

ZARZĄDZENIE NR 599/22
BURMISTRZA MIASTA BIELSK PODLASKI

z dnia 8 sierpnia 2022 r.

w sprawie wprowadzenia Systemu Zarządzania Bezpieczeństwem Informacji Urzędu Miasta Bielsk Podlaski

Na podstawie art. 30 ust. 1 i art. 33 ust. 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (t.j. Dz. U. z 2022 r. poz. 559 z późn. zm.), art. 24 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U.UE.L.2016.119.1 z późn. zm.), art. 13 ust. 1 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j. Dz. U. z 2021 r. poz. 2070 z późn. zm.) 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:

§ 1.

Burmistrz Miasta Bielsk Podlaski - jako kierownik Urzędu podejmuje wszelkie działania mające na celu zapewnienie bezpieczeństwa informacji w Urzędzie Miasta Bielsk Podlaski, zapewnienie zasobów na realizację działań i niżej określonych celów oraz przestrzeganie przez pracowników procedur zapewniających właściwą ochronę zasobów informacyjnych w referatach Urzędu.

§ 2.

Wprowadza się System Zarządzania Bezpieczeństwem Informacji Urzędu Miasta Bielsk Podlaski, zwany dalej SZBI.

§ 3.

SZBI służy do ustanawiania, wdrażania, eksploatacji, monitorowania, utrzymywania i doskonalenia bezpieczeństwa informacji. SZBI jest częścią całościowego systemu zarządzania w Urzędzie Miasta Bielsk Podlaski i jego wymagania mają charakter zintegrowany z innymi procesami realizowanymi w Urzędzie.

§ 4.

Dokumentacja SZBI określa wymagania i zasady ochrony posiadanych informacji, w celu zapewnienia odpowiedniego poziomu bezpieczeństwa informacji, a także określa strukturę dokumentacji funkcjonującej w Urzędzie.

§ 5.

Celem SZBI jest zapewnienie zachowania poufności, integralności i dostępności informacji poprzez określenie kierunków działań oraz zapewnienie bezpieczeństwa przetwarzania i przechowywania informacji, w szczególności:

- 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.

§ 6.

Zakres SZBI 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).

§ 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 incydem;
- 5) postępowania w przypadku podejrzenia naruszenia lub naruszenia ochrony danych osobowych;
- 6) nadzoru nad dokumentacją SZBI.

2. Utrzymanie odpowiedniego poziomu bezpieczeństwa informacji wymaga:

- 1) systematycznych szkoleń oraz podnoszenia kwalifikacji zawodowych pracowników (w szczególności dotyczy to informatyków i członków zespołu ds. bezpieczeństwa informacji);
- 2) okresowego wykonywania przeglądów SZBI.

§ 8.

W Urzędzie odpowiedzialność za bezpieczeństwo informacji ponoszą:

- 1) Burmistrz Miasta Bielsk Podlaski ustanowienia, wdraża, monitoruje i doskonali SZBI;
- 2) Inspektor Ochrony Danych, zwany dalej IOD, nadzoruje przestrzeganie zasad ochrony przetwarzanych w Urzędzie danych osobowych, oraz sprawuje nadzór nad opracowanymi w tym celu dokumentami;
- 3) osoby nadzorujące referaty egzekwują przestrzeganie przepisów związanych z ochroną informacji i danych w podległych referatach;
- 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) Administrator Systemu Informatycznego oraz 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 spowodować pociągnięcie do odpowiedzialności wynikającej z przepisów prawa, w szczególności Kodeksu Pracy, rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. oraz przepisów o ochronie danych osobowych i ustawy o krajowym systemie cyberbezpieczeństwa.

§ 11.

1. Zobowiązuje się pracowników Urzędu do stosowania zasad określonych w dokumentacji SZBI.
2. Każdy pracownik, stażysta, praktykant, członek komisji podpisuje oświadczenie o stosowaniu się do zasad zawartych w dokumentacji SZBI.
3. Referat Organizacyjno-Gospodarczy w porozumieniu z Inspektorem Ochrony Danych przekazuje do zapoznania się nowo zatrudnionym pracownikom wybrane dokumenty SZBI, mając na względzie zakres czynności pracownika.
4. Zgodnie z dokumentacją SZBI w umowach z podmiotami, które otrzymały fizyczny lub zdalny dostęp do zasobów Urzędu stosuje się odpowiednie zapisy dotyczące poufności, określone w art. 28 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.
5. Dokumentacja SZBI powinna być przeglądana i weryfikowana w następujących przypadkach:
 - 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 informacji dokonuje analizy dokumentacji SZBI podczas okresowych przeglądów, wykonywanych nie później niż do końca marca każdego roku, oraz w przypadku sytuacji wymienionych w ust. 5 pkt 3. Zmienione dokumenty są uzgadniane z Sekretarzem Miasta i zatwierdzane przez Burmistrza Miasta Bielsk Podlaski.
7. W skład zespołu ds. Bezpieczeństwa Informacji wchodzi:
 - 1) Inspektor Ochrony Danych;
 - 2) Zastępca Inspektora Ochrony Danych;
 - 3) Administrator Systemu Informatycznego;
 - 4) Kierownik Referatu Organizacyjno-Gospodarczego;
 - 5) Informatycy;

6) Pracownik służby BHP.

§ 12.

Na SZBI składają 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 informatycznych;
- 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;
- 10) Dokument nr 10 SZBI - Procedura szyfrowania i deszyfrowania danych osobowych przesyłanych pocztą elektroniczną;
- 11) Dokument nr 11 SZBI - Plan ciągłości działania Urzędu;
- 12) Dokument nr 12 - Procedura zarządzania incydemem;
- 13) Dokument nr 13 SZBI - Procedura postępowania w przypadku podejrzenia naruszenia lub naruszenia ochrony danych osobowych;
- 14) Dokument nr 14 SZBI - Procedura tworzenia, przechowywania i niszczenia kopii bezpieczeństwa;
- 15) Dokument nr 15 SZBI - Regulamin korzystania z internetu.

§ 13.

Traci moc Zarządzenie Nr 81/19 Burmistrza Miasta z dnia 7 czerwca 2019 r. w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji dla Urzędu Miasta Bielsk Podlaski.

§ 14.

Zarządzenie wchodzi w życie z dniem podpisania.

Burmistrz Miasta

Jarosław Borowski