

ZARZĄDZENIE NR 23.../2016
BURMISTRZA MIASTA CHOJNICE
z dnia 22. marca 2016 r.

w sprawie zmiany Zarządzenia nr 47/2013 Burmistrza Miasta Chojnice z dnia 23 maja 2013r w sprawie zatwierdzenia Polityki Bezpieczeństwa w Urzędzie Miejskim w Chojnicach.

Na podstawie art. 30 ust. 1 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (t. j. Dz. U. z 2015 r., poz. 1515) w związku z art. 36 Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t. j. Dz.U. z 2015 r. poz. 2135) oraz § 3, § 4, § 5 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. Nr 100, poz. 1024), **zarządza się, co następuje:**

Zarządzam, co następuje:

§ 1

Do Zarządzenia nr 47/2013 Burmistrza Miasta Chojnice z dnia 23 maja 2013r. w sprawie w sprawie zatwierdzenia Polityki Bezpieczeństwa w Urzędzie Miejskim w Chojnicach wprowadza się następujące zmiany:

- 1) w § 4 po ust. 4 dodaje się ustęp 5 i 6 w następującym brzmieniu:

„5. W Urzędzie Miejskim w Chojnicach przetwarza się dane osobowe pochodzące z systemu Centralnej Ewidencji Pojazdów i Kierowców (CEPIK).

6. Przyjmuje się szczegółowe procedury ochrony dostępu do danych osobowych przetwarzanych w systemie CEPIK w brzmieniu stanowiącym załącznik nr 12 do niniejszego zarządzenia.”,

- 2) wprowadza się załącznik nr 12 w brzmieniu, jak w załączniku do niniejszego zarządzenia.

§ 2

Wylacza się jawność Polityki Bezpieczeństwa w Urzędzie Miejskim w Chojnicach.

§ 3

Zarządzenie wchodzi w życie z dniem podpisania.



BURMISTRZ

Arseniusz Finster

Załącznik do Zarządzenia Nr ²³./2016
Burmistrza Miasta Chojnice
z dnia 22. marca 2016 r.

**Szczegółowe procedury ochrony dostępu do danych
osobowych przetwarzanych w systemie CEPIK**

SPIS TREŚCI

	STR.
I Zakres dokumentu	3
II. Kontrola dostępu do pomieszczenia	3
III. Przechowywanie i kontrola dostępu do danych osobowych	3
IV. Bezpieczeństwo systemu teleinformatycznego	4
V. Procedura postępowania na wypadek zalania pomieszczenia	4
VI. Ustalenia końcowe.....	4
Zestawienie załączników	5

I. Zakres dokumentu

Niniejszy dokument stanowi uzupełnienie „Polityki bezpieczeństwa w Urzędzie Miejskim w Chojnicach” i „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Chojnicach” w zakresie umożliwiającym właściwą ochronę sprzętu teleinformatycznego oraz danych przetwarzanych w systemie CEPIK zgodnie z wymaganiami ustawy o ochronie danych osobowych (Dz. U. 2002 Nr 101, poz. 926 z późn. zm.) oraz Rozporządzenia Ministra Spraw Wewnętrznych i Administracji 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. 2004 Nr 100, poz. 1024).

II. Kontrola dostępu do pomieszczenia

Dostęp do pomieszczenia w którym znajduje się system teleinformatyczny łączący się z systemem CEPIK chroniony jest poprzez metody organizacyjno-proceduralne polegające na ścisłej kontroli i rejestracji pobierania kluczy. Klucze przechowywane są u Komendanta Straży Miejskiej, który każdorazowo przed rozpoczęciem pracy wydaje klucze do pomieszczenia za pokwitowaniem odnotowanym w REJESTRZE POBIERANIA KLUCZY DO POMIESZCZENIA CEPIK. Po zakończeniu pracy klucze zdawane są ponownie Komendantowi. Po godzinach pracy pomieszczenie jest chronione przez elektroniczny system alarmowy. W przypadku nieobecności lub urlopu Komendanta, wyznacza on osobę odpowiedzialną za kontrolę dostępu do pomieszczenia.

III. Przechowywanie i kontrola dostępu do danych osobowych

Administrator Bezpieczeństwa Informacji prowadzi ewidencję osób upoważnionych do pracy z systemem CEPIK. Osoby pobierające dane osobowe z systemu CEPIK prowadzą w formie papierowej bądź elektronicznej ewidencję zawierającą informację kto, kiedy oraz jakie pozyskiwał dane z systemu CEPIK. Dane osobowe uzyskane z systemu pozwalające na identyfikację osób przechowuje się nie dłużej niż jest to potrzebne do uzyskania celu przetwarzania. Dostęp do danych systemu CEPIK realizuje się w oparciu o indywidualne karty mikroprocesorowe, z których każda jest przypisana do jednej osoby.

