

Zarządzenie Nr 52/2026

Wójta Gminy Ciechanów

z dnia 29 lipca 2026 r.

w sprawie ustanowienia i wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Gminy Ciechanów

Na podstawie art. 30 ust. 1, art. 31 oraz art. 33 ust. 3 i 5 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2026 r. poz. 662), w związku z § 19 i § 20 rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. poz. 773), a także art. 24 i art. 32 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE zarządza się, co następuje:

§ 1

1. W Urzędzie Gminy Ciechanów, zwanym dalej „Urzędem”, ustanawia się i wdraża System Zarządzania Bezpieczeństwem Informacji, zwany dalej „SZBI”.
2. SZBI obejmuje wszystkie informacje przetwarzane w związku z realizacją zadań Urzędu, niezależnie od:
 - 1) ich postaci, w szczególności papierowej, elektronicznej, ustnej, wizualnej lub audiowizualnej;
 - 2) miejsca ich przetwarzania;
 - 3) wykorzystywanego systemu, urządzenia, nośnika lub kanału komunikacji;
 - 4) tego, czy informacje są przetwarzane przez pracowników Urzędu, osoby wykonujące zadania na podstawie umów cywilnoprawnych, podmioty zewnętrzne lub inne osoby działające z upoważnienia Urzędu.
3. SZBI obejmuje w szczególności:
 - 1) pracowników Urzędu oraz inne osoby wykonujące zadania na rzecz Urzędu;
 - 2) komórki organizacyjne i samodzielne stanowiska pracy;
 - 3) systemy teleinformatyczne, sieci, urządzenia, oprogramowanie oraz usługi informatyczne;
 - 4) dokumentację papierową i elektroniczną;
 - 5) pomieszczenia, obiekty oraz strefy, w których przetwarzane lub przechowywane są informacje;
 - 6) usługi realizowane przez dostawców i podmioty zewnętrzne, jeżeli mają wpływ na bezpieczeństwo informacji Urzędu.

§ 2

1. Celem SZBI jest zapewnienie odpowiedniego poziomu bezpieczeństwa informacji przetwarzanych w Urzędzie, w szczególności ich: poufności, integralności, dostępności, autentyczności, rozliczalności, niezaprzeczalności, niezawodności.
2. SZBI służy w szczególności:
 - 1) identyfikowaniu informacji, aktywów informacyjnych, zagrożeń i podatności;
 - 2) systematycznemu zarządzaniu ryzykiem dla bezpieczeństwa informacji;
 - 3) zapewnieniu ciągłości realizacji zadań publicznych;
 - 4) zapobieganiu incydentom bezpieczeństwa informacji oraz ograniczaniu ich skutków;
 - 5) zapewnieniu zgodności z przepisami prawa, wymaganiami umownymi i regulacjami wewnętrznymi;
 - 6) zapewnieniu właściwego zarządzania dostępem do informacji;
 - 7) podnoszeniu świadomości pracowników w zakresie bezpieczeństwa informacji i cyberbezpieczeństwa;
 - 8) ciągłemu monitorowaniu, przeglądaniu, utrzymywaniu i doskonaleniu przyjętych zabezpieczeń.

§ 3

1. Dokumentację SZBI stanowią w szczególności:
 - 1) Polityka Bezpieczeństwa Informacji;
 - 2) polityki, instrukcje, procedury, regulaminy i wytyczne dotyczące bezpieczeństwa informacji;
 - 3) metodyka zarządzania ryzykiem dla bezpieczeństwa informacji;
 - 4) rejestry aktywów informacyjnych, systemów, sprzętu, oprogramowania i usług;
 - 5) wyniki analiz i ocen ryzyka oraz plany postępowania z ryzykiem;
 - 6) zasady zarządzania dostępem i uprawnieniami;
 - 7) zasady reagowania na incydenty bezpieczeństwa informacji i cyberbezpieczeństwa;
 - 8) zasady wykonywania, przechowywania i testowania kopii zapasowych;
 - 9) zasady zapewnienia ciągłości działania i odtwarzania po awarii;
 - 10) zasady bezpieczeństwa fizycznego i środowiskowego;
 - 11) zasady bezpiecznego korzystania z poczty elektronicznej, Internetu, urządzeń mobilnych, nośników danych i pracy zdalnej;
 - 12) zasady współpracy z dostawcami i podmiotami zewnętrznymi;
 - 13) plany szkoleń, audytów, przeglądów i działań doskonalących;
 - 14) rejestry incydentów, niezgodności, działań korygujących i działań doskonalących;
 - 15) protokoły, raporty oraz inne dowody funkcjonowania SZBI.
2. Dokumentacja SZBI może być prowadzona w postaci papierowej lub elektronicznej, z zapewnieniem ochrony właściwej dla jej treści i przeznaczenia.
3. Szczegółowe dokumenty składające się na SZBI zatwierdza Wójt Gminy Ciechanów.
4. Sekretarz Gminy zapewnia prowadzenie aktualnego wykazu obowiązujących dokumentów SZBI, obejmującego co najmniej nazwę dokumentu, oznaczenie wersji, datę zatwierdzenia, właściciela dokumentu i termin jego przeglądu.

