Zarządzenie Nr 88/14
Starosty Stargardzkiego
z dnia 16 kwietnia 2014r.

w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji

Podstawą niniejszego zarządzenia jest art. 34 ust 1 ustawy z dnia 5 czerwca 1998r. o samorządzie powiatowym (Dz. U. z 2013 r. poz. 595 z późn.zm.), art. 36 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. nr 101, poz. 926, z późn. zm.) oraz 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).

§ 1. 1. Wprowadza się do stosowania Politykę Bezpieczeństwa Informacji w Powiatowym Ośrodku Dokumentacji Geodezyjnej i Kartograficznej w Stargardzie Szczecińskim

2. Polityka Bezpieczeństwa Informacji, o której mowa w ust. 1 stanowi załącznik do niniejszego zarządzenia.

§ 2. Wykonanie zarządzenia powierza się Dyrektorowi Powiatowego Ośrodka Dokumentacji Geodezyjnej i Kartograficznej w Stargardzie Szczecińskim.

§ 3. Traci moc Zarządzenie nr 49/05 Starosty Stargardzkiego z dnia 28 grudnia 2005r.w sprawie ustalenia polityki bezpieczeństwa danych osobowych (...).

§ 4. Zarządzenie wchodzi w życie z dniem podpisania.

STAROSTA
Waldemar Gil

załącznik
do Zarządzenia Nr 88/14
Starosty Stargardzkiego
z dnia 16 kwietnia 2014 r.

Powiatowy Ośrodek Dokumentacji Geodezyjnej i Kartograficznej
w Stargardzie Szczecińskim

Polityka bezpieczeństwa informacji

Definicje

Urząd - Powiatowy Ośrodek Dokumentacji Geodezyjnej i Kartograficznej w Stargardzie Szczecińskim, z siedzibą przy ulicy Rynek Staromiejski 5.

Bezpieczeństwo informacji - zachowanie poufności, integralności i dostępności informacji; dodatkowo, mogą być brane pod uwagę inne własności, takie jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność [PN ISO/IEC 17799:2007]

Przetwarzanie danych – wszelkie operacje wykonywane na danych, w szczególności: zbieranie, utrwalanie, przechowywanie, opracowanie, usuwanie i zmienianie danych.

Ryzyko - prawdopodobieństwo wykorzystania określonej podatności systemu na istniejące w danym środowisku zagrożenia potencjalna sytuacja, w której dane zagrożenie wykorzysta podatności aktywów lub grupy aktywów, co spowoduje szkodę dla organizacji. Ryzyko jest funkcją prawdopodobieństwa zdarzenia i jego konsekwencji [PN ISO/IEC 27005:2010];

Polityka

Cel wdrożenia

Celem niniejszej Polityki Bezpieczeństwa Informacji (PBI) jest określenie zasad zarządzania bezpieczeństwem informacji w związku z eksploatacją zasobów informacyjnych, w celu:

- zapewnienia ochrony informacji przed nieautoryzowanym dostępem, zmianą, utratą, uszkodzeniem, zniszczeniem lub zatajeniem,
- minimalizacji ryzyka związanego z przetwarzaniem informacji w Urzędzie,
- zapewnienia zgodności z obowiązującymi przepisami prawa,
- zaangażowania wszystkich pracowników w procesy ochrony informacji.

Odbiorcy

PBI odnosi się do wszystkich pracowników Urzędu niezależnie od formy zatrudnienia, jak również do podmiotów zewnętrznych realizujących zadania na rzecz Urzędu lub współpracujących z Urzędem na podstawie stosownych umów i porozumień.

Zakres stosowania

PBI stosuje się do wszelkich informacji przetwarzanych w Urzędzie.

- W zakresie ochrony danych osobowych PBI pozostaje zgodna z aktami wykonawczymi do Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2002 r. Nr 101 poz. 926, z późn. zm.), w tym zapisy PBI oraz innych dokumentów zależnych pozostają spójne z Polityką Bezpieczeństwa i Instrukcją Zarządzania Systemem Informatycznym Powiatowego Ośrodka Dokumentacji Geodezyjnej i Kartograficznej wprowadzonymi przez Starostę Stargardzkiego.

PBI nie odnosi się do ochrony informacji niejawnych w rozumieniu ustawy o ochronie informacji niejawnych z 5 sierpnia 2010 roku (Dz. U. z 2010 r. nr 182, poz. 1228).

Deklaracja

Kierownictwo Urzędu zobowiązuje się do podejmowania wszystkich niezbędnych działań mających na celu zabezpieczenie informacji, jako zasobu podlegającego ochronie prawnej i niezbędnej do prawidłowego oraz sprawnego funkcjonowania Urzędu. W szczególności Kierownictwo:

- zapewnia widoczne wsparcie dla inicjatyw z zakresu bezpieczeństwa informacji,
- zapewnia środki potrzebne do zapewnienia bezpieczeństwa informacji,
- wyznacza zakresy odpowiedzialności związane z bezpieczeństwem informacji,
- podejmuje działania utrzymujące świadomość w zakresie bezpieczeństwa informacji.

Organizacja bezpieczeństwa

Organizacja bezpieczeństwa informacji w Urzędzie została oparta o następujące filary:

- koordynację zadań bezpieczeństwa realizowanej przez Dyrektora Urzędu,
- specjalizowane doradztwo w dziedzinie bezpieczeństwa informacji uzyskiwane w miarę potrzeb i świadczone przez konsultantów zewnętrznych,
- niezależne przeglądy i audyty bezpieczeństwa.

