

ZARZĄDZENIE NR 149/2026
PREZYDENTA MIASTA CIECHANÓW
z dnia 11 września 2026 r.

**w sprawie ustanowienia Systemu Zarządzania Bezpieczeństwem
Informacji w Urzędzie Miasta Ciechanów, wyznaczenia
Pełnomocnika ds. SZBI oraz powołania Zespołu ds.
Cyberbezpieczeństwa**

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, z późn. zm.), w związku z art. 8, art. 8c–8f, art. 14, art. 15 i art. 16d ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2026 r. poz. 20 i 252) oraz § 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. z 2024 r. poz. 773), zarządza się, co następuje:

Paragraf 1

1. W Urzędzie Miasta Ciechanów, zwanym dalej „Urzędem”, ustanawia się i wdraża System Zarządzania Bezpieczeństwem Informacji, zwany dalej „SZBI”.
2. SZBI stanowi zorganizowany system zarządzania obejmujący działania organizacyjne, osobowe, techniczne i fizyczne służące zapewnieniu bezpieczeństwa informacji oraz cyberbezpieczeństwa w Urzędzie.
3. SZBI obejmuje 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, dostawców usług lub inne osoby działające na rzecz Urzędu.
4. SZBI obejmuje w szczególności:
 - 1) wszystkie komórki organizacyjne i samodzielne stanowiska pracy Urzędu;
 - 2) pracowników oraz inne osoby wykonujące zadania na rzecz Urzędu;
 - 3) procesy i zadania realizowane przez Urząd;
 - 4) systemy informacyjne i teleinformatyczne, sieci, urządzenia, oprogramowanie, usługi informatyczne i usługi ICT;
 - 5) dokumentację papierową i elektroniczną;
 - 6) aktywa informacyjne i techniczne;
 - 7) pomieszczenia, obiekty i strefy, w których przetwarzane lub przechowywane są informacje;
 - 8) usługi świadczone przez dostawców zewnętrznych, jeżeli mogą wpływać na bezpieczeństwo informacji lub cyberbezpieczeństwo Urzędu.

Paragraf 2

1. Celem SZBI jest zapewnienie adekwatnego do występującego ryzyka poziomu ochrony informacji oraz systemów służących do ich przetwarzania.
2. SZBI zapewnia w szczególności ochronę poufności, integralności, dostępności, autentyczności, rozliczalności, niezaprzeczalności, niezawodności informacji i systemów.
3. SZBI służy w szczególności:
 - 1) identyfikowaniu informacji, procesów, usług i aktywów;
 - 2) systematycznemu identyfikowaniu zagrożeń i podatności;
 - 3) przeprowadzaniu szacowania ryzyka i zarządzaniu ryzykiem;
 - 4) stosowaniu odpowiednich i proporcjonalnych do ryzyka środków organizacyjnych, technicznych, fizycznych i osobowych;
 - 5) zapewnieniu bezpieczeństwa systemów informacyjnych w całym cyklu ich życia;
 - 6) zapewnieniu ciągłości działania, odtwarzania działalności i odporności Urzędu na zdarzenia zakłócające;
 - 7) zarządzaniu incydentami bezpieczeństwa informacji i incydentami cyberbezpieczeństwa;
 - 8) zapewnieniu bezpieczeństwa łańcucha dostaw;
 - 9) zapewnieniu właściwego zarządzania tożsamością, dostępem i uprawnieniami;
 - 10) zarządzaniu aktywami;
 - 11) zapewnieniu odpowiedniego poziomu bezpieczeństwa komunikacji elektronicznej;
 - 12) podnoszeniu świadomości pracowników oraz kształtowaniu zasad cyberhigieny;
 - 13) monitorowaniu skuteczności stosowanych zabezpieczeń;
 - 14) zapewnieniu zgodności z wymaganiami prawa, regulacjami wewnętrznymi oraz wymaganiami wynikającymi z zawartych umów;
 - 15) ciągłemu monitorowaniu, przeglądaniu, utrzymywaniu i doskonaleniu SZBI.

