Zarządzenie Nr 7/2019
Starosty Jarocińskiego
z dnia 21 stycznia 2019r.

w sprawie ustalenia organizacji ochrony informacji niejawnych w Starostwie Powiatowym w Jarocinie

Na podstawie art. 35 ust. 2 ustawy z dnia 5 czerwca 1998 r. o samorządzie powiatowym (Dz. U. z 2018 r. poz. 995 z zm.) w związku z art.14 ust.1 i 2, art. 15 ust. 2, art.52 ust. 1 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2018 r. poz. 412 z zm.) zarządzam, co następuje:

§ 1. 1. W strukturze Starostwa Powiatowego w Jarocinie, zwanego dalej „Starostwem" działa Pion Ochrony realizujący zadania określone w ustawie o ochronie informacji niejawnych.

2. W skład Pionu Ochrony wchodzą:

1) Kancelaria Niejawna;
2) Kancelista (obsługa Kancelarii Niejawnej) – OIN.I;
3) Inspektor bezpieczeństwa teleinformatycznego – OIN.II;
4) Administrator systemu – OIN.III.

§ 2. 1. Pionem Ochrony kieruje Pełnomocnik ds. ochrony informacji niejawnych Starostwa, zwany dalej „Pełnomocnikiem ochrony".

2. W przypadku czasowej nieobecności Pełnomocnika ochrony jego obowiązki przejmuje Kancelista lub upoważniony przez niego pracownik.

§ 3. Do podstawowych zadań Pionu Ochrony należy:

1) zapewnienie ochrony informacji niejawnych;
2) zapewnienie przestrzegania przepisów o ochronie informacji niejawnych;
3) zapewnienie funkcjonowania i ochrony Bezpiecznej Stacji Komputerowej;
4) opracowanie i aktualizacja dokumentacji wynikającej z przepisów o ochronie informacji niejawnych;
5) ewidencjonowanie, wykonywanie, zabezpieczanie, udostępnianie i archiwizowania materiałów niejawnych;
6) nadzorowanie obiegu informacji niejawnych;
7) prowadzenie wykazu osób uprawnionych do dostępu do informacji niejawnych w Starostwie;
8) prowadzenie szkoleń w zakresie ochrony informacji niejawnych;
9) współdziałanie z ABW i innymi instytucjami w zakresie ochrony informacji niejawnych.

§ 4. 1. Pełnomocnik ochrony z Sekretarzem Powiatu ustalą spośród pracowników Starostwa posiadających odpowiednie kwalifikacje i wiedzę pozostałe osoby do pełnienia funkcji w Pionie Ochrony.

2. Obsada osobowa Pionu Ochrony ustalona zostanie odrębnym zarządzeniem.

3. Wyznaczeni pracownicy, wymienieni w ust. 2, obejmują funkcje po spełnieniu wymagań określonych w ustawie o ochronie informacji niejawnych.

4. Zakres zadań pracowników Pionu Ochrony określa załącznik do zarządzenia.

§ 5. Traci moc Zarządzenie Nr 11/201 Starosty Jarocińskiego z dnia 23 lutego 2011r. w sprawie ustalenia Regulaminu Wewnętrznego Pionu Ochrony w Starostwie Powiatowym w Jarocinie.

§ 6. Wykonanie zarządzenia powierzam Pełnomocnikowi Ochrony i Sekretarzowi Powiatu.

§ 7. Zarządzenie wchodzi w życie z dniem podpisania.

STAROSTA
Lidia Czechak

Sprawdzono pod względem prawnym

RADCA PRAWNY
Tomasz Kuderski

Załącznik do Zarządzenia Starosty Jarocińskiego Nr 7/2019 z dnia 21 stycznia 2019 r.

