ZARZĄDZENIE Nr 46/2026
Wójta Gminy Ciechanów
z dnia 10.07.2026 roku

w sprawie zatwierdzenia dokumentacji bezpieczeństwa systemu teleinformatycznego w Urzędzie Gminy Ciechanów, udzielenia akredytacji bezpieczeństwa dla systemu teleinformatycznego „Bezpieczne Stanowisko Komputerowe" przeznaczonego do przetwarzania informacji niejawnych o klauzuli „zastrzeżone" oraz wycofania z eksploatacji dotychczasowego systemu teleinformatycznego do przetwarzania informacji niejawnych

Na podstawie art. 33 ust. 3 i 5 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (tekst jedn.: Dz. U. z 2025 r. poz. 1153 ze zm.), art. 14 ust. 1, art. 48 ust. 9, art. 49 ust. 1–3 oraz art. 52 ust. 1 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (tekst jedn.: Dz. U. z 2025 r. poz. 1209 ze zm.), a także § 18 ust. 6, § 25 i § 26 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), zarządzam, co następuje:

§ 1.

1. Zatwierdzam dokumentację bezpieczeństwa systemu teleinformatycznego przeznaczonego do przetwarzania informacji niejawnych o klauzuli „zastrzeżone" pod nazwą **„Bezpieczne Stanowisko Komputerowe"**, obejmującą:
   1) **Szczególne Wymagania Bezpieczeństwa Systemu Teleinformatycznego „Bezpieczne Stanowisko Komputerowe"**, stanowiące załącznik nr 1 do niniejszego zarządzenia;
   2) **Procedury Bezpiecznej Eksploatacji Systemu Teleinformatycznego „Bezpieczne Stanowisko Komputerowe"**, stanowiące załącznik nr 2 do niniejszego zarządzenia.
2. Udzielam akredytacji bezpieczeństwa teleinformatycznego dla systemu teleinformatycznego **„Bezpieczne Stanowisko Komputerowe"** w Urzędzie Gminy Ciechanów, przeznaczonego do przetwarzania informacji niejawnych o klauzuli **„zastrzeżone"**, na okres 5 lat, tj. **do dnia 9.07.2031 r.**
3. System teleinformatyczny, o którym mowa w ust. 1 i 2, może być wykorzystywany wyłącznie do przetwarzania informacji niejawnych o klauzuli **„zastrzeżone"**, zgodnie z zatwierdzoną dokumentacją bezpieczeństwa.
4. Wszystkich użytkowników systemu zobowiązuje się do ścisłego przestrzegania zasad określonych w dokumentacji bezpieczeństwa, o której mowa w ust. 1, oraz zasad ochrony informacji niejawnych obowiązujących w Urzędzie Gminy Ciechanów.

§ 2.

1. Dokumentację bezpieczeństwa systemu teleinformatycznego „Bezpieczne Stanowisko Komputerowe" przechowuje Pełnomocnik ds. Ochrony Informacji Niejawnych.
2. Pełnomocnik ds. Ochrony Informacji Niejawnych odpowiada za zapewnienie aktualności dokumentacji bezpieczeństwa oraz jej zgodności ze stanem faktycznym, organizacyjnym i technicznym systemu.
3. Wszelkie zmiany w konfiguracji systemu, sposobie jego eksploatacji, zakresie przetwarzanych informacji, wykorzystywanych zabezpieczeniach lub osobach pełniących

funkcje związane z bezpieczeństwem systemu wymagają uprzedniej analizy pod kątem konieczności aktualizacji dokumentacji bezpieczeństwa.

§ 3.

Wyznaczam osoby odpowiedzialne za planowanie, wdrażanie, eksploatację oraz nadzór nad bezpieczeństwem systemu teleinformatycznego *„Bezpieczne Stanowisko Komputerowe"*:

1) **Radosław Lipowski** – Pełnomocnik ds. Ochrony Informacji Niejawnych / Inspektor Bezpieczeństwa Teleinformatycznego
2) **Tomasz Mielnicki** – Administrator Systemu
3) **Ilona Mróz** – Pracownik Kancelarii Materiałów Niejawnych.

§ 4.