Paragraf 3

1. Odpowiedzialność za wykonywanie przez Urząd Miasta Ciechanów obowiązków kierownika podmiotu w zakresie cyberbezpieczeństwa ponosi Prezydent Miasta Ciechanów, zgodnie z przepisami ustawy o krajowym systemie cyberbezpieczeństwa.
2. Prezydent Miasta w szczególności:
 - 1) podejmuje decyzje dotyczące przygotowania, wdrażania, stosowania, przeglądu i nadzoru SZBI;
 - 2) zapewnia organizację i nadzór nad realizacją obowiązków w zakresie cyberbezpieczeństwa;
 - 3) planuje, w ramach obowiązujących procedur budżetowych, adekwatne środki finansowe na realizację obowiązków dotyczących bezpieczeństwa informacji i cyberbezpieczeństwa;
 - 4) przydziela zadania i odpowiedzialności w zakresie cyberbezpieczeństwa oraz nadzoruje ich wykonywanie;
 - 5) zapewnia warunki umożliwiające pracownikom realizację obowiązków wynikających z SZBI;
 - 6) zapewnia podnoszenie świadomości personelu w zakresie bezpieczeństwa informacji i cyberbezpieczeństwa;
 - 7) podejmuje decyzje dotyczące akceptacji ryzyka, w szczególności w odniesieniu do ryzyka przekraczającego ustalony poziom akceptacji;
 - 8) zatwierdza wyniki przeglądów zarządczych SZBI oraz kluczowe działania doskonalące.
3. Powierzenie określonych zadań lub obowiązków Pełnomocnikowi ds. SZBI, Zespołowi ds. Cyberbezpieczeństwa, kierownikom komórek organizacyjnych lub innym osobom nie wyłącza odpowiedzialności Prezydenta Miasta wynikającej z przepisów prawa.

Paragraf 4

1. Wyznam Panią Adrianę Saganek – Sekretarza Miasta Ciechanów – na Pełnomocnika ds. Systemu Zarządzania Bezpieczeństwem Informacji, zwanego dalej „Pełnomocnikiem ds. SZBI”.
2. Pełnomocnik ds. SZBI podlega bezpośrednio Prezydentowi Miasta Ciechanów w zakresie wykonywania zadań określonych niniejszym zarządzeniem.
3. Pełnomocnikowi ds. SZBI powierza się bieżącą koordynację wykonywania w Urzędzie obowiązków kierownika podmiotu w zakresie cyberbezpieczeństwa, w zakresie określonym niniejszym zarządzeniem i odrębnymi regulacjami.
4. Pełnomocnik ds. SZBI jest osobą, której powierzono obowiązki kierownika w zakresie cyberbezpieczeństwa w rozumieniu art. 8e ust. 1 ustawy o krajowym systemie cyberbezpieczeństwa.
5. Pełnomocnik ds. SZBI jest uprawniony do:
 - 1) żądania od pracowników, kierowników komórek organizacyjnych oraz osób wykonujących zadania na rzecz Urzędu informacji, dokumentów i wyjaśnień niezbędnych do realizacji powierzonych zadań;
 - 2) uzyskiwania dostępu do dokumentacji, rejestrów i informacji dotyczących bezpieczeństwa informacji i cyberbezpieczeństwa w zakresie niezbędnym do wykonywania powierzonych zadań;
 - 3) przedstawiania Prezydentowi Miasta wniosków dotyczących zabezpieczeń, zasobów, zmian organizacyjnych, działań korygujących i doskonalących;
 - 4) wydawania, w granicach udzielonych kompetencji, zaleceń dotyczących stosowania obowiązujących regulacji SZBI;
 - 5) zwoływania posiedzeń Zespołu ds. Cyberbezpieczeństwa.

Paragraf 5

1. Do zadań Pełnomocnika ds. SZBI należy w szczególności:
 - 1) koordynowanie ustanawiania, wdrażania, stosowania, monitorowania, przeglądania, utrzymywania i doskonalenia SZBI;
 - 2) przygotowywanie projektów polityk, procedur, instrukcji, standardów, planów i innych regulacji dotyczących SZBI oraz inicjowanie ich aktualizacji;
 - 3) prowadzenie i nadzorowanie wykazu obowiązującej dokumentacji SZBI;
 - 4) koordynowanie identyfikacji i klasyfikacji informacji, procesów, usług i aktywów;
 - 5) koordynowanie procesu zarządzania ryzykiem dla bezpieczeństwa informacji i cyberbezpieczeństwa;
 - 6) monitorowanie realizacji planów postępowania z ryzykiem;
 - 7) monitorowanie zgodności funkcjonowania Urzędu z wymaganiami SZBI oraz właściwymi przepisami prawa;
 - 8) przygotowywanie propozycji zabezpieczeń organizacyjnych, osobowych, technicznych i fizycznych;
 - 9) koordynowanie działań dotyczących cyberzagrożeń, podatności i incydentów;
 - 10) nadzorowanie prowadzenia rejestru incydentów bezpieczeństwa informacji i cyberbezpieczeństwa;
 - 11) koordynowanie realizacji obowiązków dotyczących zgłaszania incydentów właściwym podmiotom krajowego systemu cyberbezpieczeństwa;
 - 12) przygotowywanie rocznych planów szkoleń oraz działań podnoszących świadomość;
 - 13) organizowanie lub koordynowanie szkoleń wstępnych, okresowych i doraźnych;
 - 14) przygotowywanie projektu rocznego planu audytów wewnętrznych SZBI;
 - 15) monitorowanie realizacji zaleceń wynikających z audytów, kontroli, analiz ryzyka, przeglądów i incydentów;