Prywatność i zasady monitorowania

Wszelkie informacje przetwarzane przy użyciu sprzętu komputerowego Urzędu nie mogą być uznane za prywatne, a Urząd zastrzega sobie prawo do ich wglądu i monitorowania z zachowaniem pełnej dbałości o ich poufność i integralność. Powyższe ma na celu zachowanie ciągłości działania procesów Urzędu oraz ochronę przed wyciekiem informacji.

Ryzyko

Kierownictwo Urzędu dokonuje bieżącej oceny ryzyka i na tej podstawie podejmuje decyzje w zakresie wdrożenia nowych zabezpieczeń skutkujących jego minimalizacją.

Obowiązek ochrony

Obowiązek ochrony zasobów informacyjnych należących do Urzędu spoczywa na każdym pracowniku niezależnie od formy zatrudnienia. Obowiązek ochrony trwa również po ustaniu stosunku pracy lub innego stosunku prawnego, na podstawie którego była wykonywana praca na rzecz Urzędu.

W przypadku realizacji zadań przez podmioty zewnętrzne obowiązek ochrony zasobów informacyjnych regulowany jest w ramach zawartych z nimi umów.

Klasyfikacja informacji

Stosuje się zasadę, według której wszystkie dane przetwarzane w Urzędzie podlegają ochronie, chyba że Kierownictwo Urzędu nie podejmie decyzji o wyłączeniu spod ochrony określonego typu lub zbioru informacji.

Egzekwowanie przestrzegania zasad

W przypadku pracowników egzekwowanie przepisów PBI będzie odbywać się na podstawie odpowiednich przepisów prawa, w szczególności kodeksu pracy - ustawa z dnia 26 czerwca 1974 r. kodeks pracy (Dz. U. z 1998 r. nr 21 poz. 94 z późn. zm.).

W przypadku podmiotów zewnętrznych podstawą egzekwowania przestrzegania zasad ochrony informacji są przepisy prawa oraz lub stosowne zapisy umowach.

Zasady udostępniania PBI

Dokument PBI jest dokumentem jawnym (nie podlega ochronie). Intencja Kierownictwa Urzędu jest zaznajomienie i stosowanie przez wszystkich pracowników oraz podmiotów zewnętrznych regulacji określonych w PBI.

Podstawowe zasady ochrony

Do podstawowych zasad ochrony stosowanych w Urzędzie należą:

- **Zasada przywilejów koniecznych** - każdy użytkownik systemu informacyjnego i jego zasobu posiada prawa ograniczone wyłącznie do tych, które są niezbędne i konieczne do wykonywania powierzonych mu zadań.
- **Zasada usług koniecznych** - zakres dostępnych usług w ramach systemu jest ograniczony tylko do tych, które są konieczne do prawidłowego funkcjonowania firmy.
- **Zasada ubezpieczania zabezpieczeń** - konieczne jest stosowanie wielowarstwowych zabezpieczeń, które ubezpieczają się wzajemnie.
- **Zasada odpowiedzialności** - za utrzymywanie właściwego poziomu bezpieczeństwa poszczególnych elementów systemu informacyjnego i jego zasobu odpowiadają konkretne osoby, które mają świadomość tego, za co są odpowiedzialne i jakie konsekwencje poniosą, jeżeli zaniedbają swoje obowiązki.
- **Zasada świadomości** - wszyscy użytkownicy systemu informacyjnego wraz z jego zasobem są świadomi konieczności ochrony systemu i wykorzystywanych zasobów. Bezpieczeństwo systemu zależy w dużej mierze od bezpośredniego świadomego zaangażowania każdego pracownika organizacji.
- **Zasada najsłabszego ogniwa** - poziom bezpieczeństwa systemu informacyjnego wyznacza najsłabszy (najmniej zabezpieczony) element tego systemu.

Przeglądy PBI

Aby zapewnić ciągłą przydatność, adekwatność i skuteczność, PBI podlega regularnym przeglądom w zaplanowanych odstępach czasu (nie rzadziej niż raz do roku).

Utrzymanie PBI

Dokument PBI może podlegać modyfikacji na skutek:

- identyfikacji nowych podatności lub pojawieniu się nowych zagrożeń,
- zmian w obowiązujących przepisach prawa,
- zmian organizacyjnych w Urzędzie,
- wydania zaleceń poaudytowych.

Zasady szczegółowe dot. ochrony danych osobowych

- Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe jest dokumentem poufnym i stanowi załącznik „A" do niniejszej polityki bezpieczeństwa.
- Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych zbiorów jest dokumentem poufnym i stanowi załącznik „B" do niniejszej polityki bezpieczeństwa.
- Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi jest dokumentem poufnym i stanowi załącznik „C" do niniejszej polityki bezpieczeństwa.
- Opis sposobu przepływu danych pomiędzy poszczególnymi systemami jest dokumentem poufnym i stanowi załącznik „D" do niniejszej polityki bezpieczeństwa.
- Za utrzymanie dokumentacji dot. zbiorów danych osobowych, o której mowa powyżej odpowiada osoba wyznaczona przez Dyrektora Urzędu.
- Środki techniczne i organizacje niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych zostały określone w dokumentach powiązanych.

Dokumenty powiązane

„Powiatowy Ośrodek Dokumentacji Geodezyjnej i Kartograficznej - Zasady Zarządzania Bezpieczeństwem Informacji"

STAROSTA
Waldemar Gil