Podstawowy zakres zadań i czynności realizowanych przez pracowników Pionu Ochrony

I. Pełnomocnik ochrony

1. Pełnomocnik ochrony kieruje Pionem Ochrony i podlega bezpośrednio Staroście.
2. Do zadań Pełnomocnika ochrony w szczególności należy:
   a) zapewnienie ochrony informacji niejawnych, w tym stosowanie środków bezpieczeństwa fizycznego w Starostwie;
   b) zapewnienie ochrony Bezpiecznej Stacji Komputerowej;
   c) zarządzanie ryzykiem bezpieczeństwa informacji niejawnych, w tym szacowanie ryzyka;
   d) kontrola ochrony informacji niejawnych oraz przestrzeganie przepisów o ochronie tych informacji;
   e) opracowanie i aktualizowanie dokumentacji ochrony informacji niejawnych w Starostwie;
   f) prowadzenie szkoleń w zakresie ochrony informacji niejawnych;
   g) prowadzenie zwykłych postępowań sprawdzających;
   h) prowadzenie aktualnego wykazu osób w Starostwie, które posiadają dostęp do informacji niejawnych;
   i) współpraca z ABW w zakresie i na zasadach określonych w ustawie o ochronie informacji niejawnych.
3. Ponadto Pełnomocnik ochrony realizuje zadania i korzysta z uprawnień określonych w ustawie o ochronie informacji niejawnych i aktów wykonawczych wydawanych na jej podstawie oraz wykonuje inne zadania zlecone przez Starostę.

II. Kancelista

1. Kancelista obsługuje Kancelarie Niejawną oraz Pion Ochrony i podlega bezpośrednio Pełnomocnikowi ochrony.
2. Do zakresu zadań i obowiązków Kancelisty w szczególności należy:
   a) przyjmowanie, rejestrowanie, przechowywanie i wysyłanie materiałów niejawnych zgodnie z obowiązującymi przepisami;
   b) bezpośredni nadzór nad prawidłowym opracowaniem, obiegiem i przechowywaniem materiałów niejawnych w Starostwie;
   c) przygotowywanie i wysyłanie oraz odbiór korespondencji;
   d) udostępnianie materiałów niejawnych osobom uprawnionym oraz egzekwowanie ich zwrotu;
   e) prowadzenie okresowej kontroli ewidencyjnej udostępnionych z Kancelarii Niejawnej materiałów niejawne w Starostwie;
   f) wykonywanie prac techniczno-ewidencyjnych oraz biurowych dla potrzeb Pionu Ochrony;
   g) porządkowanie i archiwizowanie materiałów niejawnych oraz dokumentacji Pionu Ochrony;
   h) bieżąca kontrola przestrzegania przepisów o ochronie informacji niejawnych przez pracowników Starostwa.
3. W przypadku czasowej nieobecności Kancelisty jego obowiązki przejmuje Pełnomocnik ochrony lub upoważniony przez niego pracownik.
4. Kancelista informuje Pełnomocnika ochrony o wszelkich zdarzeniach związanych lub mogących mieć wpływ na bezpieczeństwo informacji niejawnych w Starostwie.

III. Inspektor bezpieczeństwa teleinformatycznego

1. Inspektor bezpieczeństwa teleinformatycznego, dalej Inspektor, sprawuje bieżący nadzór i kontrolę nad przestrzeganiem zasad ochrony i bezpieczeństwa systemu teleinformatycznego Bezpiecznej Stacji Komputerowej zgodnie z jego dokumentacją bezpieczeństwa i w tym zakresie podlega Pełnomocnikowi Ochrony. Realizuje zadania określone w rozporządzeniu Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego oraz zapisane w akredytowanej dokumentacji bezpieczeństwa systemu teleinformatycznego Bezpiecznej Stacji Komputerowej.
2. Do zakresu zadań i obowiązków Inspektora w szczególności należy:
   a) określanie w porozumieniu z Administratorem systemu technicznych i programowych wymagań, jakie powinno spełniać Bezpieczne Stanowisko Komputerowe;
   b) współuczestniczenie w opracowaniu i aktualizacji dokumentacji bezpieczeństwa teleinformatycznego Bezpiecznej Stacji Komputerowej do przetwarzania informacji niejawnych;
   c) prowadzenie szkoleń osób, które zostały wyznaczone do korzystania z Bezpiecznej Stacji Komputerowej;
   d) kontrolowanie zgodności funkcjonowania Bezpiecznej Stacji Komputerowej ze „Szczegółowymi wymaganiami bezpieczeństwa";
   e) kontrola stanu zabezpieczeń systemu teleinformatycznego Bezpiecznej Stacji Komputerowej w tym prowadzenie analizy rejestru zdarzeń systemu;
   f) kontrolowanie znajomość i przestrzegania przez użytkowników „Procedur bezpiecznej eksploatacji" Bezpiecznej Stacji Komputerowej;