- 16) koordynowanie przeglądów SZBI;
 - 17) współpraca z osobami odpowiedzialnymi za administrowanie systemami teleinformatycznymi;
 - 18) współpraca z Inspektorem Ochrony Danych w sprawach, w których zdarzenia dotyczące bezpieczeństwa informacji mogą jednocześnie stanowić naruszenie ochrony danych osobowych;
 - 19) współpraca z osobami odpowiedzialnymi za ochronę informacji niejawnych, zarządzanie kryzysowe, kontrolę zarządczą, bezpieczeństwo fizyczne, ciągłość działania oraz inne obszary mające wpływ na bezpieczeństwo informacji;
 - 20) opiniowanie projektów umów, zamówień, zmian organizacyjnych, wdrożeń i przedsięwzięć informatycznych, jeżeli mogą one istotnie wpływać na bezpieczeństwo informacji lub cyberbezpieczeństwo;
 - 21) przedstawianie Prezydentowi Miasta informacji o stanie SZBI, istotnych ryzykach, incydentach, niezgodnościach oraz potrzebach dotyczących zasobów;
 - 22) przygotowywanie co najmniej raz w roku raportu z funkcjonowania SZBI;
 - 23) niezwłoczne informowanie Prezydenta Miasta o poważnych incydentach, istotnych niezgodnościach oraz ryzykach przekraczających przyjęty poziom akceptacji;
 - 24) koordynowanie przygotowania Urzędu do audytów, kontroli i czynności nadzorczych dotyczących bezpieczeństwa informacji oraz cyberbezpieczeństwa;
 - 25) wykonywanie innych zadań powierzonych przez Prezydenta Miasta, związanych z bezpieczeństwem informacji lub cyberbezpieczeństwem.
2. Pełnomocnik ds. SZBI nie podejmuje samodzielnie decyzji zastrzeżonych przepisami prawa lub regulacjami wewnętrznymi do kompetencji Prezydenta Miasta.
 3. Pełnomocnik ds. SZBI nie przeprowadza audytu obszarów, za których ustanowienie lub bieżące funkcjonowanie bezpośrednio odpowiada, jeżeli nie można zapewnić wymaganej niezależności i obiektywizmu audytu.

Paragraf 6

1. Powołuje się Zespół ds. Cyberbezpieczeństwa, zwany dalej „Zespołem”, jako wewnętrzną strukturę odpowiedzialną za realizację i koordynację zadań z zakresu cyberbezpieczeństwa w Urzędzie.
2. W skład Zespołu wchodzi:
 - 1) Pełnomocnik ds. SZBI – jako Przewodniczący Zespołu;
 - 2) Administrator Systemów Informatycznych lub osoba odpowiedzialna za administrowanie systemami teleinformatycznymi Urzędu;
 - 3) pracownik lub pracownicy realizujący zadania z zakresu informatyki i cyberbezpieczeństwa;
 - 4) Kierownik Referatu ds. Bezpieczeństwa i Zarządzania Kryzysowego – w zakresie właściwości;
 - 5) inne osoby wyznaczone przez Prezydenta Miasta, odpowiednio do potrzeb i charakteru rozpatrywanych zagadnień.
3. W pracach Zespołu, z głosem doradczym, może uczestniczyć Inspektor Ochrony Danych, Pełnomocnik do spraw Ochrony Informacji Niejawnych oraz inne osoby posiadające wiedzę lub kompetencje niezbędne do rozpatrzenia określonej sprawy.
4. Udział Inspektora Ochrony Danych w pracach Zespołu nie powoduje przejęcia przez niego odpowiedzialności za operacyjne zarządzanie SZBI ani za wdrażanie środków technicznych i organizacyjnych.
5. Do zadań Zespołu należy w szczególności:
 - 1) analiza bieżącego stanu cyberbezpieczeństwa;
 - 2) wymiana informacji o zagrożeniach, podatnościach i incydentach;
 - 3) analiza incydentów oraz koordynowanie działań naprawczych;

