodne z Polską Normą PN-13335-1.
[3] – oznaczono definicje zgodne ze Statutem Dolnośląskiego Urzędu Wojewódzkiego, załącznik do Zarządzenia Nr 79 Wojewody Dolnośląskiego z dnia 27 maja 2009.

1. Cel polityki bezpieczeństwa informacji

Zapewnienie bezpieczeństwa informacji jest nie tylko normą i koniecznością, ale także obowiązkiem wynikającym z przepisów obowiązującego w Polsce prawa.

Realizacja statutowych zadań Urzędu wymaga, między innymi, efektywnego dostępu do informacji oraz zapewnienia odpowiedniego poziomu bezpieczeństwa informacji. Utrata poufności, integralności, dostępności i autentyczności danych może mieć negatywny wpływ na bieżącą działalność oraz wizerunek Urzędu.

Niniejszy dokument wyraża świadomość Kierownictwa Urzędu w zakresie potrzeb bezpieczeństwa informacji oraz określa podstawowe, przyjęte w tym obszarze cele i strategie.

Polityka Bezpieczeństwa Informacji stanowi zbiór zasad obowiązujących przy wytwarzaniu, przetwarzaniu, przechowywaniu i udostępnianiu informacji.

Polityka Bezpieczeństwa Informacji ma zastosowanie w stosunku do wszystkich informacji, niezależnie od formy jej wytwarzania, przetwarzania, udostępniania i przechowywania (dokumenty papierowe i elektroniczne). Wszelkie informacje wytwarzane, przetwarzane, przechowywane w Urzędzie lub udostępniane przez Urząd, nieoznaczone jako należące do innych podmiotów, stanowią własność Urzędu i podlegają ochronie. Informacje chronione, z uwagi na obowiązujące przepisy prawa i przestrzeganie tajemnic ustawowo chronionych, podlegają ochronie przed nieautoryzowanym: dostępem, modyfikacją lub zniszczeniem.

Polityka Bezpieczeństwa Informacji jest zbiorem zasad i procedur, którym muszą podporządkować się wszystkie osoby posiadające dostęp do zasobów informacyjnych.

Polityka Bezpieczeństwa Informacji dotyczy wszystkich pracowników Urzędu, a także innych osób mających dostęp do informacji chronionej w Urzędzie (np.: pracowników firm zewnętrznych realizujących prace na rzecz Urzędu, stażystów, praktykantów).

Polityka Bezpieczeństwa Informacji określa zasady ochrony zasobów informacyjnych oraz infrastruktury Urzędu służącej do przetwarzania informacji.

Celem Polityki Bezpieczeństwa Informacji jest zapewnienie właściwej ochrony zasobów informacyjnych w Urzędzie, maksymalne ograniczenie wielkości ryzyka dla chronionych zasobów oraz zapewnienie gotowości do podejmowania działań zmierzających do utrzymania ciągłości działania Urzędu w sytuacjach zagrożeń dla bezpieczeństwa informacji.

2. Odpowiedzialność za bezpieczeństwo informacji

Za bezpieczeństwo informacji zgromadzonych w zasobach informacyjnych Urzędu odpowiada administrator tych danych, tj. Wojewoda Dolnośląski.

Dyrektor Generalny Urzędu oraz dyrektorzy wydziałów, odpowiadają za wdrożenie i utrzymanie Polityki Bezpieczeństwa Informacji.

Dyrektor Generalny Urzędu powołuje Zespół do Opracowania, Wdrożenia Polityki Bezpieczeństwa Informacji oraz Zespół ds. Monitorowania Zagrożeń i Utrzymania Polityki Bezpieczeństwa Informacji. W przypadku naruszenia zasad bezpieczeństwa informacji, Zespół ds. Monitorowania Zagrożeń i Utrzymania Polityki Bezpieczeństwa Informacji zobowiązany jest do natychmiastowego podjęcia działań określonych w odpowiednich procedurach.

Administratorów zasobów informacji wyznacza Wojewoda na wniosek dyrektorów wydziałów, w których zarządza się danym zasobem informacji. Administratorzy zasobów informacji odpowiadają za opracowanie i utrzymanie Polityki Bezpieczeństwa Grupy Informacji oraz opracowanie i aktualizację procedur, instrukcji i regulaminów. Tworząc dokumenty, związane

z bezpieczeństwem zasobu informatycznego, administratorzy zasobów informacji współpracują z Biurem Informatyki.

Pełnomocnik ds. Ochrony Informacji Niejawnych odpowiada za zapewnienie przestrzegania przepisów o ochronie informacji niejawnych w Urzędzie.

Administrator Bezpieczeństwa Informacji odpowiada za nadzór nad opracowaniem i utrzymaniem Polityki Bezpieczeństwa Grupy Informacji oraz procedur, instrukcji i regulaminów z zakresu danych osobowych.

Administrator Systemu odpowiada za funkcjonowanie systemów lub sieci teleinformatycznych oraz za przestrzeganie zasad i wymagań bezpieczeństwa systemów i sieci teleinformatycznych dla informacji niejawnych.

Inspektor Bezpieczeństwa Teleinformatycznego odpowiada za bieżącą kontrolę zgodności funkcjonowania sieci lub systemu teleinformatycznego ze szczególnymi wymaganiami bezpieczeństwa oraz kontrolę przestrzegania procedur bezpiecznej eksploatacji dla informacji niejawnych.

