

ZARZĄDZENIE NR 0050.77.2026

Burmistrza Miasta i Gminy Suchedniów

z dnia 28.08.2026 r.

w sprawie wyznaczenia Administratora Systemu Informatycznego oraz określenia zakresu jego zadań w Urzędzie Miasta i Gminy w Suchedniowie

z 2026 r. poz. 662 i 912), art. 8 ust. 3 oraz art. 8d pkt 3 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2026 r. poz. 20 i 252,815 i 1003), § 19 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), w związku z zarządzeniem nr 0050.57.2026 Burmistrza Miasta i Gminy Suchedniów z dnia 23 czerwca 2026 r. w sprawie wprowadzenia Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta i Gminy w Suchedniowie, zarządzam, co następuje:

§ 1.

1. Wyznaczam Pana Łukasza Osucha do pełnienia funkcji Administratora Systemu Informatycznego Urzędu Miasta i Gminy w Suchedniowie, zwanego dalej „ASI”.
2. ASI wykonuje zadania techniczne, operacyjne i organizacyjne związane z administrowaniem systemami informatycznymi, bezpieczeństwem informacji oraz cyberbezpieczeństwem Urzędu, w granicach udzielonych upoważnień.

§ 2.

1. Szczegółowy zakres obowiązków ASI określa załącznik do niniejszego zarządzenia.
2. Zakres obowiązków, o którym mowa w ust. 1, stanowi uzupełnienie dotychczasowego zakresu czynności Pana Łukasza Osucha na stanowisku Informatyka.
3. ASI potwierdza zapoznanie się z powierzonym zakresem obowiązków i przyjęcie go do wykonywania przez złożenie podpisu na załączniku.

§ 3.

1. ASI współpracuje z Burmistrzem, Sekretarzem Miasta i Gminy Suchedniów, Inspektorem Ochrony Danych, kierownikami komórek organizacyjnych, osobami wyznaczonymi do realizacji zadań cyberbezpieczeństwa oraz uprawnionymi dostawcami usług informatycznych.
2. Wyznaczenie ASI nie narusza niezależności ani ustawowych zadań Inspektora Ochrony Danych i nie powoduje przeniesienia na ASI odpowiedzialności przypisanej przepisami prawa Burmistrzowi jako kierownikowi jednostki.

3. W razie nieobecności ASI zadania wymagające uprawnień administratora systemów może wykonywać wyłącznie inny pracownik posiadający odpowiednie kompetencje albo uprawniony podmiot zewnętrzny, wyznaczony lub upoważniony przez Burmistrza.

§ 4.

Traci moc zarządzenie nr 0050.55.2015 Burmistrza Miasta i Gminy Suchedniów z dnia 30 czerwca 2015 r. w sprawie powołania Administratora Bezpieczeństwa Informacji i Administratora Systemu Informatycznego w Urzędzie Miasta i Gminy w Suchedniowie.

§ 5.

1. Wykonanie zarządzenia w zakresie realizacji powierzonych obowiązków powierza się Administratorowi Systemu Informatycznego.
2. Koordynowanie i bieżące monitorowanie wykonywania zadań przez ASI oraz ich zgodności z obowiązującym Systemem Zarządzania Bezpieczeństwem Informacji powierza się Sekretarzowi Miasta i Gminy Suchedniów.
3. Powierzenie czynności, o których mowa w ust. 2, nie narusza obowiązków, nadzoru i odpowiedzialności Burmistrza jako kierownika podmiotu ważnego, wynikających z art. 8c i art. 8d ustawy o krajowym systemie cyberbezpieczeństwa.

§ 6.

Zarządzenie wchodzi w życie z dniem podpisania.

Burmistrz Miasta i Gminy Suchedniów

//Dariusz Miernik

**ZAKRES OBOWIĄZKÓW ADMINISTRATORA SYSTEMU INFORMATYCZNEGO
(ASI)
W URZĘDZIE MIASTA I GMINY W SUCHEDNIOWIE**

Osoba wyznaczona: Pan Łukasz Osuch, Informatyk w Wydziale Organizacyjnym.