Do zadań Administratora Systemu należy w szczególności:

1) instalacja, konfiguracja i techniczne utrzymanie systemu teleinformatycznego;
2) zakładanie, modyfikowanie, blokowanie i usuwanie kont użytkowników;
3) przydzielanie użytkownikom uprawnień zgodnie z zatwierdzonymi wnioskami o nadanie lub odebranie uprawnień;
4) szkolenie użytkowników z zasad korzystania z systemu teleinformatycznego w zakresie technicznym;
5) obsługa techniczna systemu oraz okresowe sprawdzanie poprawności działania zastosowanych zabezpieczeń;
6) wdrażanie i stosowanie procedur bezpieczeństwa oraz procedur ochrony przed szkodliwym oprogramowaniem;
7) aktualizacja systemu operacyjnego, oprogramowania użytkowego oraz oprogramowania antywirusowego, zgodnie z zasadami określonymi w dokumentacji bezpieczeństwa;
8) niezwłoczne informowanie Pełnomocnika ds. Ochrony Informacji Niejawnych oraz Inspektora Bezpieczeństwa Teleinformatycznego o stwierdzonych naruszeniach bezpieczeństwa systemu, awariach, nieprawidłowościach oraz wykrytym szkodliwym oprogramowaniu.

§ 5.

Do zadań Inspektora Bezpieczeństwa Systemu Teleinformatycznego należy w szczególności:

1) nadzór nad konfiguracją systemu teleinformatycznego;
2) kontrola przestrzegania Procedur Bezpiecznej Eksploatacji;
3) kontrola zastosowanych zabezpieczeń systemu teleinformatycznego;
4) udział w szacowaniu ryzyka oraz ocenie wpływu zmian organizacyjnych lub technicznych na bezpieczeństwo systemu;
5) opiniowanie zmian w dokumentacji bezpieczeństwa systemu;
6) współpraca z Administratorem Systemu i Pełnomocnikiem ds. Ochrony Informacji Niejawnych w przypadku wystąpienia incydentu, awarii lub podejrzenia naruszenia bezpieczeństwa systemu.

§ 6.

Do zadań Pełnomocnika ds. Ochrony Informacji Niejawnych należy w szczególności:

1) zapewnienie przestrzegania zasad ochrony informacji niejawnych przetwarzanych, przechowywanych lub przekazywanych w systemie teleinformatycznym;

2) nadzór nad właściwym obiegiem dokumentów niejawnych oraz informatycznych nośników danych;
3) zapewnienie bezpieczeństwa fizycznego obszaru, w którym zlokalizowany jest system teleinformatyczny;
4) zapewnienie, aby dostęp do systemu teleinformatycznego posiadały wyłącznie osoby mające wymagane uprawnienia do dostępu do informacji niejawnych oraz przeszkolone w zakresie zasad korzystania z systemu;
5) nadzór nad prowadzeniem ewidencji związanych z dostępem do systemu, nośnikami danych, kluczami oraz materiałami niejawnymi;
6) prowadzenie lub nadzorowanie postępowań wyjaśniających w przypadku wystąpienia naruszenia bezpieczeństwa systemu teleinformatycznego albo podejrzenia naruszenia zasad ochrony informacji niejawnych;
7) nadzór nad czynnościami związanymi z wycofaniem dotychczasowego systemu teleinformatycznego z eksploatacji.

§ 7.

Do zadań Pracownika Kancelarii Materiałów Niejawnych należy w szczególności:

1) wydawanie nośników USB, kluczy, dokumentów oraz innych materiałów niejawnych związanych z eksploatacją systemu, a także przyjmowanie ich zwrotu po zakończeniu pracy;
2) prowadzenie *Ewidencji pobrań kluczy i stanowiska BSK*, obejmującej w szczególności pobranie i zwrot kluczy, stanowiska, nośników danych oraz innych materiałów związanych z użytkowaniem systemu;
3) sprawdzanie, czy nośniki danych przeznaczone do użycia w systemie zostały prawidłowo oznaczone, zarejestrowane i dopuszczone do użytkowania;
4) dokonywanie rejestracji informatycznych nośników danych oraz dokumentów wykonanych w systemie, zgodnie z obowiązującymi zasadami ewidencjonowania materiałów niejawnych;
5) przechowywanie nośników danych i dokumentów niejawnych w sposób uniemożliwiający dostęp osób nieuprawnionych;
6) udział w czynnościach związanych z niszczeniem informatycznych nośników danych oraz dokumentów niejawnych wykonanych lub przetwarzanych w systemie;
7) współpraca z Pełnomocnikiem ds. Ochrony Informacji Niejawnych, Administratorem Systemu oraz Inspektorem Bezpieczeństwa Teleinformatycznego w zakresie bieżącego zabezpieczenia materiałów niejawnych i nośników danych.

§ 8.

1. Użytkownicy systemu, przed uzyskaniem fizycznego i logicznego dostępu do systemu teleinformatycznego, są zobowiązani odbyć dodatkowe szkolenie w zakresie jego funkcjonowania, zasad bezpiecznej eksploatacji oraz warunków ochrony informacji niejawnych przetwarzanych w systemie.
2. Szkolenie, o którym mowa w ust. 1, prowadzi Administrator Systemu, Inspektor Bezpieczeństwa Teleinformatycznego albo inna osoba wyznaczona przez Pełnomocnika ds. Ochrony Informacji Niejawnych.