- 4) udział w szacowaniu ryzyka;
 - 5) opiniowanie proponowanych środków bezpieczeństwa;
 - 6) udział w planowaniu i testowaniu ciągłości działania oraz odtwarzania po awarii;
 - 7) analiza wyników monitorowania systemów i zabezpieczeń;
 - 8) udział w przygotowaniu i realizacji działań korygujących i doskonalących;
 - 9) udział w przygotowaniu do audytów i kontroli;
 - 10) wspieranie Pełnomocnika ds. SZBI w realizacji zadań wynikających z przepisów prawa.
6. Posiedzenia Zespołu zwołuje Przewodniczący odpowiednio do potrzeb, w szczególności w przypadku poważnego incydentu, istotnej zmiany ryzyka albo konieczności podjęcia pilnych działań w zakresie cyberbezpieczeństwa.

Paragraf 7

1. Administrator Systemów Informatycznych oraz osoby odpowiedzialne za obsługę informatyczną Urzędu odpowiadają, w zakresie powierzonych obowiązków, za operacyjne wdrażanie i utrzymywanie technicznych środków bezpieczeństwa.
2. Do ich zadań należy w szczególności:
 - 1) zapewnienie bezpiecznej konfiguracji systemów, urządzeń i usług;
 - 2) zarządzanie kontami, tożsamością oraz uprawnieniami użytkowników;
 - 3) zapewnienie szczególnej ochrony kont uprzywilejowanych;
 - 4) wdrażanie i utrzymywanie mechanizmów uwierzytelniania, w tym uwierzytelniania wieloskładnikowego, w przypadkach wynikających z analizy ryzyka;
 - 5) zarządzanie aktualizacjami i poprawkami bezpieczeństwa;
 - 6) identyfikowanie, analizowanie i usuwanie podatności technicznych;
 - 7) wykonywanie, zabezpieczanie i testowanie kopii zapasowych;
 - 8) przeprowadzanie testów odtworzeniowych;
 - 9) monitorowanie systemów teleinformatycznych, sieci oraz zdarzeń bezpieczeństwa;
 - 10) zapewnianie właściwego rejestrowania i ochrony dzienników systemowych;
 - 11) wdrażanie i utrzymywanie zabezpieczeń sieciowych, systemowych i aplikacyjnych;
 - 12) stosowanie środków kryptograficznych i szyfrowania zgodnie z wymaganiami SZBI i wynikami analizy ryzyka;
 - 13) udział w obsłudze incydentów;
 - 14) zabezpieczanie materiału dowodowego związanego z incydentami;
 - 15) udział w analizach ryzyka, testach bezpieczeństwa, audytach i kontrolach;
 - 16) prowadzenie i aktualizowanie wymaganej dokumentacji technicznej;
 - 17) utrzymywanie aktualnych informacji o sprzęcie, oprogramowaniu, konfiguracji i usługach informatycznych;
 - 18) współpraca z dostawcami usług i systemów w zakresie bezpieczeństwa;
 - 19) zgłaszanie Pełnomocnikowi ds. SZBI istotnych podatności, zagrożeń, niezgodności i potrzeb dotyczących bezpieczeństwa;
 - 20) dokumentowanie wykonywania czynności mających znaczenie dla bezpieczeństwa informacji i cyberbezpieczeństwa.
3. Zmiany techniczne mogące istotnie wpływać na poziom bezpieczeństwa informacji powinny być odpowiednio analizowane, testowane i dokumentowane przed ich wdrożeniem, z uwzględnieniem wyników analizy ryzyka.

