

ZARZĄDZENIE nr 114/2021
BURMISTRZA MIASTA PIONKI
z dnia 3 grudnia 2021 roku

w sprawie powołania „Pionu Ochrony Informacji Niejawnych” oraz wyznaczenia
Inspektora Bezpieczeństwa Teleinformatycznego i Administratora Systemu
Teleinformatycznego w Urzędzie Miejskim w Pionkach.

Na podstawie art. 30 ust. 1 ustawy z dnia 8 marca 1990 roku o samorządzie gminnym (Dz. U. 2021 poz. 1372 ze zm.) w związku z art. 14 ust. 1, art. 15 ust. 2 i ust. 4, art. 16, art. 52 ustawy z dnia 5 sierpnia 2010 roku o ochronie informacji niejawnych (Dz. U. 2019 poz. 742) oraz § 13 i § 14 Rozporządzenia Prezesa Rady Ministrów z dnia 20 lipca 2011 roku w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz. U. 2011 nr 159 poz. 948), zarządzam co następuje:

§ 1.

1. W celu zapewnienia właściwej ochrony informacji niejawnych w Urzędzie Miejskim w Pionkach, powołuję „Pion Ochrony Informacji Niejawnych”, zwany dalej „pionem ochrony”.
2. Pion ochrony podlega Pełnomocnikowi do spraw ochrony informacji niejawnych.
3. Pion ochrony przy oznakowaniu spraw posługuje się symbolem POIN.

§ 2.

W skład pionu ochrony wchodzi:

1. Pełnomocnik do spraw ochrony informacji niejawnych.
2. Inspektor Bezpieczeństwa Teleinformatycznego
3. Kierownik Wydziału Porządku, Obrony Cywilnej i Zarządzania Kryzysowego.
4. Administrator Systemu Teleinformatycznego.

§ 3.

Z dniem 9 grudnia 2021 roku wyznaczam do pełnienia funkcji Inspektora Bezpieczeństwa Teleinformatycznego – pracownika Urzędu Miejskiego w Pionkach Pana Karol Łobodźca.

§ 4.

Z dniem 9 grudnia 2021 roku wyznaczam do pełnienia funkcji Administratora Systemu Teleinformatycznego – pracownika Urzędu Miejskiego w Pionkach Pana Kamila Łobodźca.

§ 5.

Pracownicy pionu ochrony podlegają Pełnomocnikowi do spraw ochrony informacji niejawnych a do czasu jego powołania Burmistrzowi Miasta Pionki.

§ 6.

Zadania Pełnomocnika do spraw ochrony informacji niejawnych określa ustawa z dnia 5 sierpnia 2010 roku o ochronie informacji niejawnych (Dz. U. 2019 poz. 742 ze zm.) oraz akty wykonawcze do tej ustawy.

§ 7.

Inspektor Bezpieczeństwa Teleinformatycznego realizuje zadania w zakresie weryfikacji i bieżącej kontroli zgodności funkcjonowania systemu teleinformatycznego ze szczególnymi wymaganiami bezpieczeństwa oraz przestrzegania procedur bezpiecznej eksploatacji, bierze udział w procesie zarządzania ryzykiem systemie teleinformatycznym weryfikując:

- a) przestrzeganie zasad ochrony przetwarzanych w systemie teleinformatycznym informacji niejawnych;
- b) poprawność realizacji zadań wykonywanych przez administratora systemu teleinformatycznego;
- c) właściwe zarządzanie konfiguracją systemu teleinformatycznego oraz uprawnieniami przydzielanymi użytkownikom;
- d) znajomość i przestrzeganie przez użytkowników zasad ochrony informacji niejawnych oraz procedur bezpiecznej eksploatacji w systemie teleinformatycznym, w tym w zakresie wykorzystywania urządzeń i narzędzi służących do ochrony informacji niejawnych;
- e) stan zabezpieczeń systemu teleinformatycznego, w tym analizując rejestry zdarzeń systemu teleinformatycznego;
- f) aktualność wykazów osób mających dostęp do systemu teleinformatycznego.

Ponadto inspektor bezpieczeństwa teleinformatycznego:

1. Uczestniczy w opracowywaniu programów organizacyjno – użytkowych, projektów koncepcyjnych i technicznych planowanych do budowy systemów teleinformatycznych.

§ 8.

Administrator Systemu Teleinformatycznego jest odpowiedzialny za funkcjonowanie systemu teleinformatycznego oraz odpowiada za przestrzeganie zasad i wymagań bezpieczeństwa przewidzianych dla systemu teleinformatycznego, a w szczególności:

1. Bierze udział w opracowaniu i aktualizowaniu dokumentacji bezpieczeństwa systemu teleinformatycznego.
2. Przechowuje oryginały zatwierdzonej dokumentacji bezpieczeństwa systemu teleinformatycznego.
3. Bierze udział w procesie zarządzania ryzykiem w systemie teleinformatycznym.
4. Szkoli użytkowników systemu teleinformatycznego z zakresu procedur bezpiecznej eksploatacji.
5. Utrzymuje zgodność systemu teleinformatycznego z jego dokumentacją bezpieczeństwa.
6. Wdraża zabezpieczenia w systemie teleinformatycznym oraz procedury bezpiecznej eksploatacji.
7. Systematycznie kontroluje funkcjonowanie mechanizmów zabezpieczeń i poprawność działania systemu teleinformatycznego.
8. Analizuje i archiwizuje rejestr zdarzeń w systemie teleinformatycznym.
9. Zapewnia dostęp do systemu teleinformatycznego wyłącznie użytkownikom posiadającym wymagane uprawnienia oraz odpowiednie i ważne poświadczenia bezpieczeństwa lub upoważnienie.

10. Przydziela użytkownikom konta, zgodnie z uprawnieniami nadanymi przez kierownika jednostki (komórki) organizacyjnej.
11. Prowadzi wykaz osób mających dostęp do systemu teleinformatycznego zawierający, co najmniej:
 - imię i nazwisko;
 - nazwę jednostki (komórki) organizacyjnej;
 - posiadane poświadczenie bezpieczeństwa lub upoważnienie (jego numer, klauzulę i datę ważności);
12. Odpowiada za tworzenie kopii bezpieczeństwa plików.
13. Przeprowadza czynności serwisowe w przypadku awarii sprzętu.
14. Prowadzi dokumentację eksploatacyjną systemu - „Dziennik działań Administratora Systemu Teleinformatycznego”.
15. Współpracuje z Pełnomocnikiem do spraw ochrony informacji niejawnych przy wydawaniu i przechowywaniu elektronicznych nośników danych.
16. Informuje Pełnomocnika ochrony o stwierdzonych naruszeniach bezpieczeństwa systemu teleinformatycznego.
17. Zgłasza do pełnomocnika ochrony potrzeby w zakresie serwisowania i certyfikacji środków ochrony elektromagnetycznej.

§ 9.

Zarządzenie wchodzi w życie z dniem podpisania.

BURMISTRZ


mgr Robert Kowalczyk

RADCA PRAWNY

Marcin Jasek
KL. 152