5. Dokumentacja SZBI podlega przeglądowi nie rzadziej niż raz w roku oraz każdorazowo w przypadku:
- 1) istotnej zmiany przepisów prawa lub wymagań właściwych dla Urzędu;
 - 2) zmiany organizacyjnej, technologicznej, kadrowej lub lokalowej mogącej wpływać na bezpieczeństwo informacji;
 - 3) wdrożenia albo istotnej modyfikacji systemu teleinformatycznego, usługi lub procesu;
 - 4) wystąpienia poważnego incydentu lub naruszenia bezpieczeństwa informacji;
 - 5) stwierdzenia niezgodności w wyniku audytu, kontroli lub przeglądu;
 - 6) zidentyfikowania nowych zagrożeń, podatności lub istotnej zmiany poziomu ryzyka..

§ 4

1. Wójt Gminy Ciechanów ponosi odpowiedzialność za ustanowienie, wdrożenie, funkcjonowanie i doskonalenie SZBI w Urzędzie.
2. Do zadań Wójta Gminy Ciechanów należy w szczególności:
 - 1) zatwierdzanie dokumentacji SZBI, wyników analiz ryzyka i planów postępowania z ryzykiem;
 - 2) podejmowanie decyzji dotyczących akceptacji ryzyka oraz wdrażania zabezpieczeń;
 - 3) przydzielanie zadań z zakresu bezpieczeństwa informacji i nadzorowanie ich wykonania;
 - 4) zapewnienie, w granicach dostępnych środków, zasobów organizacyjnych, kadrowych, technicznych i finansowych niezbędnych do funkcjonowania SZBI;
 - 5) zapewnienie, aby pracownicy znali swoje obowiązki i posiadali kompetencje adekwatne do wykonywanych zadań;
 - 6) dokonywanie okresowego przeglądu SZBI i podejmowanie decyzji w sprawie jego doskonalenia;
 - 7) zapewnienie zgodności działania Urzędu z przepisami prawa oraz wewnętrznymi regulacjami w zakresie bezpieczeństwa informacji.
3. Powierzenie wykonywania określonych zadań innym osobom nie wyłącza odpowiedzialności Wójta Gminy Ciechanów za funkcjonowanie SZBI.

§ 5

1. Sekretarz Gminy koordynuje od strony organizacyjnej funkcjonowanie SZBI, bez tworzenia odrębnej funkcji Pełnomocnika do spraw SZBI.
2. Do zadań Sekretarza Gminy należy w szczególności:
 - 1) koordynowanie opracowywania, uzgadniania i aktualizacji dokumentacji SZBI;
 - 2) koordynowanie identyfikacji procesów, informacji i aktywów oraz przeprowadzania analiz ryzyka;
 - 3) koordynowanie realizacji szkoleń, audytów, przeglądów i działań doskonalących;
 - 4) monitorowanie realizacji zaleceń wynikających z analiz ryzyka, audytów, kontroli, przeglądów i incydentów;

- 5) zapewnienie przepływu informacji między Wójtem, kierownikami komórek organizacyjnych, osobami odpowiedzialnymi za obsługę informatyczną oraz Inspektorem Ochrony Danych;
 - 6) przedstawianie Wójtowi informacji o stanie funkcjonowania SZBI, zidentyfikowanych ryzykach, istotnych niezgodnościach i potrzebach w zakresie zasobów;
 - 7) koordynowanie przygotowania, nie rzadziej niż raz w roku, raportu z funkcjonowania SZBI.
3. Sekretarz Gminy nie przejmuje odpowiedzialności kierowników komórek organizacyjnych, osób odpowiedzialnych za obsługę informatyczną ani innych osób za zadania przypisane im w niniejszym zarządzeniu i dokumentacji SZBI.