Paragraf 8

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, usług i aktywów wykorzystywanych w podległym obszarze;
- 2) udział w analizach ryzyka i przeglądach SZBI;
- 3) zapewnianie przestrzegania zasady minimalnych niezbędnych uprawnień;
- 4) zgłaszanie potrzeb nadania, zmiany, przeglądu lub odebrania uprawnień;
- 5) niezwłoczne zgłaszanie incydentów, podatności, niezgodności i zagrożeń;
- 6) zapewnienie pracownikom możliwości uczestnictwa w obowiązkowych szkoleniach;
- 7) realizowanie zatwierdzonych działań wynikających z analizy ryzyka;
- 8) nadzorowanie przestrzegania przez pracowników obowiązujących polityk, procedur i instrukcji;
- 9) współpraca z Pełnomocnikiem ds. SZBI, Zespołem ds. Cyberbezpieczeństwa, osobami odpowiedzialnymi za obsługę informatyczną oraz Inspektorem Ochrony Danych w zakresie ich właściwości.

Paragraf 9

1. Każda osoba posiadająca dostęp do informacji lub zasobów Urzędu jest obowiązana do:
 - 1) zapoznania się z regulacjami SZBI właściwymi dla wykonywanych zadań;
 - 2) przestrzegania zasad bezpieczeństwa informacji i cyberbezpieczeństwa;
 - 3) ochrony powierzonych informacji, dokumentów, urządzeń, kont i danych uwierzytelniających;
 - 4) wykorzystywania informacji i zasobów Urzędu wyłącznie w zakresie niezbędnym do wykonywania powierzonych zadań;
 - 5) stosowania zasad cyberhigieny;
 - 6) niezwłocznego zgłaszania incydentów, podejrzeń incydentów, podatności, utraty dokumentów lub urządzeń, błędnego ujawnienia informacji oraz innych zdarzeń mogących wpływać na bezpieczeństwo informacji;
 - 7) udziału w wymaganych szkoleniach;
 - 8) współpracy podczas analiz ryzyka, audytów, kontroli, przeglądów i postępowań wyjaśniających.
2. Zapoznanie się z regulacjami SZBI może być dokumentowane w postaci papierowej lub elektronicznej.
3. Naruszenie zasad SZBI może skutkować odpowiedzialnością określoną w przepisach prawa oraz regulacjach wewnętrznych Urzędu.

Paragraf 10

1. Analizę ryzyka dla bezpieczeństwa informacji i cyberbezpieczeństwa przeprowadza się systematycznie, a w szczególności:
 - 1) nie rzadziej niż raz w roku;
 - 2) przed wdrożeniem nowego albo istotnie zmienianego systemu, usługi, procesu lub technologii;
 - 3) w przypadku istotnej zmiany organizacyjnej;
 - 4) po wystąpieniu poważnego incydentu;
 - 5) w przypadku zidentyfikowania istotnych nowych zagrożeń lub podatności;
 - 6) w przypadku istotnej zmiany wymagań prawnych, organizacyjnych lub technologicznych.
2. Wyniki analizy ryzyka podlegają udokumentowaniu.
3. Dla ryzyk przekraczających ustalony poziom akceptacji opracowuje się plan postępowania z ryzykiem.
4. Decyzje dotyczące akceptacji ryzyka podejmuje osoba posiadająca odpowiednie kompetencje decyzyjne, zgodnie z obowiązującą metodyką zarządzania ryzykiem, przy

czym ryzyka istotne dla funkcjonowania Urzędu lub wykonywania obowiązków podmiotu kluczowego przedstawia się Prezydentowi Miasta.

