ZARZĄDZENIE NR 482/18
BURMISTRZA MIASTA BIELSK PODLASKI

z dnia 12 stycznia 2018 r.

w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji dla Urzędu Miasta Bielsk Podlaski

Na podstawie art. 30 ust. 1 ustawy z dnia 8marca 1990 r. o samorządzie gminnym (Dz. U. z 2017 r. poz 1875, poz. 2232) oraz § 20 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2010 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (t.j. Dz. U. z 2017 r. poz. 2247) zarządza się, co następuje:

Rozdział 1.
Postanowienia ogólne

§ 1.

Wprowadza się Politykę Bezpieczeństwa Informacji dla Urzędu Miasta Bielsk Podlaski.

§ 2.

System Zarządzania Bezpieczeństwem Informacji (SZBI) jest systemem zarządzania odnoszącym się do ustanawiania, wdrażania, eksploatacji, monitorowania, utrzymywania i doskonalenia bezpieczeństwa informacji;

§ 3.

1. Bezpieczeństwo informacji oraz systemów, w których są one przetwarzane jest jednym z kluczowych elementów zapewniających realizację zadań Urzędu. Utrata poufności, integralności, dostępności, autentyczności lub niezawodności może mieć negatywny wpływ na bieżącą działalność oraz wizerunek Urzędu.

2. Polityka Bezpieczeństwa Informacji, zwana dalej PBI, jest podstawowym dokumentem, który określa wymagania i zasady ochrony posiadanych informacji w celu zapewnienia odpowiedniego poziomu bezpieczeństwa w tym zakresie.

Rozdział 2.
Cel i zakres Polityki Bezpieczeństwa Informacji

§ 4.

Celem PBI, jest określenie kierunków działań oraz zapewnienie bezpieczeństwa przetwarzania i przechowywania informacji oraz taki opis struktury dokumentacji SZBI funkcjonującego w Urzędzie, aby zapewnić właściwą ochronę zasobów informacyjnych w referatach Urzędu. Przez bezpieczeństwo informacji należy rozumieć:

- poufność;
- dostępność;
- integralność.

§ 5.

Zakres PBI Urzędu obejmuje:

1) wszystkie systemy informatyczne Urzędu;

2) wszystkie pomieszczenia Urzędu, w których są przetwarzane informacje;

3) wszystkich pracowników Urzędu, stażystów i inne osoby mające dostęp do informacji przetwarzanych w Urzędzie (np. pracowników firm zewnętrznych realizujących prace na rzecz Urzędu w ramach zawartych umów);

4) wszystkie informacje, niezależnie od formy, w jakiej są przechowywane (papierowej, elektronicznej i innej) z wyjątkiem informacji niejawnych, których ochrona uregulowana jest odrębnymi regulacjami prawnymi.

Rozdział 3.
System Zarządzania Bezpieczeństwem Informacji

§ 6.

Głównymi celami SZBI, są:

1) zapewnienie zgodności działań z obowiązującymi wymaganiami prawnymi;

2) ochrona systemów przetwarzania informacji przed nieuprawnionym dostępem bądź zniszczeniem;

3) zmniejszanie ryzyka utraty informacji do poziomu akceptowalnego;

4) zaangażowanie wszystkich pracowników Urzędu w ochronę informacji.

§ 7.

1. Wprowadzony SZBI uwzględnia procesy utrzymania odpowiedniego poziomu bezpieczeństwa w tym:

   1) zarządzania ryzykiem;

   2) zarządzania dostępem do zasobów;

   3) monitorowania poziomu bezpieczeństwa;

   4) zarządzania incydentem;

   5) nadzoru nad dokumentacją SZBI.

2. Dla utrzymania odpowiedniego poziomu bezpieczeństwa informacji istotne jest:

   1) systematyczne szkolenie oraz podnoszenie kwalifikacji zawodowych pracowników (w szczególności dotyczy to informatyków i członków zespołu ds. bezpieczeństwa informacji);

   2) okresowe wykonywanie przeglądów Polityki Bezpieczeństwa Informacji.

§ 8.

W Urzędzie odpowiedzialność za bezpieczeństwo informacji ponoszą:

1) Burmistrz Miasta Bielsk Podlaski, zwany dalej Burmistrzem, odpowiada za ustanowienie wdrożenie, eksploatowanie, monitorowanie, przeglądanie, utrzymywanie i doskonalenie SZBI;

2) Administrator Bezpieczeństwa Informacji, zwany dalej ABI, nadzoruje przestrzeganie zasad ochrony przetwarzanych w Urzędzie danych osobowych, oraz sprawuje nadzór nad opracowanymi w tym celu dokumentami;

3) kierownicy referatów Urzędu odpowiadają za przestrzeganie, przez podległych pracowników, zasad i obowiązków związanych z ochroną informacji na stanowiskach pracy oraz zapewnienie odpowiedniego poziomu wiedzy w zakresie przepisów prawa oraz wewnętrznych zasad obowiązujących w Urzędzie dotyczących ochrony informacji;

4) informatycy odpowiadają za funkcjonowanie systemów i sieci teleinformatycznych, realizację zadań związanych z zarządzaniem systemem teleinformatycznym Urzędu, w tym za zabezpieczenie sieci komputerowej tzn. wdrażanie stosownych środków administracyjnych, technicznych i fizycznych w celu zabezpieczenia zasobów infrastruktury teleinformatycznej oraz ochrony danych przed nieuprawnioną modyfikacją, zniszczeniem, dostępem i ujawnieniem, a także ich utratą, ponadto są odpowiedzialni za opracowanie, aktualizację procedur lub instrukcji systemów informatycznych.