§ 6

1. Osoby odpowiedzialne za obsługę informatyczną Urzędu realizują zadania techniczne i operacyjne w zakresie bezpieczeństwa systemów teleinformatycznych, odpowiednio do zakresu powierzonych obowiązków lub zawartych umów.
2. Do zadań tych osób należy w szczególności:
 - 1) prowadzenie lub zapewnienie aktualności inwentaryzacji sprzętu, oprogramowania, systemów, usług, kont i konfiguracji;
 - 2) wdrażanie, utrzymywanie i monitorowanie zabezpieczeń technicznych wynikających z przepisów, dokumentacji SZBI i analizy ryzyka;
 - 3) zarządzanie kontami, uprawnieniami administracyjnymi, mechanizmami uwierzytelniania oraz procesem nadawania, zmiany i odbierania dostępów;
 - 4) zapewnienie aktualizacji oprogramowania, ochrony przed złośliwym oprogramowaniem i ograniczania ryzyka wynikającego z podatności technicznych;
 - 5) wykonywanie, zabezpieczanie i testowanie kopii zapasowych oraz udział w testach odtwarzania działania;
 - 6) zapewnienie prowadzenia i ochrony dzienników systemowych w zakresie wymaganym przepisami prawa, dokumentacją SZBI i analizą ryzyka;
 - 7) udział w obsłudze incydentów, zabezpieczaniu dowodów i przywracaniu prawidłowego działania systemów;
 - 8) współpraca z dostawcami usług informatycznych oraz weryfikowanie realizacji wymagań bezpieczeństwa określonych w umowach;
 - 9) udział w analizach ryzyka, audytach, kontrolach i przeglądach SZBI oraz przekazywanie wymaganych informacji i dowodów.
3. W przypadku powierzenia obsługi informatycznej podmiotowi zewnętrznemu zakres obowiązków i odpowiedzialności tego podmiotu określa umowa, z uwzględnieniem wymagań SZBI oraz zasad ochrony informacji i danych osobowych.

§ 7

1. Kierownicy komórek organizacyjnych oraz osoby zatrudnione na samodzielnych stanowiskach odpowiadają za przestrzeganie wymagań SZBI w zakresie powierzonych im zadań i procesów.
2. Do ich obowiązków należy w szczególności:
 - 1) identyfikowanie informacji, procesów, aktywów i wymagań prawnych właściwych dla podległego obszaru;
 - 2) udział w analizach ryzyka, audytach, kontrolach i przeglądach SZBI;
 - 3) zapewnienie, aby dostęp do informacji i zasobów posiadały wyłącznie osoby uprawnione w zakresie niezbędnym do realizacji zadań;
 - 4) niezwłoczne zgłaszanie potrzeb nadania, zmiany, zawieszenia lub odebrania uprawnień;
 - 5) niezwłoczne zgłaszanie incydentów, podatności, niezgodności i zagrożeń;
 - 6) zapewnienie pracownikom możliwości udziału w wymaganych szkoleniach;
 - 7) wdrażanie zatwierdzonych działań ograniczających ryzyko i działań korygujących;
 - 8) nadzorowanie przestrzegania polityk, procedur i instrukcji bezpieczeństwa;
 - 9) współpraca z Sekretarzem Gminy, osobami odpowiedzialnymi za obsługę informatyczną oraz Inspektorem Ochrony Danych, odpowiednio do zakresu ich zadań.

§ 8

1. Inspektor Ochrony Danych wykonuje zadania określone w art. 39 rozporządzenia 2016/679, zachowując niezależność przewidzianą w art. 38 tego rozporządzenia.
2. Inspektor Ochrony Danych uczestniczy w funkcjonowaniu SZBI w zakresie dotyczącym ochrony danych osobowych, w szczególności przez:
 - 1) udzielanie zaleceń i konsultacji dotyczących zgodności przetwarzania danych osobowych i adekwatności środków ochrony;
 - 2) udział w ocenie skutków dla ochrony danych oraz analizach ryzyka dla praw i wolności osób fizycznych;
 - 3) współpracę przy analizie naruszeń ochrony danych osobowych i realizacji obowiązków wynikających z przepisów o ochronie danych;
 - 4) monitorowanie przestrzegania przepisów o ochronie danych osobowych oraz regulacji wewnętrznych dotyczących tej ochrony.
3. Udział Inspektora Ochrony Danych w funkcjonowaniu SZBI nie obejmuje podejmowania decyzji dotyczących celów i sposobów przetwarzania danych osobowych ani zarządzania środkami bezpieczeństwa, których zgodność Inspektor następnie ocenia.