§ 9.

1. Użytkownicy systemu teleinformatycznego „Bezpieczne Stanowisko Komputerowe" ponoszą odpowiedzialność za przestrzeganie przepisów prawa, dokumentacji bezpieczeństwa oraz zasad ochrony informacji niejawnych podczas korzystania z systemu.
2. Użytkownik systemu jest obowiązany w szczególności do:
   1) korzystania z systemu wyłącznie w zakresie posiadanych uprawnień;
   2) ochrony indywidualnych danych uwierzytelniających;
   3) korzystania wyłącznie z dopuszczonych i zarejestrowanych nośników danych;
   4) niezwłocznego zgłaszania wszelkich nieprawidłowości, awarii, incydentów oraz podejrzeń naruszenia bezpieczeństwa systemu;
   5) przestrzegania zasad postępowania z dokumentami i nośnikami zawierającymi informacje niejawne.

§ 10.

1. Z dniem 30.06.2026 r. wycofuje się z eksploatacji dotychczasowy system teleinformatyczny wykorzystywany w Urzędzie Gminy Ciechanów do przetwarzania informacji niejawnych o klauzuli „zastrzeżone".
2. Od dnia wycofania dotychczasowego systemu z eksploatacji zabrania się jego dalszego wykorzystywania do bieżącego tworzenia, przetwarzania, utrwalania, kopiowania, przechowywania lub przekazywania informacji niejawnych, z wyjątkiem czynności niezbędnych do:
   1) zabezpieczenia danych;
   2) wykonania kopii zabezpieczającej;
   3) przeniesienia danych do nowego systemu;
   4) rozliczenia użytkowników, nośników, dokumentów i materiałów;
   5) zamknięcia eksploatacji systemu;
   6) sporządzenia protokołu wycofania systemu z eksploatacji.
3. Czynności, o których mowa w ust. 2, mogą wykonywać wyłącznie osoby upoważnione, posiadające wymagane uprawnienia do dostępu do informacji niejawnych oraz wyznaczone do realizacji czynności związanych z wycofaniem systemu.

§ 11.

1. W celu przeprowadzenia czynności związanych z wycofaniem dotychczasowego systemu teleinformatycznego z eksploatacji powołuję Komisję w składzie:
   1) **Radosław Lipowski** – Przewodniczący Komisji / Pełnomocnik ds. Ochrony Informacji Niejawnych / Inspektor Bezpieczeństwa Teleinformatycznego;
   2) **Tomasz Mielnicki** – Administrator Systemu;
   3) **Iiona Mróz** – Pracownik Kancelarii Materiałów Niejawnych;
   4) **Dorota Filipowicz** – członek Komisji.
2. Do zadań Komisji należy w szczególności:
   1) ustalenie faktycznego stanu dotychczasowego systemu na dzień rozpoczęcia czynności wycofania;
   2) sporządzenie wykazu sprzętu, oprogramowania, nośników danych, kont użytkowników, kopii zabezpieczających oraz dokumentacji związanej z systemem;
   3) zabezpieczenie danych przetwarzanych w dotychczasowym systemie;
   4) nadzorowanie przeniesienia danych do systemu „Bezpieczne Stanowisko Komputerowe" albo zabezpieczenie danych w innej dopuszczalnej formie;

5) sprawdzenie kompletności, integralności i czytelności przeniesionych danych;
6) rozliczenie użytkowników z nośników, kopii, materiałów, kluczy oraz dostępu do systemu;
7) wskazanie nośników przeznaczonych do dalszego przechowywania, archiwizacji, wykorzystania, wycofania albo zniszczenia;
8) sporządzenie protokołu wycofania dotychczasowego systemu teleinformatycznego z eksploatacji.

§ 12.