I. Organizacja pracy ASI i System Zarządzania Bezpieczeństwem Informacji

1. Administrowanie systemami informatycznymi, urządzeniami, sieciami i usługami teleinformatycznymi Urzędu w zakresie wynikającym z przyznanych uprawnień.
2. Uczestniczenie w opracowywaniu, wdrażaniu, utrzymywaniu, monitorowaniu, przeglądzie i doskonaleniu Systemu Zarządzania Bezpieczeństwem Informacji (SZBI).
3. Przygotowywanie i aktualizowanie, w części technicznej, polityk, procedur, instrukcji, ewidencji i innych dokumentów dotyczących systemów informacyjnych, dostępu, kopii zapasowych, incydentów oraz ciągłości działania.
4. Prowadzenie i aktualizowanie ewidencji infrastruktury teleinformatycznej, w szczególności systemów, serwerów, stacji roboczych, urządzeń sieciowych, urządzeń przenośnych, oprogramowania, licencji, usług, dostawców i istotnych zasobów informacyjnych.
5. Identyfikowanie zagrożeń i podatności oraz przedstawianie Sekretarzowi i Burmistrzowi informacji potrzebnych do analizy ryzyka, doboru zabezpieczeń i zaplanowania działań naprawczych.
6. Prowadzenie dokumentacji konfiguracji i istotnych zmian w infrastrukturze, z uwzględnieniem zależności między systemami i możliwości ich odtworzenia.
7. Niezwłoczne zgłaszanie przełożonemu stwierdzonych niezgodności, braków zabezpieczeń, przestarzałych rozwiązań oraz potrzeb organizacyjnych i finansowych dotyczących bezpieczeństwa IT.
8. Wykonywanie obowiązków zgodnie z przyjętą w Urzędzie dokumentacją SZBI, poleceniami Burmistrza i udzielonymi upoważnieniami.

II. Zarządzanie dostępem, kontami i uprawnieniami

1. Tworzenie, modyfikowanie, blokowanie i usuwanie kont użytkowników wyłącznie na podstawie zatwierdzonych wniosków, poleceń albo upoważnień wydanych przez osoby uprawnione.

2. Nadawanie dostępu do systemów i informacji zgodnie z zakresem obowiązków pracownika, zasadą minimalnych uprawnień oraz zasadą wiedzy koniecznej.
3. Sprawdzanie czy dostęp do danych osobowych odpowiada aktualnemu upoważnieniu do ich przetwarzania; współpraca z Inspektorem Ochrony Danych przy wyjaśnianiu stwierdzonych rozbieżności.
4. Niezwłoczne odbieranie lub zmienianie uprawnień po ustaniu zatrudnienia, zmianie stanowiska, zmianie zakresu obowiązków, zakończeniu współpracy albo ustaniu podstawy dostępu, na podstawie otrzymanej informacji.
5. Prowadzenie lub współprowadzenie ewidencji kont, uprawnień, kont uprzywilejowanych i dostępu podmiotów zewnętrznych oraz okresowe przeglądanie aktualności tych dostępu.
6. Zapewnianie odrębności kont administracyjnych od zwykłych kont użytkowników, stosowanie uwierzytelniania wieloskładnikowego tam, gdzie jest dostępne oraz ochronę zdalnego dostępu.
7. Bezpieczne nadawanie danych inicjalnych i resetowanie danych uwierzytelniających; niedopuszczanie do pozyskiwania, przechowywania lub ujawniania indywidualnych haseł użytkowników poza zakresem niezbędnym i dozwolonym przez przyjętą procedurę.
8. Stosowanie zasad uwierzytelniania, długości haseł, ich zmiany i ochrony zgodnych z obowiązującą polityką Urzędu; zgłaszanie potrzeby aktualizacji tych zasad, jeżeli odbiegają od aktualnych zaleceń bezpieczeństwa.
9. Zawieszanie lub ograniczanie dostępu w sytuacjach określonych w przepisach, polityce Urzędu albo po stwierdzeniu zagrożenia; dokumentowanie takich czynności.
10. Zabezpieczanie danych dostępowych do kont uprzywilejowanych oraz zapewnianie możliwości awaryjnego dostępu osobie upoważnionej przez Burmistrza.

III. Zabezpieczenia techniczne, aktualizacje i monitorowanie

1. Konfigurowanie, utrzymywanie i monitorowanie technicznych zabezpieczeń sieci, serwerów, stacji roboczych, urządzeń mobilnych, poczty elektronicznej oraz usług wykorzystywanych przez Urząd.
2. Zapewnianie działania i aktualności zabezpieczeń antywirusowych, zapór sieciowych, mechanizmów filtrowania, segmentacji sieci i innych wdrożonych środków ochronnych.
3. Monitorowanie komunikatów producentów, właściwych CSIRT, CERT Polska i dostawców dotyczących nowych podatności, zagrożeń oraz dostępnych aktualizacji.
4. Planowanie, testowanie i instalowanie aktualizacji bezpieczeństwa systemów operacyjnych, aplikacji, urządzeń sieciowych i pozostałych komponentów IT, z uwzględnieniem ich krytyczności oraz ciągłości pracy Urzędu.