Pełnomocnika ds. Ochrony Informacji Niejawnych powołuje Wojewoda Dolnośląski.

Administratora Bezpieczeństwa Informacji, Administratora Systemu oraz Inspektora Bezpieczeństwa Teleinformatycznego wyznacza Wojewoda Dolnośląski.

Wszyscy pracownicy są zobowiązani, odpowiednio do zakresu swoich obowiązków i zajmowanych stanowisk, do przestrzegania Polityki Bezpieczeństwa Informacji, a zwłaszcza zasad zawartych w procedurach, regulaminach i instrukcjach.

Pracownicy w szczególności zobowiązani są do przestrzegania:

- zasad ochrony informacji prawnie chronionej,
- procedur eksploatacji systemów informatycznych,
- procedur opisujących zasady użytkowania sprzętu komputerowego stacjonarnego i przenośnego,
- zasad korzystania z Internetu i poczty elektronicznej,
- procedur ochrony antywirusowej,
- zasad tworzenia zapasowych kopii bezpieczeństwa,
- zakazu korzystania z nielegalnego oprogramowania,
- zakazu samowolnego instalowania jakiegokolwiek oprogramowania i przemieszczania sprzętu informatycznego bez zgody Biura Organizacyjno-Administracyjnego i Biura Informatyki.

Całokształt obsługi informatycznej i utrzymania sieci w Urzędzie realizuje Biuro Informatyki w ramach zadań statutowych.

3. Struktura dokumentu Polityki Bezpieczeństwa Informacji

Dokument Programowy Polityki Bezpieczeństwa Informacji, określa podstawowe zasady zarządzania bezpieczeństwem informacji na poziomie jednostki organizacyjnej – Urzędu.

Kwestie związane z bezpieczeństwem informacji są rozwiązywane na kolejnych poziomach szczegółowości:

- poziom grupy informacji występujących w Urzędzie

- poziom procedur, instrukcji i regulaminów.

Polityka Bezpieczeństwa Grupy Informacji odzwierciedla zasady bezpieczeństwa i zarządzania, wynikające z Polityki Bezpieczeństwa Informacji Urzędu oraz zasady wynikające ze specyfiki danej grupy informacji (np.: dane osobowe, finansowo-księgowe, informacje niejawne).

Procedury, instrukcje i regulaminy określają szczegółowe zasady korzystania z zasobów informacyjnych Urzędu, użytkowania systemów informatycznych i infrastruktury informatycznej w Dolnośląskim Urzędzie Wojewódzkim.

Polityka Bezpieczeństwa Informacji musi być opracowana zgodnie ze Statutem i Regulaminem Urzędu. Definicje i terminy używane w Polityce Bezpieczeństwa Informacji muszą być jednorodne, zgodne z zasobem pojęciowym określonym w stosownych uregulowaniach prawnych, oraz z zasobem pojęciowym określonym w Dokumencie Programowym Polityki Bezpieczeństwa Informacji.

4. Sposoby realizacji celów

Realizując Politykę Bezpieczeństwa Informacji Urząd utrzymuje zabezpieczenia wynikające z przepisów prawa i polskich norm, adekwatne do oszacowanego ryzyka. Bezpieczeństwo informacji zapewnione jest poprzez:

- opracowywanie i aktualizację dokumentów polityki bezpieczeństwa i szczegółowych procedur,
- zgodne z obowiązującym prawem i dokumentacją bezpieczeństwa wykonywanie obowiązków przez administratorów zasobów informacji, którzy przeprowadzają również szacowanie ryzyka,
- kształtowanie świadomości pracowników w zakresie bezpieczeństwa informacji, poprzez zapewnienie im dostępu do szkoleń z tego zakresu,
- wykorzystywanie systemów i sieci teleinformatycznych minimalizujących ryzyko towarzyszące wytwarzaniu, przetwarzaniu, przechowywaniu i udostępnianiu informacji,
- monitorowanie zagrożeń i raportowanie incydentów związanych z bezpieczeństwem informacji.

Bezpieczeństwo informacji jest procesem ciągłym i dynamicznym, wymagającym stałego nadzoru i przystosowywania się do zmiennych warunków otoczenia. Musi być na bieżąco analizowane w aspekcie organizacyjnym, technicznym i prawnym.

5. Sankcje za naruszenie zasad bezpieczeństwa informacji

Nieprzestrzeganie zasad zawartych w dokumentach Polityki Bezpieczeństwa Informacji Urzędu, jest naruszeniem obowiązków pracowniczych i skutkować będzie pociągnięciem do odpowiedzialności dyscyplinarnej wynikającej z właściwych przepisów prawa. W razie ciężkiego naruszenia obowiązków pracowniczych może skutkować rozwiązaniem stosunku pracy na podstawie art.52 kodeksu pracy.

Ponadto, naruszenie zasad ochrony informacji może powodować pociągnięcie do odpowiedzialności karnej wynikającej z przepisów:

- ustawy o ochronie danych osobowych,
- kodeksu karnego dotyczących przestępstw przeciwko ochronie informacji,
- chroniących tajemnice zawodowe.