

ZARZĄDZENIE NR 40/2022
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 2019r. 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 **Administradora Systemu Teleinformatycznego – Pana Tomasza Tarasa.**

§ 2.

1. Administrator 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 Administratora 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 **Administradora Systemu Teleinformatycznego**

Wymagane kwalifikacje: - wykształcenie wyższe, specjalność informatyka lub elektronika.

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.
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. Okresowej analizy zagrożeń systemu teleinformatycznego w celu określenia ryzyka mającego wpływ na bezpieczeństwo systemu, określając czy są one w dalszym ciągu akceptowalne czy też wymagane są nowe środki zaradcze celem ich wyeliminowania
2. Administrator Systemu jest odpowiedzialny przed Pełnomocnikiem Ochrony oraz Kierownikiem Jednostki Organizacyjnej Starostwa Powiatowego w Sochaczewie za bezpieczeństwo systemu teleinformatycznego „BSK-Z”.
3. Do obowiązków Administratora Systemu należy zapewnienie by wszyscy użytkownicy stosowali się do Procedur Bezpiecznej Eksploatacji.
4. Szczegółowy zakres odpowiedzialności i obowiązków jest następujący:
 - Udział w procesie zarządzania ryzykiem w systemie TI oraz tworzeniu dokumentacji bezpieczeństwa systemu;
 - Utrzymaniu zgodności dokumentacji bezpieczeństwa z konfiguracją systemu TI;
 - Tworzenie i usuwanie kont użytkowników (na polecenie Kierownika Jednostki Organizacyjnej lub uprawnionego przez niego pracownika), wdrażanie uprawnień w systemie wynikających z przydzielonych praw dostępu, przydzielane pierwszych haseł;
 - Szkolenie użytkowników;
 - Konfigurowanie urządzeń i oprogramowania;
 - Monitorowanie zmian (np. w funkcjonowaniu mechanizmów zabezpieczeń);
 - Reagowanie na sygnały o incydentach w zakresie bezpieczeństwa wyjaśnianie przyczyn i usuwanie ich skutków;
 - Prowadzenie ewidencji sprzętu, oprogramowania i nośników danych;
 - Tworzenie kopii zapasowych (bezpieczeństwa) danych i systemu;
 - Informowanie przełożonych, w tym Inspektora BTI, o wszelkich zdarzeniach związanych lub mogących mieć związek z bezpieczeństwem systemu TI;
 - Utrzymanie i aktualizację list autoryzowanych użytkowników systemu teleinformatycznego;
 - Zapewnienie zgodności ze Szczególnymi Wymaganiami Bezpieczeństwa systemu;
 - Doradzanie użytkownikom systemu w zakresie bezpieczeństwa;
 - Przygotowanie i archiwizowanie „Oświadczeń osób zapoznanych z Procedurami Bezpiecznej Eksploatacji”, który jest podpisywany przez wszystkich użytkowników systemu „BSK-Z”;

- Sprawdzanie i zapewnienie by niejawne odpady były niszczone w regularnych odstępach czasu, zgodnie z procedurami zawartymi w obowiązujących unormowaniach w tym zakresie;
- Przygotowywanie i utrzymywanie „Dziennika administratora systemu” zawierających wszystkie usługi serwisowe wykonane na sprzęcie;
- Przeprowadzanie kontroli i utrzymywanie ewidencji tych sprawdzeń, dotyczących obecności klasyfikowanych mediów magnetycznych i poprawności ich opisu;
- Meldowanie do Pełnomocnika Ochrony o wszelkich wykrytych lukach, naruszeniach i zagrożeniach;
- Wspieranie Kierownika Kancelarii Informacji Niejawnych w zakresie zarządzania nośnikami informacji niejawnych.

III. ZAKRES ODPOWIEDZIALNOŚCI

Administrator Systemu Teleinformatycznego odpowiada za realizację powierzonych obowiązków bezpośrednio przed Kierownikiem Jednostki Organizacyjnej.

Powyższy zakres obowiązków powierzam do stosowania

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

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

.....
Tomasz Tom
 (Podpis pracownika)