Paragraf 11

1. W ramach SZBI zapewnia się okresowy audyt wewnętrzny w zakresie bezpieczeństwa informacji wymagany przepisami dotyczącymi Krajowych Ram Interoperacyjności, przeprowadzany nie rzadziej niż raz w roku.
2. Audyt, o którym mowa w ust. 1, przeprowadza się z zapewnieniem odpowiednich kompetencji, bezstronności i obiektywizmu osób wykonujących audyt.
3. Niezależnie od audytu, o którym mowa w ust. 1, zapewnia się przeprowadzanie audytu bezpieczeństwa systemu informacyjnego wymaganego wobec podmiotu kluczowego na podstawie art. 15 ustawy o krajowym systemie cyberbezpieczeństwa, co najmniej raz na trzy lata, z zachowaniem terminów, wymagań i zasad określonych w tej ustawie.
4. Pierwszy audyt, o którym mowa w ust. 3, przeprowadza się w terminie wynikającym z przepisów ustawy o krajowym systemie cyberbezpieczeństwa.
5. Audyt, o którym mowa w ust. 3, nie może być przeprowadzony przez osobę realizującą w audytowanym podmiocie zadania, o których mowa w art. 8 oraz art. 9–13 ustawy o krajowym systemie cyberbezpieczeństwa, ani przez osobę, która realizowała te zadania w okresie roku poprzedzającego rozpoczęcie audytu.
6. Raport z audytu, o którym mowa w ust. 3, podlega przekazaniu właściwemu organowi w terminie i na zasadach określonych w ustawie o krajowym systemie cyberbezpieczeństwa.
7. Audyt wewnętrzny, o którym mowa w ust. 1, oraz audyt wymagany ustawą o krajowym systemie cyberbezpieczeństwa mogą być organizowane w sposób skoordynowany, jeżeli zostaną spełnione wymagania dotyczące zakresu, kompetencji, niezależności, dokumentowania oraz sposobu przeprowadzenia właściwe dla każdego z tych audytów.
8. Wyniki audytów przedstawia się Prezydentowi Miasta oraz osobom odpowiedzialnym za realizację wynikających z nich działań.
9. Pełnomocnik ds. SZBI monitoruje realizację zaleceń i działań korygujących wynikających z audytów.

Paragraf 12

1. Prezydent Miasta dokonuje przeglądu funkcjonowania 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, cyberzagrożeniach i podatnościach;
 - 5) stan realizacji działań korygujących i doskonalących;
 - 6) ocenę skuteczności stosowanych środków bezpieczeństwa;
 - 7) zmiany prawne, organizacyjne i technologiczne;
 - 8) wyniki testów bezpieczeństwa i ciągłości działania;
 - 9) realizację planu szkoleń;
 - 10) ocenę zasobów kadrowych, organizacyjnych, technicznych i finansowych;
 - 11) informacje dotyczące dostawców oraz bezpieczeństwa łańcucha dostaw;
 - 12) propozycje zmian i usprawnień SZBI.
3. Z przeglądu sporządza się protokół albo raport określający w szczególności podjęte decyzje, działania do realizacji, osoby odpowiedzialne oraz terminy wykonania.

Paragraf 13

1. Prezydent Miasta oraz Pełnomocnik ds. SZBI, jako osoba, której powierzono obowiązki kierownika w zakresie cyberbezpieczeństwa, uczestniczą raz w roku kalendarzowym w szkoleniu wymaganym na podstawie art. 8e ustawy o krajowym systemie cyberbezpieczeństwa.
2. Udział w szkoleniu, o którym mowa w ust. 1, podlega udokumentowaniu.
3. Pracownicy Urzędu uczestniczą w szkoleniach z zakresu bezpieczeństwa informacji i cyberbezpieczeństwa odpowiednio do wykonywanych zadań oraz posiadanych uprawnień.
4. Zapewnia się w szczególności:
 - 1) szkolenia dla nowo zatrudnionych osób przed dopuszczeniem ich do samodzielnego korzystania z zasobów informacyjnych w zakresie określonym w regulacjach wewnętrznych;
 - 2) okresowe szkolenia pracowników;
 - 3) szkolenia specjalistyczne dla osób wykonujących zadania administracyjne lub techniczne;
 - 4) szkolenia doraźne wynikające z incydentów, zmian przepisów prawa, zmian technologicznych albo zidentyfikowanych ryzyk.

Paragraf 14

1. Osoby realizujące w Urzędzie zadania, o których mowa w art. 8 lub art. 11 ustawy o krajowym systemie cyberbezpieczeństwa, w szczególności Pełnomocnik ds. SZBI oraz osoby odpowiedzialne za realizację zadań technicznych i obsługę incydentów, mogą zostać dopuszczone do ich wykonywania po spełnieniu wymagań określonych w art. 8f tej ustawy.
2. Przed rozpoczęciem wykonywania zadań, o których mowa w ust. 1, osoba przedstawia informację z Krajowego Rejestru Karnego stwierdzającą niekaralność za przestępstwa przeciwko ochronie informacji, chyba że zgodnie z ustawą wymaganie to uważa się za spełnione z uwagi na posiadanie właściwego poświadczenia bezpieczeństwa.
3. Spełnienie wymagań, o których mowa w ust. 1 i 2, podlega udokumentowaniu.
4. W przypadku powzięcia uzasadnionego podejrzenia, że osoba wykonująca zadania, o których mowa w ust. 1, została skazana za przestępstwo przeciwko ochronie informacji, stosuje się zasady określone w art. 8f ustawy o krajowym systemie cyberbezpieczeństwa.