5. Identyfikowanie produktów niewspieranych przez producentów, oprogramowania wycofanego z użycia oraz konfiguracji stwarzających ryzyko; przedstawianie propozycji ich wymiany lub zabezpieczenia.
6. Konfigurowanie rejestrowania zdarzeń, zabezpieczenie logów przed nieuprawnioną zmianą lub usunięciem oraz analizowanie zdarzeń istotnych dla bezpieczeństwa.
7. Zapewnienie ochrony transmisji danych i nośników informacji, w tym stosowanie szyfrowania w przypadkach wymaganych analizą ryzyka, przepisami lub dokumentacją SZBI.
8. Nadzorowanie zabezpieczeń technicznych serwerowni i urządzeń IT, w szczególności systemów kontroli dostępu, warunków środowiskowych, zasilania awaryjnego oraz mechanizmów alarmowania o awariach.
9. Monitorowanie legalności używanego oprogramowania, ważności licencji i zgodności instalowanych aplikacji z zatwierdzonymi zasadami Urzędu.
10. Bezpieczne przygotowywanie sprzętu do serwisu, przekazania, wycofania z użytkowania lub utylizacji, w tym trwałe usuwanie danych albo zapewnianie zniszczenia nośników zgodnie z właściwą procedurą.

IV. Kopie zapasowe, odtwarzanie i ciągłość działania

1. Planowanie i wykonywanie kopii zapasowych systemów, konfiguracji i danych zgodnie z ich istotnością, zatwierdzoną polityką oraz wymaganym czasem odtworzenia.
2. Bieżąca obsługa systemu NetAlert PRO albo innego wdrożonego systemu o analogicznym przeznaczeniu – jeżeli takie rozwiązanie jest wykorzystywane w Urzędzie.
3. Zapewnianie odpowiedniej ochrony, szyfrowania i ograniczenia dostępu do kopii zapasowych, a także logicznego lub fizycznego oddzielenia kopii od środowiska produkcyjnego.
4. Okresowe wykonywanie prób odtworzenia danych i systemów z kopii zapasowych oraz dokumentowanie wyników testów i stwierdzonych problemów.
5. Prowadzenie lub aktualizowanie dokumentacji dotyczącej harmonogramów kopii, miejsc ich przechowywania, okresów retencji i procedur odtworzeniowych.
6. Uczestniczenie w przygotowywaniu i testowaniu planów ciągłości działania oraz planów odtwarzania systemów po awarii lub incydencie.
7. Podejmowanie działań technicznych służących przywróceniu dostępności systemów i danych po awarii albo incydencie oraz informowanie kierownictwa o przewidywanym czasie i skutkach przerwy.

V. Techniczna obsługa zdarzeń i incydentów cyberbezpieczeństwa

1. Monitorowanie zdarzeń w systemach informatycznych, dokonywanie ich wstępnej analizy i dokumentowanie podejrzeń incydentów cyberbezpieczeństwa.
2. Niezwłoczne informowanie Burmistrza, Sekretarza oraz właściwej osoby odpowiedzialnej za kontakty z podmiotami krajowego systemu cyberbezpieczeństwa o incydencie, poważnym zagrożeniu lub istotnej podatności.
3. Podejmowanie działań technicznych ograniczających skutki zdarzenia, w szczególności izolowanie zagrożonych zasobów, blokowanie nieuprawnionego dostępu i zabezpieczanie środowiska informatycznego.
4. Zabezpieczanie logów, danych, konfiguracji i innych informacji niezbędnych do ustalenia przyczyny, przebiegu oraz skutków incydentu.
5. Przygotowywanie informacji technicznych potrzebnych do terminowego zgłoszenia incydentu poważnego właściwemu CSIRT sektorowemu; zgłoszenia w imieniu Urzędu dokonuje wyłącznie osoba upoważniona przez Burmistrza.
6. Niezwłoczne informowanie Inspektora Ochrony Danych, jeżeli zdarzenie może stanowić naruszenie ochrony danych osobowych oraz przekazywanie informacji potrzebnych do oceny obowiązków wynikających z RODO.
7. Współpraca techniczna z osobami kontaktowymi, właściwym CSIRT i dostawcami usług, w zakresie udzielonych upoważnień, przy ograniczaniu skutków incydentu i przywracaniu bezpiecznego działania systemów.
8. Prowadzenie dokumentacji działań technicznych, udział w analizie przyczyn zdarzenia i przygotowywanie propozycji zabezpieczeń ograniczających ryzyko jego powtórzenia.