5) wszyscy pracownicy Urzędu ponoszą odpowiedzialność za bezpieczeństwo informacji zgodnie z posiadanymi zakresami obowiązków, ponadto każdy pracownik obowiązany jest dbać o bezpieczeństwo powierzonych mu do przetwarzania informacji zgodnie z obowiązującymi przepisami prawa oraz przepisami wewnętrznymi Urzędu.

§ 9.

Dobiera się zabezpieczenia fizyczne, techniczne i organizacyjne odpowiednio do wymagań prawnych i wyników analizy ryzyka dla bezpieczeństwa informacji. Zabezpieczenia fizyczne, techniczne i organizacyjne uzupełniają się wzajemnie zapewniając wspólnie wymagany poziom bezpieczeństwa informacji.

§ 10.

Nieprzestrzeganie zasad zawartych w dokumentach SZBI Urzędu, jest naruszeniem obowiązków pracowniczych i może pociągnąć za sobą skutki dyscyplinarne oraz spowodować pociągnięcie do odpowiedzialności wynikającej z przepisów prawa, w szczególności Kodeksu Pracy, Ustawy o Ochronie Danych Osobowych.

§ 11.

1. Do zapoznania się z PBI oraz zobowiązaniem się do jej stosowania zobowiązana jest kadra kierownicza oraz pracownicy.

2. Każdy pracownik, stażysta, praktykant podpisuje oświadczenie o stosowaniu się do zasad PBI.

3. Referat Organizacyjno-Gospodarczy przekazuje do zapoznania się nowo zatrudnionym pracownikom PBI oraz mając na względzie zakres czynności pracownika wybrane dokumenty SZBI.

4. Zgodnie z postanowieniami PBI w umowach z podmiotami, które otrzymały fizyczny dostęp do zasobów Urzędu stosuje się odpowiednie zapisy dotyczące poufności.

5. Dokumentacja SZBI powinna być przeglądana i weryfikowana:

1) nie rzadziej niż raz w roku;

2) na polecenie Burmistrza;

3) w przypadku wystąpienia poważnych incydentów związanych z bezpieczeństwem informacji;

4) w celu realizacji zaleceń wynikających z przeprowadzonych audytów i kontroli;

5) w przypadku wejścia w życie nowych przepisów dotyczących bezpieczeństwa informacji;

6) w przypadku poważnych modyfikacji infrastruktury teleinformatycznej;

7) w przypadku zawarcia umów, z których wynikają zobowiązania związane z bezpieczeństwem informacji.

6. Zespół do spraw bezpieczeństwa dokonuje analizy dokumentacji SZBI podczas okresowych przeglądów, wykonywanych nie później niż do końca marca każdego roku, oraz w przypadku sytuacji wymienionych w ust. 3. Zmienione dokumenty są uzgadniane z Sekretarz Miasta i zatwierdzane przez Burmistrza Miasta Bielsk Podlaski.

7. W skład zespołu ds. Bezpieczeństwa Informacji, powoływanego zarządzeniem Burmistrza wchodzą:

1) ABI;

2) Informatycy;

3) Kierownik Referatu Zarządzania Kryzysowego;

4) Pracownik służby BHP.

5) Kierownik Referatu Organizacyjno-Gospodarczego.

§ 12.

Na SZBI składaja się następująca dokumentacja:

1) Dokument nr 1 SZBI - Polityka bezpieczeństwa danych osobowych w Urzędzie Miasta Bielsk Podlaski;

2) Dokument nr 2 SZBI - Instrukcja zarządzania systemem informatycznym;

3) Dokument nr 3 SZBI - Procedura nadawania, zarządzania i użytkowania uprawnieniami do systemów teleinformatycznych;

4) Dokument nr 4 SZBI - Procedura oceny i zarządzania ryzykiem w obszarze ochrony informacji;

5) Dokument nr 5 SZBI - Zasada czystego biurka - zasady związane z zapewnieniem bezpieczeństwa informacji podczas wykonywania obowiązków służbowych;

6) Dokument nr 6 SZBI - Procedura postępowania z kluczami i alarmami;

7) Dokument nr 7 SZBI - Standard stacji roboczej;

8) Dokument nr 8 SZBI - Procedura testowania i wymiany akumulatorów w urządzeniach UPS;

9) Dokument nr 9 SZBI - Regulamin korzystania z pamięci zewnętrznych i urządzeń mobilnych.

§ 13.

Informacje podlegają ochronie zgodnie z następującymi wymogami prawa:

1) Ustawa z dnia 17 lutego 2005 roku o informatyzacji działalności podmiotów realizujących zadania publiczne;

2) Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych;

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

4) 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 w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.

§ 14.

Traci moc Zarządzenie Nr 269/16 Burmistrza Miasta z dnia 26 sierpnia 2016 r. w sprawie wprowadzenia w życie „Polityki bezpieczeństwa danych osobowych w Urzędzie Miasta Bielsk Podlaski" oraz „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miasta Bielsk Podlaski".

§ 15.

Zarządzenie wchodzi w życie z dniem podpisania.

BURMISTRZ MIASTA

Jarosław Borowski

Od strony formalno-prawnej i redakcyjnej bez zastrzeżeń
sp. Urszula Curlilla
podpis