Paragraf 15

1. Każdy incydent, podejrzenie incydentu, cyberzagrożenie lub istotna podatność podlega niezwłocznemu zgłoszeniu zgodnie z obowiązującą w Urzędzie procedurą.
2. Pełnomocnik ds. SZBI, przy współpracy Zespołu ds. Cyberbezpieczeństwa oraz osób odpowiedzialnych za obsługę informatyczną, koordynuje:
 - 1) ocenę zgłoszonego zdarzenia;
 - 2) klasyfikację incydentu;
 - 3) ustalenie zakresu i skutków incydentu;
 - 4) działania ograniczające skutki incydentu;
 - 5) działania naprawcze i odtworzeniowe;
 - 6) zabezpieczenie materiału dowodowego;
 - 7) realizację obowiązków informacyjnych i zgłoszeniowych wynikających z ustawy o krajowym systemie cyberbezpieczeństwa;
 - 8) analizę przyczyn źródłowych incydentu;
 - 9) wdrożenie działań korygujących i zapobiegawczych.

3. Jeżeli incydent może jednocześnie stanowić naruszenie ochrony danych osobowych, o zdarzeniu niezwłocznie informuje się Inspektora Ochrony Danych.
4. Realizacja obowiązków dotyczących incydentów cyberbezpieczeństwa nie zastępuje obowiązków wynikających z przepisów dotyczących ochrony danych osobowych, informacji niejawnych, tajemnic prawnie chronionych ani innych przepisów szczególnych.

Paragraf 16

1. Dokumentację SZBI stanowią w szczególności:
 - 1) Polityka Bezpieczeństwa Informacji;
 - 2) polityki, procedury, instrukcje, standardy, zasady i wytyczne dotyczące bezpieczeństwa informacji i cyberbezpieczeństwa;
 - 3) metodyka zarządzania ryzykiem;
 - 4) dokumentacja analiz ryzyka i planów postępowania z ryzykiem;
 - 5) rejestry aktywów, systemów, sprzętu, oprogramowania i usług;
 - 6) dokumentacja zarządzania dostępem i uprawnieniami;
 - 7) dokumentacja dotycząca incydentów, podatności i cyberzagrożeń;
 - 8) dokumentacja ciągłości działania i odtwarzania po awarii;
 - 9) dokumentacja kopii zapasowych i testów odtworzeniowych;
 - 10) dokumentacja dotycząca dostawców;
 - 11) dokumentacja szkoleń;
 - 12) plany i raporty z audytów;
 - 13) dokumentacja przeglądów SZBI;
 - 14) rejestry niezgodności oraz działań korygujących i doskonalących;
 - 15) protokoły, raporty, wyniki testów, zapisy systemowe oraz inne dowody funkcjonowania SZBI.
2. Szczegółowa dokumentacja SZBI jest opracowywana i zatwierdzana odrębnie od niniejszego zarządzenia.
3. Dokumenty SZBI zatwierdza Prezydent Miasta.
4. Pełnomocnik ds. SZBI prowadzi aktualny wykaz obowiązującej dokumentacji SZBI, obejmujący co najmniej nazwę dokumentu, wersję, datę zatwierdzenia, właściciela dokumentu oraz termin jego kolejnego przeglądu.
5. Dokumentacja SZBI podlega przeglądowi nie rzadziej niż raz w roku oraz każdorazowo, jeżeli jest to uzasadnione w szczególności:
 - 1) zmianą przepisów prawa;
 - 2) zmianą organizacyjną;
 - 3) wdrożeniem albo istotną zmianą systemu lub usługi;
 - 4) poważnym incydem;
 - 5) wynikami audytu lub kontroli;
 - 6) wynikami analizy ryzyka;
 - 7) zidentyfikowaniem nowych istotnych zagrożeń lub podatności.