§ 9

1. Każda osoba posiadająca dostęp do informacji lub zasobów Urzędu jest zobowiązana do:
 - 1) zapoznania się z dokumentacją SZBI właściwą dla wykonywanych zadań;
 - 2) przestrzegania zasad bezpieczeństwa informacji;
 - 3) ochrony powierzonych informacji, dokumentów, urządzeń, kont i danych uwierzytelniających;

- 4) wykorzystywania informacji i zasobów Urzędu wyłącznie w zakresie niezbędnym do realizacji powierzonych zadań;
 - 5) niezwłocznego zgłaszania incydentów, podejrzeń incydentów, utraty dokumentów lub urządzeń, błędnego ujawnienia informacji oraz innych zdarzeń mogących naruszyć bezpieczeństwo informacji;
 - 6) uczestnictwa w wymaganych szkoleniach;
 - 7) współpracy podczas audytów, kontroli, analiz ryzyka i postępowań wyjaśniających.
2. Zapoznanie się z wymaganiami SZBI może zostać potwierdzone w postaci papierowej albo elektronicznej.
 3. Naruszenie zasad SZBI może skutkować odpowiedzialnością porządkową, pracowniczą, cywilną, administracyjną lub karną, na zasadach określonych w odrębnych przepisach.

§ 10

1. Analizę ryzyka dla bezpieczeństwa informacji przeprowadza się:
 - 1) nie rzadziej niż raz w roku;
 - 2) przed wdrożeniem nowych albo istotnie zmienianych systemów, usług lub procesów;
 - 3) po wystąpieniu poważnego incydentu;
 - 4) w przypadku istotnych zmian organizacyjnych, prawnych, technicznych lub środowiskowych.
2. Wyniki analizy ryzyka podlegają udokumentowaniu. Ryzyka przekraczające poziom zaakceptowany przez Wójta Gminy Ciechanów wymagają opracowania i realizacji planu postępowania z ryzykiem.
3. Audyt wewnętrzny w zakresie bezpieczeństwa informacji przeprowadza się nie rzadziej niż raz w roku, z zapewnieniem odpowiednich kompetencji, bezstronności, obiektywizmu i niezależności od audytowanego obszaru.
4. Wyniki audytów przedstawia się Wójtowi Gminy Ciechanów oraz osobom odpowiedzialnym za realizację działań korygujących

§ 11

1. Wójt Gminy Ciechanów dokonuje przeglądu SZBI nie rzadziej niż raz w roku.
2. Przegląd obejmuje w szczególności:
 - 1) wyniki audytów i kontroli;
 - 2) stan realizacji działań wynikających z poprzednich przeglądów;
 - 3) wyniki analiz ryzyka;
 - 4) informacje o incydentach i naruszeniach bezpieczeństwa;
 - 5) stan realizacji działań korygujących i doskonalących;
 - 6) zmiany prawne, organizacyjne i technologiczne;
 - 7) stan realizacji szkoleń;
 - 8) potrzeby dotyczące personelu, środków finansowych, infrastruktury i narzędzi;
 - 9) propozycje zmian i usprawnień SZBI.

3. Z przeglądu sporządza się protokół albo raport zawierający podjęte decyzje, określone działania, osoby odpowiedzialne i terminy ich wykonania.

§ 12

1. Dostęp do dokumentacji SZBI przysługuje osobom uprawnionym w zakresie niezbędnym do wykonywania powierzonych zadań.
2. Dokumenty zawierające szczegółowe informacje o architekturze systemów, konfiguracji zabezpieczeń, podatnościach, sposobach uwierzytelniania, kopiach zapasowych, planach ciągłości działania lub innych zabezpieczeniach podlegają szczególnej ochronie.
3. Udostępnienie dokumentacji SZBI osobom lub podmiotom zewnętrznym wymaga uprzedniej oceny zakresu informacji podlegających ochronie oraz zgody osoby uprawnionej, z uwzględnieniem przepisów o dostępie do informacji publicznej i tajemnicach prawnie chronionych.
4. Postanowienia ust. 1–3 nie stanowią samoistnej podstawy odmowy udostępnienia informacji publicznej.

§ 13

1. Wykonanie zarządzenia powierza się Sekretarzowi Gminy, kierownikom komórek organizacyjnych, pracownikom zatrudnionym na samodzielnych stanowiskach, osobom odpowiedzialnym za obsługę informatyczną oraz wszystkim pracownikom i innym osobom wykonującym zadania na rzecz Urzędu, odpowiednio do zakresu powierzonych obowiązków.
2. Dokumenty, procedury i instrukcje dotyczące bezpieczeństwa informacji obowiązujące przed wejściem w życie niniejszego zarządzenia zachowują moc w zakresie, w jakim nie są z nim sprzeczne, do czasu ich aktualizacji albo uchylecia.
3. Zobowiązuje się pracowników Urzędu oraz inne osoby wykonujące zadania na jego rzecz do zapoznania się z niniejszym zarządzeniem oraz dokumentacją SZBI właściwą dla realizowanych przez nich zadań.
4. Nadzór nad wykonaniem zarządzenia sprawuje Wójt Gminy Ciechanów.
5. Zarządzenie wchodzi w życie z dniem podpisania.

WÓJT GMINY

Stefan Pawłowski