g) prowadzenie dokumentacji wynikającej z „Procedur bezpiecznej eksploatacji" oraz „Szczegółowych wymagań bezpieczeństwa" Bezpiecznej Stacji Komputerowej;
h) weryfikowanie i aktualizowanie dokumentacji bezpieczeństwa Bezpiecznego Stanowiska Komputerowego w zakresie wprowadzenia zmian wpływających na zwiększenie bezpieczeństwa informacji niejawnych.

3. Inspektor w przypadku czasowej nieobecności Administratora systemu i sytuacji wymagającej podjęcia działań przez niego, zastępuje Administratora.
4. Inspektor informuje Pełnomocnika ochrony o wszelkich zdarzeniach związanych lub mogących mieć wpływ na bezpieczeństwo informacji niejawnych w Starostwie.

IV. Administrator systemu

1. Administrator systemu (teleinformatycznego), dalej Administrator, realizuje zadania w zakresie wyposażania systemu teleinformatycznego Bezpiecznej Stacji Komputerowej w mechanizmy lub procedury zapobiegające incydentom bezpieczeństwa teleinformatycznego, w tym zabezpieczające przed działaniem oprogramowania złośliwego, a także umożliwiające jak najszybsze wykrywanie incydentów bezpieczeństwa teleinformatycznego oraz zapewniające niezwłoczne informowanie odpowiednich osób o wykrytym incydencie i w tym zakresie podlega Pełnomocnikowi Ochrony. Realizuje zadania określone w rozporządzeniu Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego oraz zapisane w akredytowanej dokumentacji bezpieczeństwa systemu teleinformatycznego Bezpiecznej Stacji Komputerowej.
2. Do zakresu zadań i obowiązków Administratora w szczególności należy:
a) określanie, w porozumieniu z Inspektorem, technicznych i programowych wymagań, jakie powinno spełniać Bezpieczne Stanowisko Komputerowe;
b) współuczestniczenie w opracowaniu i aktualizacji dokumentacji bezpieczeństwa teleinformatycznego Bezpiecznej Stacji Komputerowej do przetwarzania informacji niejawnych;
c) prowadzenie szkoleń osób, które zostały wyznaczone do korzystania z Bezpiecznej Stacji Komputerowej;
d) instalowanie systemu teleinformatycznego (oprogramowania) i konfiguracji sprzętu Bezpiecznej Stacji Komputerowej;
e) utrzymywać zgodność systemu teleinformatycznego Bezpiecznej Stacji Komputerowej z jego dokumentacją bezpieczeństwa;
f) przydzielenie użytkownikom Bezpiecznej Stacji Komputerowej konta, zgodnie z nadanymi uprawnieniami;
g) czuwanie nad bezawaryjną pracą Bezpiecznej Stacji Komputerowej
h) prowadzenie dokumentacji wynikającej z „Procedur bezpiecznej eksploatacji" oraz „Szczegółowych wymagań bezpieczeństwa" Bezpiecznej Stacji Komputerowej;
i) weryfikowanie i aktualizowanie dokumentacji bezpieczeństwa Bezpiecznego Stanowiska Komputerowego w zakresie wprowadzenia zmian wpływających na zwiększenie bezpieczeństwa informacji niejawnych.

3. Administratora w przypadku czasowej jego nieobecności i sytuacji wymagającej podjęcia natychmiastowych działań zastępuje Inspektora.
4. Administrator informuje Pełnomocnika ochrony o wszelkich zdarzeniach związanych lub mogących mieć wpływ na bezpieczeństwo informacji niejawnych w Starostwie.

STAROSTA
Lidia Czechak