Zarządzenie Nr 37/2021

Burmistrza Suraża

z dnia 06 października 2021r.

w sprawie zmiany Regulaminu Organizacyjnego Urzędu Miejskiego w Surażu.

Działając na podstawie art. 33 ust. 2 ustawy z dnia 8 marca 1990r. o samorządzie gminnym (Dz.U. z 2021r. poz. 1372) zarządzam co następuje:

§ 1

W regulaminie Organizacyjnym Urzędu Miejskiego w Surażu stanowiący załącznik Nr 1 i załącznik Nr 2 do Zarządzenia Nr 21/13 Burmistrza Suraża z dnia 12 sierpnia 2013r. w sprawie nadania Regulaminu Organizacyjnego Urzędu Miejskiego w Surażu z późniejszymi zmianami, wprowadza się następujące zmiany:

1. **W rozdziale III § 6 ust.1 dodaje się pkt. 6 i 7 w brzmieniu:**

6) Pion Ochrony Informacji Niejawnych – symbol POIN

7) Inspektor Ochrony Danych Osobowych – symbol IOD

2. **W rozdziale V dodaje się § 14 a i 14 b w brzmieniu:**

14 a. Do zadań Pionu Ochrony Informacji Niejawnych należy w szczególności:

1) Do zadań wspólnych pracowników **Kancelarii Dokumentów Niejawnych** należy:

a) inicjowanie i podejmowanie przedsięwzięć organizacyjnych w celu zapewnienia właściwej i terminowej realizacji zadań określonych w planach pracy i wynikających z aktów prawnych,

b) zapewnienie ochrony informacji niejawnych,

c) kontrola ochrony informacji niejawnych oraz przestrzegania przepisów o ochronie tych informacji w Urzędzie,

d) opracowanie szczegółowych wymagań w zakresie ochrony informacji niejawnych oznaczonych klauzulą „zastrzeżone", „poufne",

e) prowadzenie kontroli w Urzędzie.

2) W zakresie wykonywania zadań **Pełnomocnika ds. Ochrony Informacji Niejawnych**

a) zapewnienie ochrony informacji niejawnych, w tym stosowanie środków bezpieczeństwa fizycznego,

b) zapewnienie ochrony systemów teleinformatycznych, w których są przetwarzane informacje niejawne,

c) zarządzanie ryzykiem bezpieczeństwa informacji niejawnych, w szczególności szacowanie ryzyka,

d) kontrola ochrony informacji niejawnych oraz przestrzegania przepisów o ochronie tych informacji, w szczególności okresowa (co najmniej raz na trzy lata) kontrola ewidencji, materiałów i obiegu dokumentów,

e) prowadzenie szkoleń w zakresie ochrony informacji niejawnych mających na celu zapoznanie z:

- przepisami dotyczącymi ochrony informacji niejawnych oraz odpowiedzialności karnej, dyscyplinarnej i służbowej za ich naruszenie, w szczególności za nieuprawnione ujawnienie informacji niejawnych,

- zasadami ochrony informacji niejawnych w zakresie niezbędnym do wykonywania pracy lub pełnienia służby, z uwzględnieniem zasad zarządzania ryzykiem bezpieczeństwa informacji niejawnych, w szczególności szacowania ryzyka,

- sposobami ochrony informacji niejawnych oraz postępowania w sytuacjach zagrożenia dla takich informacji lub w przypadku ich ujawnienia,

- sposobami ochrony informacji niejawnych oraz postępowania w sytuacjach zagrożenia dla takich informacji lub w przypadku ich ujawnienia,

f) prowadzenie zwykłych postępowań sprawdzających oraz kontrolnych postępowań sprawdzających,

g) prowadzenie aktualnego wykazu osób zatrudnionych lub pełniących służbę w jednostce organizacyjnej albo wykonujących czynności zlecone, które posiadają uprawnienia do dostępu do informacji niejawnych, oraz osób którym odmówiono wydania poświadczenia bezpieczeństwa lub je cofnięto,

h) przekazywanie odpowiednio ABW lub SKW do ewidencji danych osób uprawnionych do dostępu do informacji niejawnych, a także osób, którym odmówiono wydania poświadczenia bezpieczeństwa lub wobec których podjęto decyzję o cofnięciu poświadczenia bezpieczeństwa, na podstawie wykazu, o którym mowa w pkt. 7,

