

ZARZĄDZENIE NR 41/2022
STAROSTY SOCHACZEWSKIEGO
z dnia 21 września 2022 roku

Mając na uwadze postanowienia ustawy o ochronie informacji niejawnych z dnia 05 sierpnia 2010 r (tekst jedn. Dz. U. z 2019., poz. 742) (dalej zwaną Ustawą OIN), zarządza się co następuje:

§ 1.

Działając na podstawie art. 52 ust. 1 pkt. 1) Ustawy OIN Kierownik Jednostki Organizacyjnej Starostwa Powiatowego W Sochaczewie powołuję na stanowisko **Inspektora Bezpieczeństwa Teleinformatycznego – Pana Wiesława Mirosława Gorzkiego.**

§ 2.

1. Inspektor Bezpieczeństwa Teleinformatycznego odpowiada za weryfikację i bieżącą kontrolę zgodności funkcjonowania systemu teleinformatycznego przeznaczonego do przetwarzania informacji niejawnych w Starostwie Powiatowym w Sochaczewie.
2. Szczegółowy zakres praw i obowiązków Inspektora Bezpieczeństwa Teleinformatycznego regulują załącznik do niniejszego Zarządzenia.

§ 3.

1. Zarządzenie wchodzi w życie z dniem podpisania

STAROSTA

Jolanta Gonta

Zakres obowiązków
w Pionie Ochrony Informacji Niejawnych

na stanowisku **Inspektora Bezpieczeństwa Teleinformatycznego**

Wymagane dokumenty, uprawnienia:

- poświadczenie bezpieczeństwa osobowego upoważniające do dostępu do informacji niejawnych o klauzuli co najmniej „POUFNE” lub upoważnienie do dostępu do informacji niejawnych o klauzuli „ZASTRZEŻONE” wydane przez Kierownika Jednostki Organizacyjnej;
- szkolenie z ochrony informacji niejawnych przeprowadzone przez Pełnomocnika Ochrony potwierdzone zaświadczeniem zgodnie z art. 20 ustawy o ochronie informacji niejawnych z dnia 5 sierpnia 2010r (tekst jedn. Dz. U. z 2019., poz. 742);
- specjalistyczne szkolenie z zakresu bezpieczeństwa teleinformatycznego organizowanego przez Agencję Bezpieczeństwa Wewnętrznego.

I. OBOWIĄZKI OGÓLNE

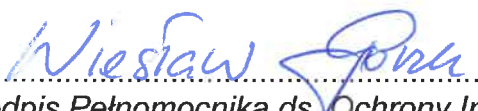
1. Sprawowanie pieczy nad systemem teleinformatycznym zgodnie z ustawą z dnia 05 sierpnia 2010r. o ochronie informacji niejawnych (tekst jedn. Dz. U. z 2019., poz. 742) oraz aktami wykonawczymi do tej ustawy.
2. Przestrzeganie tajemnicy państwowej i służbowej
3. Przestrzeganie zasad bezpieczeństwa i higieny pracy oraz przepisów ppoż.
4. Przestrzeganie przepisów prawa pracy i regulaminu pracy oraz innych postanowień i przepisów wewnętrznych.
5. Przestrzeganie dyscypliny pracy, dbanie o powierzone mienie oraz zachowanie ładu i porządku na stanowisku pracy.
6. Wykonywanie pracy i poleceń przełożonych w sposób zgodny z prawem, optymalnie wykorzystując do tego dostępne środki pracy, wiedzę i doświadczenie zawodowe oraz zasady racjonalnego, a w szczególności ekonomicznego działania.
7. Znajomość obowiązujących przepisów, instrukcji i zarządzeń dotyczących systemów teleinformatycznych.
8. Stałe podnoszenie kwalifikacji zawodowych poprzez zaznajamianie się z publikacjami w prasie i wydawnictwach fachowych, śledzenie i czytanie nowości literatury fachowej oraz inne dostępne formy samokształcenia.