VI. Systemy monitorowania zagrożeń, w tym NetAlert PRO

1. Współpraca przy instalacji, konfiguracji i utrzymaniu systemów wykrywania oraz monitorowania cyberzagrożeń stosowanych w sieci Urzędu.
2. Bieżąca obsługa NetAlert PRO, jeżeli rozwiązanie to jest wykorzystywane w Urzędzie albo innego wdrożonego systemu o analogicznym przeznaczeniu.
3. Odbieranie i analizowanie alertów dotyczących w szczególności prób rozpoznania zasobów, nietypowych połączeń, nieuprawnionego dostępu, przejęcia kont i aktywności odbiegającej od przyjętego profilu pracy systemów.
4. Podejmowanie albo inicjowanie działań technicznych odpowiednich do poziomu zagrożenia oraz eskalowanie istotnych alertów zgodnie z procedurą incydentową.
5. Dokumentowanie istotnych alertów, wyników analizy i podjętych działań oraz przedstawianie właściwych informacji przełożonemu.

6. Monitorowania wyłącznie w celach bezpieczeństwa, w zakresie niezbędnym, zgodnym z przepisami i wewnętrznymi zasadami ochrony danych.

VII. Dostawcy, wdrożenia, szkolenia oraz audyty

1. Uwzględnianie wymagań bezpieczeństwa przy planowaniu zakupu, wdrażaniu i zmianie systemów, urządzeń, oprogramowania, usług chmurowych oraz innych rozwiązań teleinformatycznych.
2. Przygotowywanie wymagań technicznych oraz rekomendacji dotyczących bezpieczeństwa dostawców i usług; decyzje zakupowe, organizacyjne i finansowe pozostają po stronie osób uprawnionych.
3. Przyznawanie dostawcom i serwisantom dostępu wyłącznie na podstawie udzielonego upoważnienia, w minimalnym niezbędnym zakresie i na wymagany czas oraz zapewnianie odebrania dostępu po zakończeniu prac.
4. Współpraca przy weryfikowaniu wymagań bezpieczeństwa w umowach dotyczących obsługi IT, serwisu, dostępu zdalnego, chmury i przetwarzania danych.
5. Uczestniczenie w audytach, kontrolach, testach i przeglądach przez przygotowywanie dokumentacji technicznej, udzielanie wyjaśnień oraz realizację zatwierdzonych zaleceń w obszarze IT.
6. Nieprzeprowadzanie samodzielnej oceny albo audytu, którego niezależność byłaby naruszona przez ocenianie własnych czynności administracyjnych.
7. Współpraca przy organizowaniu szkoleń i działań informacyjnych dotyczących bezpiecznego korzystania z systemów, rozpoznawania phishingu, ochrony kont oraz zgłaszania zagrożeń i incydentów.
8. Przekazywanie Burmistrzowi i Sekretarzowi informacji o potrzebie aktualizacji dokumentacji, zabezpieczeń, szkoleń, licencji, sprzętu i planów ciągłości działania.

VIII. Współpraca, poufność i granice odpowiedzialności

1. Współpraca z Burmistrzem, Sekretarzem Miasta i Gminy Suchedniów, Naczelnikiem Wydziału Organizacyjnego, Inspektorem Ochrony Danych, pracownikami Urzędu oraz uprawnionymi podmiotami zewnętrznymi.
2. Wykonywanie czynności związanych z ochroną danych osobowych w porozumieniu z Inspektorem Ochrony Danych w zakresie konsultacyjnym; ASI nie przejmuje jego ustawowych zadań kontrolnych ani doradczych.
3. Przedstawienie Burmistrzowi spraw wymagających decyzji kierownika jednostki, w tym decyzji o akceptacji ryzyka, finansowaniu, wyborze dostawcy i zatwierdzaniu dokumentacji, Burmistrzowi lub osobie przez niego umocowanej.

4. Zachowanie w poufności informacji o konfiguracji infrastruktury, zastosowanych zabezpieczeniach, podatnościach, incydentach, danych uwierzytelniających i innych informacjach mogących wpłynąć na bezpieczeństwo Urzędu.
5. Wykonywanie czynności wyłącznie w granicach posiadanych uprawnień, właściwego upoważnienia do przetwarzania danych oraz poleceń zgodnych z prawem.
6. Dokumentowanie wykonanych zadań w zakresie wynikającym z obowiązujących procedur oraz przedstawianie informacji i raportów Burmistrzowi lub Sekretarzowi.
7. Powierzenie zadań ASI nie powoduje przeniesienia na pracownika odpowiedzialności przypisanej kierownikowi podmiotu przez ustawę o krajowym systemie cyberbezpieczeństwa.
8. Niniejszy zakres obowiązków uzupełnia dotychczasowy zakres czynności Pana Łukasza Osucha na stanowisku Informatyka.