i) W przypadku stwierdzenia naruszenia w jednostce organizacyjnej przepisów o ochronie informacji niejawnych zawiadamianie o tym kierownika jednostki organizacyjnej i podejmowanie niezwłocznie działań zmierzających do wyjaśnienia okoliczności tego naruszenia oraz ograniczenia jego negatywnych skutków,

j) W przypadku stwierdzenia naruszenia przepisów o ochronie informacji niejawnych o klauzuli „ poufne" lub wyższej zawiadamianie niezwłocznie również odpowiedniego ABW lub SKW,

k) opracowywanie i uaktualnianie (wymagające akceptacji kierownika jednostki organizacyjnej) następujące dokumenty:

- w razie wprowadzenia stanu nadzwyczajnego,

- sposób i tryb przetwarzania informacji niejawnych o klauzuli „poufne" w podległych komórkach organizacyjnych,

- dokumentację określającą poziom zagrożeń związanych z nieuprawnionym dostępem do informacji niejawnych lub ich utratą (w jednostce organizacyjnej, w której są przetwarzane informacje niejawne o klauzuli „poufne" lub wyższej), instrukcję dotyczącą sposobu i trybu

przetwarzania informacji niejawnych o klauzuli „zastrzeżone" w podległych komórkach organizacyjnych oraz zakres i warunki stosowania środków bezpieczeństwa fizycznego w celu ich ochrony,

- plan ochrony informacji niejawnych w jednostce organizacyjnej, w tym

i) zapewnienie ochrony systemów teleinformatycznych funkcjonujących w jednostce organizacyjnej (z wyłączeniem organizacyjnych, technicznych, programowych i eksploatacyjnych aspektów ochrony kryptograficznej) , w szczególności za:

- zapewnienie przestrzegania zasad ochrony informacji niejawnych przetwarzanych w systemach teleinformatycznych, w tym właściwego i bezpiecznego obiegu dokumentów oraz informatycznych nośników danych,

- zapewnienie bezpieczeństwa fizycznego obszarów, w których usytuowane są systemy teleinformatyczne,

- organizację i prowadzenie szkoleń użytkowników w zakresie bezpieczeństwa teleinformatycznego,

- nadzór nad konfiguracją systemów teleinformatycznych i przemieszczaniem ich elementów składowych,

- prowadzenie ewidencji systemów teleinformatycznych,

m) prowadzenie ewidencji środków ochrony elektromagnetycznej,

n) prowadzenie procesu szacowania ryzyka dla bezpieczeństwa informacji niejawnych,

o) Uczestniczenie w opracowaniu projektów dokumentów regulujących w danej jednostce organizacyjnej problematykę ochrony przetwarzanych w systemach teleinformatycznych informacji niejawnych, w tym:

- programów organizacyjno- użytkowych, projektów koncepcyjnych i technicznych planowanych do budowy systemów teleinformatycznych,

- dokumentacji bezpieczeństwa systemów teleinformatycznych,

p) Uzgadnianie dokumentacji bezpieczeństwa:

- organizowanych w danej jednostce organizacyjnej systemów teleinformatycznych, dla elementów rozległych systemów teleinformatycznych funkcjonujących w danej jednostce organizacyjnej.

3) **Inspektor Bezpieczeństwa Teleinformatycznego** realizuje zadania w zakresie weryfikacji i bieżącej kontroli zgodności funkcjonowania eksploatowanego w danej jednostce organizacyjnej systemu teleinformatycznego z jego dokumentacją bezpieczeństwa, a w szczególności odpowiada za:

a) ustalenie wymagań bezpieczeństwa dla systemu TI i opracowanie odpowiedniej dokumentacji,

b) kontrolę znajomości i przestrzegania „Procedur Bezpiecznej Eksploatacji Systemu TI" przez użytkowników systemu TI,

c) monitorowanie stanu zabezpieczeń fizycznych, elektromagnetycznych i elektronicznych pomieszczeń, w których usytuowany jest system TI,

d) kontrolowanie zgodności wykorzystywania zaimplementowanych środków ochrony z zatwierdzoną dokumentacją bezpieczeństwa systemu TI,