12. Przeprowadzanie okresowej analizy zagrożeń;
13. Tworzenie planów awaryjnych i organizowanie treningów w ich realizacji;
14. Informowanie Pełnomocnika Ochrony o wszelkich zdarzeniach związanych lub mogących mieć związek z bezpieczeństwem systemu TI;
15. Prowadzenie *Dziennika inspektora BTI*

III. ZAKRES ODPOWIEDZIALNOŚCI

Inspektor Bezpieczeństwa Teleinformatycznego odpowiada za realizację powierzonych obowiązków bezpośrednio przed Pełnomocnikiem do spraw ochrony informacji niejawnych. Za naruszanie przepisów o tajemnicy państwowej i służbowej, postanowień Kodeksu Pracy oraz obowiązujących w zakładzie pracy przepisów i zarządzeń mogą być wyciągnięte sankcje karne i dyscyplinarne określone w stosownych przepisach.

Powyższy zakres obowiązków powierzam do stosowania


.....
(Podpis Pełnomocnika ds. Ochrony Informacji Niejawnych)

Oświadczam, że zapoznałem się z powierzonymi obowiązkami i przyjmuję je do wiadomości oraz ciągłego wykonywania.


.....
(Podpis pracownika)

9. Organizowanie pracy na swoim stanowisku w sposób zapewniający prawidłowe i terminowe wykonywanie powierzonych obowiązków oraz stosowanie estetycznych form wykonywania pracy i należytego poszanowania dokumentów.
10. Postępowanie zgodnie ze swoją najlepszą wiedzą, przestrzeganie zasad etyki oraz stosowanie ich wobec współpracowników i kontrahentów firmy.

II. OBOWIĄZKI SZCZEGÓLNE

1. Uczestniczenie w opracowaniu szczególnych wymagań bezpieczeństwa i procedur bezpiecznej eksploatacji.
2. Udział w procesie zarządzania ryzykiem w systemie teleinformatycznym oraz tworzeniu dokumentacji;
3. Nadzorowanie i kontrolowanie konfiguracji systemu, przemieszczania sprzętu oraz prowadzenia jego ewidencji;
4. Przegląd rejestrów systemowych;
5. Kontrolowanie znajomości Procedur Bezpiecznej Eksploatacji przez wszystkich użytkowników systemu teleinformatycznego.
6. Prowadzenie bieżącej z częstotliwością raz na pół roku kontroli zabezpieczeń oraz zgodności funkcjonowania systemu ze Szczególnymi Wymaganiami Bezpieczeństwa.
7. Prowadzenie nadzoru nad szkoleniami z zakresu bezpieczeństwa teleinformatycznego dla użytkowników systemu TI i wspieranie Administratora Systemu w przeprowadzaniu szkoleń.
8. Wykonywanie poleceń Pełnomocnika ds. Ochrony Informacji Niejawnych.
9. Bieżąca kontrola zgodności funkcjonowania systemu TI ze Szczególnymi Wymaganiami Bezpieczeństwa oraz przestrzegania Procedur Bezpiecznej Eksploatacji, w ramach, której sprawdza:
 - Poprawność realizacji zadań przez Administratora Systemu, w szczególności właściwe zarządzanie konfiguracją oraz uprawnieniami przydzielanymi użytkownikom;
 - Znajomość i przestrzeganie przez użytkowników zasad ochrony informacji niejawnych oraz Procedur Bezpiecznej Eksploatacji w systemie TI, a w szczególności w zakresie wykorzystania urządzeń i narzędzi służących do ochrony informacji niejawnych w systemie;
 - Stan zabezpieczeń systemu TI, w szczególności analizując rejestry zdarzeń systemu TI;
10. Monitorowanie zmian (np. w funkcjonowaniu mechanizmów zabezpieczeń, aktualizacji oprogramowania itp.);
11. Reagowanie na sygnały o incydentach w zakresie bezpieczeństwa, wyjaśnianie ich przyczyn, okresowe przeglądanie i dokumentowanie logów systemowych;