ZARZĄDZENIE NR 127/2018
STAROSTY ŁÓDZKIEGO WSCHODNIEGO
z dnia 20 listopada 2018 r.

w sprawie utworzenia Pionu Ochrony Informacji Niejawnych w Starostwie Powiatowym w Łodzi

Na podstawie art. 14 ust. 1, art. 15 ust. 1, 2 i 4 oraz art. 52 ust. 1 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2018 r. poz. 412, poz. 650, poz. 1000, poz. 1083 i poz. 1669) oraz § 13 i § 14 Rozporządzenia Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz. U. z 2011 r. Nr 159, poz. 948) zarządza się, co następuje:

§ 1.1. Tworzy się Pion Ochrony Informacji Niejawnych w Starostwie Powiatowym w Łodzi, który jest odpowiedzialny za zapewnienie ochrony informacji niejawnych oraz ochrony systemu teleinformatycznego Autonomicznego Stanowiska Komputerowego „ASK", w składzie:

1) Pełnomocnik ds. Ochrony Informacji Niejawnych - Roman Rutkowski,
2) Pracownik Kancelarii Dokumentów Niejawnych - Marianna Zelek,
3) Administrator Systemu Teleinformatycznego - Jan Wiechno,
4) Inspektor Bezpieczeństwa Teleinformatycznego - Arkadiusz Niecka,
5) Użytkownik Systemu Teleinformatycznego - Wacław Kryński.

2. Pionem Ochrony kieruje Pełnomocnik ds. Ochrony Informacji Niejawnych,

3. Pracownicy Pionu Ochrony Informacji Niejawnych podlegają Pełnomocnikowi ds. Ochrony Informacji Niejawnych,

4. Pełnomocnik ds. Ochrony Informacji Niejawnych podlega bezpośrednio Staroście Łódzkiemu Wschodniemu.

§ 2.1. Do zadań Pełnomocnika ds. Ochrony Informacji Niejawnych należy:

1) nadzór merytoryczny nad pracownikami Pionu Ochrony Informacji Niejawnych,
2) zapewnienie ochrony informacji niejawnych, w tym stosowanie środków bezpieczeństwa fizycznego,
3) zapewnienie ochrony systemu teleinformatycznego, w którym są przetwarzane informacje niejawne,
4) zarządzanie ryzykiem bezpieczeństwa informacji niejawnych, w szczególności szacowanie ryzyka,
5) kontrola ochrony informacji niejawnych oraz przestrzegania przepisów o ochronie tych informacji,
6) opracowywanie i aktualizowanie, wymagającego akceptacji Starosty Łódzkiego Wschodniego, planu ochrony informacji niejawnych w Starostwie Powiatowym w Łodzi, w tym w razie wprowadzenia stanu nadzwyczajnego, i nadzorowanie 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 Starostwie Powiatowym w Łodzi albo wykonujących czynności zlecone, które posiadają uprawnienia do dostępu do informacji niejawnych oraz osób, którym odmówiono wydania poświadczenia bezpieczeństwa lub je cofnięto,
10) przekazywanie do Agencji Bezpieczeństwa Wewnętrznego 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.

2. W przypadku stwierdzenia naruszenia w Starostwie Powiatowym w Łodzi przepisów o ochronie informacji niejawnych Pełnomocnik ds. Ochrony Informacji Niejawnych zawiadamia o tym Starostę Łódzkiego Wschodniego i podejmuje niezwłoczne działania zmierzające do wyjaśnienia okoliczności tego naruszenia oraz ograniczenia jego negatywnych skutków.

§ 3. Do zadań Pracownika Kancelarii Dokumentów Niejawnych w szczególności należy:
1) bezpośredni nadzór nad obiegiem dokumentów niejawnych w Starostwie Powiatowym w Łodzi,
2) udostępnianie lub wydawanie dokumentów niejawnych osobom do tego uprawnionym,
3) egzekwowanie zwrotu dokumentów niejawnych,
4) kontrola przestrzegania właściwego oznaczania i rejestrowania dokumentów w kancelarii dokumentów niejawnych w Starostwie Powiatowym w Łodzi,
5) prowadzenie bieżącej kontroli postępowania z dokumentami zawierającymi informacje niejawne, które zostały udostępnione pracownikom,
6) prowadzenie archiwizacji dokumentów niejawnych.