Karty mikroprocesorowe udostępniane są wyłącznie osobom upoważnionym do przetwarzania danych osobowych w systemie CEPIK. Prowadzi się rejestr pobierania karty mikroprocesorowej.

IV. Bezpieczeństwo systemu teleinformatycznego

System teleinformatyczny łączący się z bazą danych CEPIK poprzez łącze internetowe zabezpiecza się przed nieuprawnionym dostępem od strony Internetu poprzez zastosowanie sprzętowego routera brzegowego. Sam system operacyjny stacji roboczej chroniony jest przez oprogramowanie Antywirusowe ESET NOD32, które automatycznie sprawdza aktualność sygnatur antywirusowych. Sprzęt komputerowy przeznaczony do pracy z systemem CEPIK oznacza się naklejką zawierającą informację: SYSTEM CEPIK — ZAKAZ UŻYWANIA PRZEZ OSOBY NIEUPOWAŻNIONE.

V. Procedura postępowania na wypadek zalania pomieszczenia

W przypadku zalania lub zatopienia pomieszczenia w pierwszej kolejności należy uprzednio odcinając energię elektryczną do pomieszczenia, ewakuować jednostkę centralną zawierającą dyski twarde oraz niezwłocznie przekazać informatykowi w celu jej zabezpieczenia przed utratą danych. W drugiej kolejności należy ewakuować dokumenty w formie papierowej a następnie pozostały sprzęt biurowy w tym monitory i urządzenia drukujące.

VI. Ustalenia końcowe

W sprawach nieuregulowanych niniejszymi procedurami stosuje się zasady i procedury zawarte w „Polityce bezpieczeństwa przetwarzania danych osobowych w Urzędzie Miejskim w Chojnicach” i „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Chojnicach”. W przypadku jakichkolwiek wątpliwości mających wpływ na bezpieczeństwo należy skonsultować się z Administratorem Bezpieczeństwa Informacji.

Zestawienie załączników:

Załącznik 1: Rejestr pobierania kluczy do pomieszczenia CEPIK.

Załącznik 2: Wykaz osób upoważnionych do przetwarzania danych osobowych przy pomocy systemu CEPIK.

Załącznik 3: Książka wejść i wyjść do pomieszczenia CEPIK.

Załącznik 4: Rejestr zapytań do CEPIK.

Załącznik 5: Rejestr osób nieupoważnionych przebywających w strefie CEPIK.

Załącznik 6: Rejestr pobierania karty mikroprocesorowej do systemu CEPIK.

Do użytku służbowego

**REJESTR POBIERANIA KLUCZY DO
POMIESZCZENIA CEPIK**

OSOBY UPOWAŻNIONE DO POBIERANIA KLUCZY

ID	Imię	Nazwisko	Zakres / ograniczenia	Data ważności poświadczenia bezpieczeństwa	Nr poświadczenia	Uwagi
1.						
2.						
3.						
4.						
5.						
6.						

POBIERNIE KLUCZY

Miesiąc Rok ...20

Dzień miesiąca	Godzina pobrania kluczy	ID osoby	Podpis	Godzina zdania kluczy	Podpis	Uwagi
1.						
2.						
3.						
4.						
5.						
6.						
7.						
8.						
9.						
10.						
11.						
12.						
13.						
14.						
15.						
16.						
17.						
18.						
19.						
20.						
21.						
22.						
23.						
24.						
25.						
26.						

**Wykaz osób
upoważnionych do przetwarzania danych osobowych przy pomocy systemu CEPIK.**

Lp	Imię	Nazwisko	Data	Podpis
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				
14.				
15.				
16.				
17.				
18.				
19.				
20.				
21.				
22.				

Do użytku służbowego

**KSIAŻKA
WEJŚĆ I WYJŚĆ**

POMIESZCZENIE „CEPIK”

Rozpoczęto

Zakończono

[illegible]

Do użytku służbowego

REJRSTR ZAPYTAŃ

DO „CEPIK”

Rozpoczęto

Zakończono

Rejestr zapytań do CEPIK

[illegible]

Do użytku służbowe

REJESTR
OSÓB NIEUPOWAŻNIONYCH PRZEBYWAJĄCYCH
W STREFIE „CEPIK”

Rozpoczęto

Zakończono

[illegible]

Do użytku służbowego

**REJESTR POBIERNIA KLUCZY DO
POBIERNIA KARTY MIKROPROCESOROWEJ
DO SYSTEMU CEPIK**

**OSOBY UPOWAŻNIONE DO POBIERNIA
KARTY MIKROPROCESOROWEJ DO SYSTEMU CEPIK**

[illegible]

POBIERNIA KARTY MIKROPROCESOROWEJ

Miesiąc **Rok**

[illegible]