Paragraf 17

1. Dostęp do dokumentacji SZBI przysługuje wyłącznie osobom uprawnionym, w zakresie wynikającym z powierzonych im zadań.
2. Szczegółnej ochronie podlegają dokumenty i informacje zawierające w szczególności dane dotyczące:
 - 1) architektury systemów i sieci teleinformatycznych;
 - 2) konfiguracji zabezpieczeń;
 - 3) podatności i słabości zabezpieczeń;
 - 4) mechanizmów uwierzytelniania;
 - 5) kont uprzywilejowanych i zarządzania dostępem;

- 6) szczegółowej konfiguracji urządzeń i systemów;
 - 7) sposobu wykonywania i przechowywania kopii zapasowych;
 - 8) planów ciągłości działania i odtwarzania po awarii;
 - 9) sposobów monitorowania i wykrywania incydentów;
 - 10) wyników testów bezpieczeństwa;
 - 11) scenariuszy reagowania na incydenty;
 - 12) innych informacji, których ujawnienie mogłoby zwiększyć ryzyko naruszenia bezpieczeństwa Urzędu.
3. Dokumentacja SZBI wraz z załącznikami oraz dokumentacja wykonawcza i operacyjna związana z jej stosowaniem stanowią dokumentację przeznaczoną do użytku wewnętrznego w Urzędzie Miasta Ciechanów.
 4. Z uwagi na charakter dokumentacji, w szczególności możliwość zawarcia w niej informacji dotyczących organizacji bezpieczeństwa informacji i ochrony danych osobowych, stosowanych środków, technicznych i organizacyjnych, zasad zarządzania dostępem, sposobów reagowania na incydenty, wyników analiz ryzyka, konfiguracji zabezpieczeń oraz innych informacji, których ujawnienie mogłoby wpływać na poziom bezpieczeństwa przetwarzanych informacji, dokumentacji tej nie publikuje się w Biuletynie Informacji Publicznej ani na innych publicznie dostępnych stronach internetowych Urzędu.
 5. Udostępnienie dokumentacji SZBI podmiotowi zewnętrznemu w związku z audytem, kontrolą, realizacją umowy lub świadczeniem usług następuje wyłącznie w zakresie niezbędnym do realizacji określonego celu i z zastosowaniem odpowiednich środków ochrony.

Paragraf 18

1. Kierownictwo Urzędu zapewnia, odpowiednio do zidentyfikowanego ryzyka i obowiązujących wymagań prawnych, zasoby organizacyjne, kadrowe, techniczne i finansowe niezbędne do funkcjonowania i doskonalenia SZBI.
2. Pełnomocnik ds. SZBI przedstawia Prezydentowi Miasta potrzeby dotyczące zasobów, w szczególności, jeżeli wynikają one z analizy ryzyka, audytu lub kontroli, incydentu, przeglądu SZBI, zmiany przepisów prawa, zmian technologicznych, konieczności utrzymania odpowiedniego poziomu cyberbezpieczeństwa.

Paragraf 19

1. Dokumenty, procedury, instrukcje oraz inne regulacje dotyczące bezpieczeństwa informacji obowiązujące w Urzędzie przed wejściem w życie niniejszego zarządzenia zachowują moc w zakresie, w jakim nie są sprzeczne z niniejszym zarządzeniem oraz obowiązującymi przepisami prawa, do czasu ich aktualizacji, zastąpienia albo uchylenia.
2. Pełnomocnik ds. SZBI dokonuje przeglądu dokumentacji, o której mowa w ust. 1, i przedstawia Prezydentowi Miasta propozycje jej aktualizacji, zastąpienia albo uchylenia.
3. Zobowiązuje się kierowników komórek organizacyjnych, pracowników oraz inne osoby wykonujące zadania na rzecz Urzędu do współpracy z Pełnomocnikiem ds. SZBI i Zespołem ds. Cyberbezpieczeństwa w zakresie niezbędnym do wdrożenia i utrzymania SZBI.

Paragraf 20

4. Wykonanie zarządzenia powierza się:
 - 1) Pełnomocnikowi ds. SZBI;
 - 2) Zespołowi ds. Cyberbezpieczeństwa;
 - 3) kierownikom komórek organizacyjnych;
 - 4) osobom zatrudnionym na samodzielnych stanowiskach;

- 5) Administratorowi Systemów Informatycznych oraz innym osobom odpowiedzialnym za obsługę informatyczną;
 - 6) wszystkim pracownikom oraz innym osobom wykonującym zadania na rzecz Urzędu – odpowiednio do zakresu powierzonych zadań.
5. Nadzór nad wykonaniem zarządzenia sprawuje Prezydent Miasta Ciechanów.

Paragraf 21

Zarządzenie wchodzi w życie z dniem podpisania.

Prezydent Miasta Ciechanów
Krzysztof Kosiński