§ 4.1. Administrator Systemu Teleinformatycznego jest odpowiedzialny za właściwe funkcjonowanie systemu teleinformatycznego oraz za przestrzeganie zasad i wymagań bezpieczeństwa przewidzianych dla tego systemu.

2. Do zadań Administratora Systemu Teleinformatycznego w szczególności należy:
1) udział w tworzeniu dokumentacji bezpieczeństwa systemu teleinformatycznego,
2) udział w procesie zarządzania ryzykiem w systemie teleinformatycznym,
3) utrzymanie zgodności systemu teleinformatycznego z jego dokumentacją bezpieczeństwa,
4) nadawnie/odbieranie uprawnień użytkownikom i prowadzenie wykazu użytkowników systemu teleinformatycznego,
5) utrzymanie systemu teleinformatycznego w pełnej sprawności, sprawdzanie poprawności działania systemu teleinformatycznego oraz wdrażanie jego zabezpieczeń,
6) instalacja systemu operacyjnego i oprogramowania z listy dopuszczonych do instalacji programów oraz ich bieżące aktualizowanie,

7) przeprowadzenie szkoleń z zakresu bezpieczeństwa teleinformatycznego dla użytkowników systemu,
8) zabezpieczenie stanowiska przed pożarem i osobami postronnymi,
9) nadzór rejestracji i oznaczenia elektronicznych nośników danych,
10) tworzenie kopii zapasowych,
11) zabezpieczanie plombami sprzętu komputerowego.

§ 5.1. Inspektor Bezpieczeństwa Teleinformatycznego jest odpowiedzialny za weryfikację i bieżącą kontrolę zgodności funkcjonowania systemu teleinformatycznego ze szczególnymi wymaganiami bezpieczeństwa oraz przestrzegania procedur bezpiecznej eksploatacji.

2. Do zadań Inspektora Bezpieczeństwa Teleinformatycznego w szczególności należy:
1) weryfikacja poprawności realizacji zadań przez Administratora Systemu Teleinformatycznego,
2) weryfikacja znajomości i przestrzegania przez użytkowników zasad ochrony informacji niejawnych oraz procedur bezpiecznej eksploatacji w systemie teleinformatycznym,
3) weryfikacja stanu zabezpieczeń systemu teleinformatycznego, w tym analiza rejestrów zdarzeń systemu teleinformatycznego,
4) udział w procesie zarządzania ryzykiem w systemie teleinformatycznym,
5) wspólne z Administratorem prowadzenie postępowania wyjaśniającego w związku z wystąpieniem incydentu naruszenia bezpieczeństwa teleinformatycznego,
6) przeprowadzanie wewnętrznego audytu bezpieczeństwa oraz prowadzenie stosownej dokumentacji,
7) kontrola zabezpieczenia i przechowywania nośników oraz weryfikowanie wykazu udostępniania elektronicznych nośników informacji,
8) prowadzenia szkoleń z zakresu bezpieczeństwa teleinformatycznego dla użytkowników systemu,
9) nadzorowanie napraw i przeglądów diagnostycznych.

§ 6. Do zadań Użytkownika Systemu w szczególności należy:
1) bezpośredni nadzór nad wykonywaniem i obiegiem dokumentów niejawnych,
2) udostępnianie dokumentów niejawnych osobom do tego uprawnionym,
3) przestrzeganie właściwego oznaczania i rejestrowania dokumentów niejawnych w jednostce organizacyjnej,
4) zabezpieczanie stanowiska przed osobami postronnymi.

§ 7. Wykonanie zarządzenia powierza się Pełnomocnikowi ds. Ochrony Informacji Niejawnych.

§ 8. Traci moc Zarządzenie Nr 39/2010 Starosty Łódzkiego Wschodniego z dnia 7 maja 2010 r. w sprawie utworzenia pionu ochrony i wyznaczenia kierownika kancelarii tajnej.

§ 9. Zarządzenie wchodzi w życie z dniem podpisania.

STAROSTA
Andrzej Opala