Zarządzenie nr 33/2022

Burmistrza Miasta i Gminy Sztum

z dnia 30 marca 2022 roku

W sprawie wdrożenia dokumentacji systemu zarządzania bezpieczeństwem informacji w Urzędzie Miasta i Gminy w Sztumie

Na podstawie art. 24 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz. Urz. UE L. 119) w związku z § 20 rozporządzenia 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 (Dz. U. z 2017 poz. 2247) oraz art. 31 i art. 33 ust. 3 ustawy z dnia 8 marca 1990 roku o samorządzie gminnym (Dz. U. z 2021 poz. 1372 ze zm.), zarządza się co następuje:

§1

1. Przyjmuje się deklarację stosowania zasad bezpieczeństwa informacji stanowiącą załącznik nr 0 do zarządzenia.

2. Wprowadza się do stosowania w Urzędzie Miasta i Gminy w Sztumie dokumentację systemu zarządzania bezpieczeństwem informacji, opisującą w szczególności środki techniczne i organizacyjne wdrożone w celu zminimalizowania ryzyka naruszenia praw i wolności osób fizycznych, których dane przetwarzane są w Urzędzie.

3. Dokumentacja systemu zarządzania bezpieczeństwem informacji (SZBI) o której mowa w ust. 2, obejmuje:

Politykę bezpieczeństwa informacji (PBI), stanowiącą załącznik nr 1 do zarządzenia oraz związaną z nią dokumentację bezpieczeństwa na którą składają się:

1) Polityka bezpieczeństwa danych osobowych (PBDO), stanowiąca załącznik nr 1 do PBI;
2) Polityka bezpieczeństwa fizycznego (PBF), stanowiąca załącznik nr 2 do PBI;
3) Polityka bezpieczeństwa teleinformatycznego (PBT), stanowiąca załącznik nr 3 do PBI;
4) Polityka zarządzania incydentami i monitorowania systemu zarządzania bezpieczeństwem informacji (PZIM), stanowiąca załącznik nr 4 do PBI;
5) Analiza ryzyka ogólnego i ocena skutków dla przetwarzania danych (ARO i DPIA), stanowiąca załącznik nr 5 do PBI;
6) Polityka ciągłości działania (PCD), stanowiąca załącznik nr 6 do PBI;

4. Dokumentacja, o której mowa w ust. 3 ma zastosowanie do wszystkich stanowisk pracy w Urzędzie, natomiast jej aktualizacja nie wymaga zmiany niniejszego zarządzenia.

5. Dokumentacja, o której mowa w ust. 3 stanowi wewnętrzną regulację i nie podlega publikacji.

§2

1. Osoby na stanowiskach kierowniczych w Urzędzie odpowiedzialne są w szczególności za:

1) bezpośredni nadzór nad przestrzeganiem oraz właściwym stosowaniem polityk, o których mowa w §1 ust.3, u podległych pracowników;
2) wdrożenie środków technicznych i organizacyjnych zapewniających bezpieczeństwo informacji, w szczególności ochronę przetwarzanych danych osobowych, odpowiednich do zagrożeń oraz kategorii danych objętych ochroną;
3) zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawioną, przetwarzaniem z naruszeniem przepisów prawa oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

§3

Za monitorowanie i przegląd systemu zarządzania bezpieczeństwem informacji, w celu jego utrzymania i doskonalenia powierza się Inspektorowi Ochrony Danych.

§4

Nadzór nad funkcjonowaniem systemu zarządzania bezpieczeństwem informacji w Urzędzie Miasta i Gminy w Sztumie sprawuje Sekretarz.

§5

Traci moc zarządzenie nr 7/2018 Burmistrza Miasta i Gminy Sztum z dnia 12 grudnia 2018r. w sprawie wprowadzenia dokumentacji zapewniającej ochronę przetwarzania danych osobowych w Urzędzie Miasta i Gminy Sztum wraz z opisem środków technicznych i organizacyjnych stosowanych w jednostce.

§6

Zarządzenie wchodzi w życie z dniem podpisania, z mocą obowiązującą od 25 maja 2018 roku.

Burmistrz Miasta i Gminy Sztum

Leszek Tabor

Podpisano elektronicznie

Załącznik nr 0 do Zarządzenia Nr 33/2022
Burmistrza Miasta i Gminy Sztum z dnia 30 marca 2022 roku
określającego System Zarządzania Bezpieczeństwem Informacji

Deklaracja stosowania zasad bezpieczeństwa informacji w Urzędzie Miasta i Gminy w Sztumie.

Urząd Miasta i Gminy w Sztumie, niniejszym deklaruje, iż:

1. Zapewnienie bezpieczeństwa informacji i danych przetwarzanych w Urzędzie, w tym za pomocą systemów informatycznych, jest jednym z kluczowych elementów dążących do zaspokojenia potrzeb i oczekiwań klientów Urząd;

2. W celu zagwarantowania sprawnej i skutecznej ochrony informacji i utrzymania wysokiego poziomu bezpieczeństwa informacji przetwarzanych oraz przemyślanych i adekwatnych do zagrożeń rozwiązań w Urzędzie ustanowiony został system zarządzania bezpieczeństwem informacji (SZBI)

3. System zarządzania bezpieczeństwem informacji obejmuje ochroną dane i informacje powierzone przez klientów, zarówno indywidualnych jak i instytucjonalnych, a także własne zasoby informacyjne, których przetwarzanie odbywa się w ramach procesów zgodnie z obowiązującymi przepisami prawa, zapewniając:
   a) dostęp wyłącznie osobom uprawnionym (poufność informacji)
   b) dokładność i kompletność informacji oraz metod jej przetwarzania (integralność informacji)
   c) dostęp do informacji i związanych z nią aktywów tylko wówczas, gdy istnieje taka konieczność (dostępność informacji);

4. Stosowanie zasad określonych w systemie zarządzania bezpieczeństwem informacji obejmuje wszystkich pracowników Urzędu.

5. Wdrożenie systemu zarządzania bezpieczeństwem informacji w Urzędzie Miasta i Gminy Sztum ma zapewnić:
   a) zgodność z obowiązującymi przepisami prawa oraz przyjętymi regulacjami wewnętrznymi wszelkich działań podejmowanych przez pracowników Urzędu oraz podmioty działające na jego rzecz;
   b) zabezpieczenie posiadanych aktywów informacyjnych raz systemów informatycznych poprzez wdrożenie odpowiednich mechanizmów mających na celu zapewnienie ochrony przed nieupoważnionym dostępem, fizycznym zniszczeniem, działalnością szkodliwego oprogramowania oraz utratą integralności informacji
   c) określenie zasad postępowania w sytuacjach awaryjnych i wystąpienia incydentu w obszarze bezpieczeństwa informacji;
   d) podnoszenie świadomości, wiedzy i zaangażowania pracowników w zakresie bezpieczeństwa informacji;
   e) kreowanie i utrzymanie pozytywnego wizerunku Urzędu jako instytucji wykazującej szczególną dbałość o bezpieczeństwo przetwarzanych informacji, własnych i powierzonych.