1. Przed zakończeniem eksploatacji dotychczasowego systemu Administrator Systemu, pod nadzorem Pełnomocnika ds. Ochrony Informacji Niejawnych oraz Inspektora Bezpieczeństwa Teleinformatycznego, dokonuje zabezpieczenia danych znajdujących się w tym systemie.
2. Zabezpieczenie danych obejmuje w szczególności:
   1) identyfikację danych, plików użytkowych, katalogów, kopii oraz dokumentów elektronicznych znajdujących się w dotychczasowym systemie;
   2) ustalenie użytkowników odpowiedzialnych za poszczególne katalogi i pliki;
   3) wykonanie kopii zabezpieczającej danych na zarejestrowanym i odpowiednio oznaczonym informatycznym nośniku danych;
   4) oznaczenie nośnika klauzulą tajności odpowiadającą najwyższej klauzuli informacji znajdujących się na tym nośniku;
   5) wpisanie nośnika do właściwych ewidencji prowadzonych w Kancelarii Materiałów Niejawnych;
   6) zabezpieczenie nośnika w szafie metalowej znajdującej się w Kancelarii Materiałów Niejawnych;
   7) odnotowanie wykonanych czynności w protokole wycofania systemu.
3. Przeniesienie danych do systemu „Bezpieczne Stanowisko Komputerowe" może nastąpić wyłącznie po zatwierdzeniu dokumentacji bezpieczeństwa tego systemu oraz udzieleniu mu akredytacji bezpieczeństwa teleinformatycznego.
4. Przeniesienie danych powinno zostać wykonane w sposób zapewniający zachowanie poufności, integralności, dostępności i rozliczalności informacji niejawnych.
5. Po przeniesieniu danych Komisja dokonuje weryfikacji:
   1) kompletności przeniesionych danych;
   2) możliwości ich odczytu w nowym systemie;
   3) zgodności przeniesionych danych z wykazem danych zabezpieczonych w dotychczasowym systemie;
   4) poprawności oznaczeń klauzul tajności;
   5) prawidłowości nadania uprawnień użytkownikom w nowym systemie.
6. Wyniki weryfikacji, o której mowa w ust. 5, zamieszcza się w protokole wycofania systemu.

§ 13.

1. Po zakończeniu czynności zabezpieczenia i przeniesienia danych Komisja dokonuje oceny dalszego sposobu postępowania ze sprzętem, dyskiem twardym, nośnikami danych, kopiami zabezpieczającymi, nośnikami instalacyjnymi oraz dokumentacją dotychczasowego systemu.
2. Nośniki nienadające się do dalszego użycia, zbędne albo przeznaczone do likwidacji niszczy się w sposób uniemożliwiający odtworzenie zapisanych na nich informacji, zgodnie z

dokumentacją bezpieczeństwa oraz obowiązującymi zasadami ochrony informacji niejawnych.

3. Dokumentacja bezpieczeństwa dotychczasowego systemu, po jego wycofaniu z eksploatacji, podlega zabezpieczeniu i dalszemu przechowywaniu jako dokumentacja systemu wycofanego z użytkowania.

§ 14.

1. Z czynności wycofania dotychczasowego systemu teleinformatycznego z eksploatacji sporządza się protokół.
2. Protokół, po podpisaniu przez członków Komisji, przedkłada się Wójtowi Gminy Ciechanów do zatwierdzenia.

§ 15.

3. Wykonanie zarządzenia powierzam Pełnomocnikowi ds. Ochrony Informacji Niejawnych.
4. Administrator Systemu odpowiada za techniczne przygotowanie systemu „Bezpieczne Stanowisko Komputerowe" do eksploatacji oraz za czynności techniczne związane z zabezpieczeniem i przeniesieniem danych z dotychczasowego systemu.
5. Inspektor Bezpieczeństwa Teleinformatycznego odpowiada za bieżącą kontrolę zgodności czynności technicznych z dokumentacją bezpieczeństwa oraz wymaganiami bezpieczeństwa teleinformatycznego.
6. Pracownik Kancelarii Materiałów Niejawnych odpowiada za ewidencjonowanie, wydawanie, przyjmowanie i zabezpieczanie nośników, dokumentów oraz materiałów niejawnych związanych z systemem.

§ 16.

Treść załączników do niniejszego zarządzenia stanowi wewnętrzną dokumentację bezpieczeństwa systemu teleinformatycznego oraz dokumentację związaną z ochroną informacji niejawnych i nie podlega publikacji w Biuletynie Informacji Publicznej z uwagi na charakter informacji w nich zawartych oraz konieczność zapewnienia bezpieczeństwa systemu teleinformatycznego.

§ 17.

Traci moc zarządzenie Nr 36/21 Wójta Gminy Ciechanów z dnia 9.07.2021 roku w sprawie zatwierdzenia dokumentacji bezpieczeństwa systemu teleinformatycznego w Urzędzie Gminy Ciechanów i udzielenia akredytacji bezpieczeństwa dla systemu teleinformatycznego „Bezpieczne Stanowisko Komputerowe" przeznaczonego do przetwarzania informacji niejawnych o klauzuli „zastrzeżone".

§ 18.

Zarządzenie wchodzi w życie z dniem podpisania.

WÓJT GMINY
Stefan Pawłowski

GMINA CIECHANÓW
06-400 Ciechanów
ul. Fabryczna 8
tel./fax 23 672 26 46