Pion Ochrony Informacji Niejawnych
Karolina Kowalska
tel. (63) 270-40-11 wew. 121
dowody@slesin.pl

Wyciąg z Regulaminu Organizacyjnego Urzędu Miasta i Gminy w Ślesinie wprowadzonego Zarządzeniem Nr 5/2021 Burmistrza Miasta i Gminy Ślesin z dnia 1 lutego 2021 r.

Do zadań Pionu Informacji Niejawnych w Urzędzie Miasta i Gminy Ślesin [BIN] należą w szczególności:

1. Zapewnienie ochrony informacji niejawnych, w tym ich ochrony fizycznej.
2. Opracowanie i prowadzenie dokumentacji bezpieczeństwa systemu teleinformatycznego.
3. Zarządzenie bezpieczeństwem systemu teleinformatycznego.
4. Zarządzanie ryzykiem bezpieczeństwa informacji niejawnych, w szczególności szacowanie ryzyka.
5. Kontrola ochrony informacji niejawnych oraz przestrzeganie przepisów o ochronie tych informacji, okresowa kontrola ewidencji, materiałów i obiegu dokumentów.
6. Opracowywanie dokumentów wynikających z ustawy oraz innych obowiązujących aktów normatywnych z zakresu ochrony informacji niejawnych i nadzorowanie ich realizacji.
7. Prowadzenie szkoleń pracowników w zakresie ochrony informacji niejawnych.

W skład „Pionu Ochrony Informacji Niejawnych" wchodzą:

1) Pełnomocnik ds. Ochrony Informacji Niejawnych,
2) Inspektor Bezpieczeństwa Teleinformatycznego,
3) Administrator Systemu Teleinformatycznego,
4) Pracownik ds. ewidencjonowania i przetwarzania materiałów niejawnych.

1. **Do zakresu zadań Pełnomocnika ds. Ochrony Informacji Niejawnych należy:**
   1) kierowanie wyodrębnioną komórką zwaną „Pionem Ochrony Informacji Niejawnych",
   2) zapewnienie ochrony informacji niejawnych, w tym stosowanie środków bezpieczeństwa fizycznego,
   3) zapewnienie ochrony systemów teleinformatycznych, w których są przetwarzane informacje niejawne,
   4) zarządzenie ryzykiem bezpieczeństwa informacji niejawnych, w szczególności szacowanie ryzyka,

5) 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,
6) opracowanie i aktualizowanie, wymagające akceptacji kierownika jednostki organizacyjnej, planu ochrony informacji niejawnych w jednostce organizacyjnej, w tym w razie wprowadzenia stanu nadzwyczajnego i nadzorowania jego realizacji,
7) prowadzenie szkoleń w zakresie ochrony informacji niejawnych,
8) prowadzenie zwykłych postępowań sprawdzających oraz kontrolnych postępowań sprawdzających,
9) 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 wydanie poświadczenia bezpieczeństwa lub je cofnięto, obejmującego włącznie (imię i nazwisko, numer PESEL, imię ojca, datę i miejsce urodzenia, adres miejsca zamieszkania lub pobytu, określenie dokumentu kończącego procedurę, datę jego wydania oraz numer),
10) Przekazywanie odpowiednio ABW lub SKW do ewidencji, o których mowa w art. 73 ust.1 ustawy o ochronie informacji niejawnych, danych o których mowa w art.73 ust.2 wskazanej ustawy, osób uprawnionych do dostępu do informacji niejawnych, a także osób, którym odmówiono wydania poświadczenia bezpieczeństwa lub wobec których podjęto decyzje o cofnięciu poświadczenia bezpieczeństwa na podstawie wykazu, o którym mowa w pkt.9.

2. Do zakresu zadań Inspektora Bezpieczeństwa Teleinformatycznego należy:

1) weryfikacja i bieżąca kontrola zgodności funkcjonowania systemu teleinformatycznego ze szczególnymi wymaganiami bezpieczeństwa oraz przestrzegania procedur bezpiecznej eksploatacji,
2) przestrzeganie zasad ochrony przetwarzanych w systemie teleinformatycznym informacji niejawnych,
3) ocena poprawności realizacji zadań wykonywanych przez administratora,
4) nadzorowanie zgodności konfiguracji systemu teleinformatycznego z dokumentacją bezpieczeństwa systemu teleinformatycznego,
5) aktualizacja wykazów osób mających dostęp do systemu teleinformatycznego, w tym dbałość o prawidłowe przydzielanie kont użytkownikom,
6) znajomość i nadzorowanie przestrzegania przez użytkowników procedur bezpiecznej eksploatacji systemu teleinformatycznego.

3. Do zakresu zadań Administratora Systemu Teleinformacyjnego należy:

1) realizacja zadań w zakresie odpowiedzialności za właściwe funkcjonowanie systemu teleinformatycznego oraz za przestrzeganie zasad i wymagań bezpieczeństwa przewidzianych dla tego systemu,
2) opracowywanie i uaktualnianie dokumentacji bezpieczeństwa systemu teleinformatycznego,

3) wdrażanie, szkolenie użytkowników systemu teleinformatycznego z zakresu procedur bezpiecznej eksploatacji,
4) systematyczne kontrolowanie funkcjonowania mechanizmów zabezpieczeń i poprawność działania systemu teleinformatycznego,
5) zakładanie kont w oprogramowaniu systemu operacyjnego komputera i przydzielenie im pierwszych haseł dostępu,
6) zapewnienie obsługi technicznej systemu i sprawdzanie poprawności jego działania,
7) prowadzenie rejestru osób mających dostęp do sytemu teleinformatycznego,
8) informowanie inspektora bezpieczeństwa teleinformatycznego o zagrożeniach i stwierdzonych naruszeniach bezpieczeństwa teleinformatycznego.

4. Do zakresu zadań Pracownika ds. ewidencjonowania i przetwarzania materiałów niejawnych należy:

1) rejestracja i ewidencja dokumentów niejawnych,
2) przygotowywanie, wysyłanie i odbieranie przesyłek niejawnych.