

Zarządzenie Nr 130/23
Marszałka Województwa Świętokrzyskiego
z dnia 19 października 2023 r.

w sprawie powołania w Urzędzie Marszałkowskim Województwa Świętokrzyskiego w Kielcach Administratora Systemu Teleinformatycznego oraz Inspektora Bezpieczeństwa Teleinformatycznego dla Bezpiecznego Stanowiska Komputerowego.

Na podstawie art. 52 ust. 1 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (t. j. Dz. U. z 2023 r., poz. 756 z późn. zm.) oraz 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), oraz § 8 Regulaminu Organizacyjnego Urzędu Marszałkowskiego Województwa Świętokrzyskiego w Kielcach, stanowiącego załącznik do uchwały Nr 6525/23 Zarządu Województwa Świętokrzyskiego z dnia 21 stycznia 2023 r., w sprawie przyjęcia tekstu jednolitego Regulaminu Organizacyjnego Urzędu Marszałkowskiego Województwa Świętokrzyskiego w Kielcach z późn. zm., zarządza się co następuje:

§ 1

Wyznaczam **Pana Krzysztofa Ceglińskiego** głównego specjalistę w Departamencie IT na Administratora Systemu Teleinformatycznego Bezpiecznego Stanowiska Komputerowego (dalej: BSK) odpowiedzialnego za funkcjonowanie systemu teleinformatycznego oraz za przestrzeganie zasad i wymagań bezpieczeństwa przewidzianych dla systemu teleinformatycznego.

§ 2

Wyznaczam **Pana Cezarego Kuśmierza** inspektora w Biurze Spraw Obronnych, Bezpieczeństwa i Ochrony Informacji Niejawnych (dalej: BSO) na Inspektora Bezpieczeństwa Teleinformatycznego BSK odpowiedzialnego za opracowanie, weryfikację i bieżącą kontrolę zgodności funkcjonowania systemu teleinformatycznego ze *Szczególnymi Wymaganiami Bezpieczeństwa* oraz przestrzegania *Procedur Bezpiecznej Eksploatacji*.

§ 3

Administrator Systemu Teleinformatycznego BSK realizując zadania polegające na zapewnieniu funkcjonowania oraz przestrzegania zasad bezpieczeństwa systemu teleinformatycznego, w szczególności:

- 1) bierze udział w tworzeniu i aktualizacji dokumentacji bezpieczeństwa systemu oraz w procesie zarządzania ryzykiem w systemie;
- 2) wdraża zabezpieczenia sytemu oraz procedury jego bezpiecznej eksploatacji;
- 3) utrzymuje zgodność konfiguracji i parametrów systemu z jego dokumentacją bezpieczeństwa;
- 4) analizuje rejestr zdarzeń w systemie;
- 5) tworzy kopie bezpieczeństwa;
- 6) reaguje na sygnały o incydentach w zakresie bezpieczeństwa teleinformatycznego i ochrony informacji niejawnych oraz usuwa ich skutki;
- 7) prowadzi na bieżąco wykaz osób mających dostęp do systemu teleinformatycznego oraz przydziela użytkownikom konta na wniosek Pełnomocnika ds. Ochrony Informacji Niejawnych;
- 8) realizuje szkolenia użytkowników BSK z zakresu procedur bezpiecznej eksploatacji;
- 9) zapewnienia ciągłość działania BSK poprzez przeglądy okresowe BSK i bieżącą konserwację, aktualizację oprogramowania, monitoring awarii systemu i niezwłoczną naprawę;
- 10) prowadzi dokumentację eksploatacyjną systemu;
- 11) informuje Pełnomocnika ds. Ochrony Informacji Niejawnych Ochrony oraz Inspektora Bezpieczeństwa Teleinformatycznego BSK o wszystkich zdarzeniach związanych lub mogących mieć związek z bezpieczeństwem i przetwarzaniem informacji niejawnych w BSK.

§ 4

Do obowiązków Inspektora Bezpieczeństwa Teleinformatycznego BSK w zakresie opracowania oraz bieżącej kontroli zgodności funkcjonowania systemu teleinformatycznego z jego dokumentacją bezpieczeństwa należy w szczególności:

- 1) opracowanie i wdrożenie dokumentów: *Szczególne Wymagania Bezpieczeństwa i Procedury Bezpiecznej Eksploatacji*;
- 2) organizowanie i prowadzenie szkolenia z użytkownikami w zakresie ochrony informacji niejawnych wytwarzanych, przetwarzanych i przechowywanych w systemie;
- 3) kontrolę znajomości procedur bezpieczeństwa przez wszystkich użytkowników BSK;
- 4) zapewnienie dostępu do BSK wyłącznie osobom posiadającym upoważnienie bądź poświadczenia bezpieczeństwa;

- 5) sprawowanie nadzoru nad konfiguracją systemu, przemieszczaniem sprzętu oraz nad prowadzeniem jego ewidencji;
- 6) sprawdzanie zgodności stanu faktycznego ze *Szczególnymi Wymaganiami Bezpieczeństwa* oraz kontrolę przestrzegania *Procedur Bezpieczeństwa*;
- 7) monitorowanie zmian dotyczących mechanizmów zabezpieczeń;
- 8) reagowanie na sygnały o incydentach w zakresie bezpieczeństwa, wyjaśnienie ich przyczyny;
- 9) prowadzenie okresowej analizy zagrożeń i szacowanie ryzyka dla bezpieczeństwa informacji niejawnych;
- 10) informowanie Pełnomocnika ds. Ochrony Informacji Niejawnych Ochrony o wszelkich zdarzeniach, związanych lub mogących mieć wpływ na bezpieczeństwo BSK;
- 11) prowadzenie dokumentacji zgodnej ze *Szczególnymi Wymaganiami Bezpieczeństwa*;
- 12) nadzór nad bieżącą konserwacją BSK, a także przeglądami realizowanymi przez Administratora BSK oraz prowadzenie spraw związanych ze zleceniami w zakresie napraw elementów wchodzących w skład BSK;
- 13) zlecenie i monitorowanie bieżącej konserwacji i naprawy środków bezpieczeństwa fizycznego w celu ochrony informacji niejawnych przetwarzanych w BSO UMWŚ.

§ 5

Nadzór nad wykonaniem Zarządzenia powierza się Pełnomocnikowi ds. Ochrony Informacji Niejawnych.

§ 6

Zarządzenie wchodzi w życie z dniem podpisania.

Marszałek Województwa Świętokrzyskiego

Andrzej Bętkowski

/dokument podpisano elektronicznie/

Potwierdzenie zgodności kopii z dokumentem elektronicznym:

Znak pisma dokumentu: OK-I.120.130.2023
Identyfikator dokumentu: 2249603
Nazwa dokumentu: ZARZĄDZENIE BSK ADMINISTRATOR I
INSPEKTOR 1.2.DOC
Suma kontrolna SHA256 dokumentu: 925029a01ac863f9674d935f29caaac4f6698f2d44
18f7dca66a7ad0b12c57a6

Wydrukował(a): Lidia Skrzeczyna OK-I

Data wydruku: 2023-10-20 08:22:56

Podpisy dokumentu:

.....
Andrzej Krzysztof Bętkowski

Data podpisu: 2023-10-19 15:15:28

Rodzaj podpisu: Kwalifikowany podpis elektroniczny

Numer certyfikatu: 668391214802324668076174841025955321103462527975

Wystawca certyfikatu: Krajowa Izba Rozliczeniowa S.A.