e) monitorowanie bezpieczeństwa teleinformatycznego,

f) okresowe przeglądy ryzyk i analizowanie skuteczności zabezpieczeń,

g) tworzenie planów awaryjnych i organizowanie treningów w ich realizacji,

h) kontrola utrzymania zgodności konfiguracji systemu TI z dokumentacją bezpieczeństwa teleinformatycznego,

i) przeprowadzenie szkoleń i podnoszenie świadomości w zakresie bezpieczeństwa,

j) zaznajomienie i przestrzeganie przez użytkowników „Procedur Bezpiecznej Eksploatacji Systemu TI",

k) wyjaśnianie i reagowanie na incydenty naruszenia bezpieczeństwa,

l) analizowanie rejestru zdarzeń w systemie TI i prawidłowe dokumentowanie i archiwizowanie zdarzeń,

m) informowanie Pełnomocnika ds .Ochrony Informacji Niejawnych o wszelkich zdarzeniach związanych lub mogących mieć związek z bezpieczeństwem systemu TI,

14 b. W zakresie realizacji zadań Inspektora Ochrony Danych Osobowych

1.Inspektor Ochrony Danych nadzoruje przestrzeganie zasad ochrony danych osobowych zarówno w systemach informatycznych, jak również w zbiorach danych osobowych prowadzonych w formie papierowej.

2. Do kompetencji Inspektora Ochrony Danych należy:

1) określenie zasad ochrony danych osobowych,

2) wnioskowanie o ukaranie osób winnych naruszenia przepisów i zasad dotyczących ochrony danych osobowych.

3. Do obowiązków Inspektora Ochrony Danych należy:

1) nadzór nad wdrożeniem stosownych środków organizacyjnych, technicznych i fizycznych w celu ochrony przetwarzanych danych osobowych,

2)prowadzenie dokumentacji opisującej zastosowaną ochronę danych osobowych (polityka oraz wynikające z niej instrukcje i procedury),

3) zapoznawanie pracowników z przepisami i zasadami ochrony danych osobowych oraz informowanie o zagrożeniach związanych z ich przetwarzaniem,

4) odbieranie od pracowników oświadczenia o znajomości przepisów o ochronie danych osobowych oraz zobowiązania do zachowania w tajemnicy danych osobowych oraz informacji na temat zabezpieczania danych osobowych,

5) reprezentowanie administratora w kontaktach z Urzędem Ochrony Danych Osobowych,

6) prowadzenie rejestru osób upoważnionych do przetwarzania danych osobowych,

7) reagowanie na zgłaszane incydenty związane z naruszeniem ochrony danych osobowych oraz analizowanie ich przyczyn i kierowanie wniosków dla administratora, \

8) kontrola oraz sprawdzanie wypełnienia obowiązków technicznych i organizacyjnych związanych z ochroną danych osobowych,

9) prowadzenie rejestru czynności przetwarzania danych osobowych,

10) prowadzenie rejestru wydanych upoważnień do przetwarzania danych osobowych,

11) opracowywanie sprawozdań dla administratora,

12) opiniowanie projektów aktów prawnych, umów, porozumień w zakresie przetwarzania danych osobowych.

4. Inspektor Ochrony Danych w zakresie realizacji swoich obowiązków, ma prawo żądania od pracowników bezzwłocznej pomocy w razie stwierdzenia naruszenia przepisów o ochronie danych osobowych, które mogłoby skutkować odpowiedzialnością karną.

5. Inspektor Danych osobowych jest zobowiązany do zachowania tajemnicy lub poufności co do wykonywania swoich zadań.

6. Wykonywanie innych zadań zleconych przez Burmistrza Suraża.

3. Schemat organizacyjny Urzędu Miejskiego w Surażu stanowiący załącznik Nr 2 do zarządzenia Nr 21/13 Burmistrza Suraża z dnia 12 sierpnia 2013r. w sprawie nadania Regulaminu Organizacyjnego Urzędu Miejskiego w Surażu otrzymuje brzmienie jak w załączniku do niniejszego zarządzenia.

§ 2

Pozostałe zapisy Zarządzenia pozostają bez zmian.

§ 3

Zarządzenie wchodzi w życie z dniem podpisania.

BURMISTRZ

mgr inż. Henryk Łapiński

: