Stanowisko Rady do Spraw Cyfryzacji w sprawie cyberbezpieczeństwa jednostek samorządu terytorialnego.

Jednostki samorządu terytorialnego (JST), obejmujące gminy, powiaty i województwa samorządowe, wykonują – zgodnie z ustawą o samorządzie gminnym[1], ustawą o samorządzie powiatowym[2] oraz ustawą o samorządzie województwa[3] – zróżnicowane zadania publiczne o charakterze lokalnym i regionalnym. Zakres ich kompetencji różni się w zależności od szczebla samorządu. Gminy realizują przede wszystkim zadania związane z zaspokajaniem zbiorowych potrzeb wspólnoty samorządowej, obejmujące m.in. ewidencję ludności, gospodarkę komunalną, zaopatrzenie w wodę, gospodarkę odpadami, edukację, pomoc społeczną, lokalny transport zbiorowy czy zarządzanie kryzysowe. Powiaty odpowiadają m.in. za szkolnictwo ponadpodstawowe, ochronę zdrowia na poziomie powiatowym, drogi powiatowe oraz zadania z zakresu administracji zespolonej, natomiast województwa samorządowe realizują zadania o charakterze regionalnym, w szczególności w zakresie rozwoju regionalnego, transportu wojewódzkiego i koordynacji polityk rozwoju.

Ze względu na zakres realizowanych zadań oraz postępującą cyfryzację usług publicznych JST stanowią istotny element krajowego systemu cyberbezpieczeństwa. Zgodnie z ustawą o krajowym systemie cyberbezpieczeństwa (KSC)[4], zasadniczą rolę w zapewnieniu cyberbezpieczeństwa pełnią podmioty krajowego systemu cyberbezpieczeństwa, w szczególności organy właściwe do spraw cyberbezpieczeństwa, CSIRT poziomu krajowego, podmioty kluczowe i ważne oraz dostawcy usług cyfrowych. Jednostki samorządu terytorialnego uczestniczą w tym systemie przede wszystkim jako podmioty publiczne realizujące zadania publiczne z wykorzystaniem systemów teleinformatycznych oraz – w określonych przypadkach – jako podmioty objęte obowiązkami wynikającymi z ustawy o KSC.

Jednocześnie należy zauważyć, że niezależnie od wielkości jednostki samorządu terytorialnego wszystkie urzędy przetwarzają dane osobowe mieszkańców oraz świadczą usługi publiczne z wykorzystaniem systemów teleinformatycznych. Oznacza to, że skuteczność działań w zakresie cyberbezpieczeństwa wpływa bezpośrednio na ciągłość funkcjonowania administracji lokalnej, ochronę informacji oraz poziom zaufania obywateli do instytucji publicznych.

Cyberbezpieczeństwo JST nie może być postrzegane wyłącznie jako element informatyzacji lub odpowiedzialność komórek IT. Stanowi ono jeden z warunków zapewnienia ciągłości realizacji zadań publicznych przez administrację samorządową. Obejmuje zarówno środki techniczne, jak i organizacyjne, w tym zarządzanie ryzykiem, zarządzanie ciągłością działania,

[1] Ustawa z dnia 8 marca 1990 r. o samorządzie gminnym (Dz.U. 2026, poz. 662)
[2] Ustawa z dnia 5 czerwca 1998 r. o samorządzie powiatowym (Dz.U. 2025, poz. 1684)
[3] Ustawa z dnia 5 czerwca 1998 r. o samorządzie województwa (Dz.U. 2026, poz. 720)
[4] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. 2026, poz. 20)

ochronę informacji, rozwój kompetencji pracowników, szkolenia, procedury reagowania na incydenty oraz zdolność do odtworzenia usług po awarii lub cyberataku.

Dane wskazują na systemowy charakter zagrożeń cyberbezpieczeństwa. W 2025 r. CERT Polska odnotował 658 320 zgłoszeń (wzrost o 10% względem 2024 r.) oraz zarejestrował 260 783 unikalnych incydentów bezpieczeństwa (wzrost o 152% względem 2024 r.). Rosnąca liczba incydentów dotyczy również administracji samorządowej, która pozostaje atrakcyjnym celem cyberprzestępców ze względu na zakres przetwarzanych danych oraz znaczenie świadczonych usług publicznych.

Kontrola Najwyższej Izby Kontroli z 2025 r. wykazała, że większość skontrolowanych jednostek samorządu terytorialnego nie podejmowała skutecznych i rzetelnych działań na rzecz zapewnienia bezpieczeństwa informacji. Negatywnie oceniono przygotowanie do zapewnienia ciągłości działania systemów informatycznych w 71% skontrolowanych urzędów, a istotne nieprawidłowości stwierdzono w 23 z 24 jednostek. Najczęściej występowały: brak polityk ciągłości działania, brak planów ciągłości działania i planów odtworzeniowych, nieprawidłowości w zakresie wykonywania kopii zapasowych, niewystarczające zabezpieczenia serwerowni, brak szkoleń dla pracowników oraz nieprzestrzeganie wymagań dotyczących stosowania haseł.

Szczególnie narażone na cyberataki pozostają strony internetowe urzędów, systemy komunikacji elektronicznej oraz systemy teleinformatyczne wykorzystywane do świadczenia usług publicznych i przetwarzania danych. Badania CSIRT NASK wykazały podatności bezpieczeństwa w ponad połowie analizowanych serwisów internetowych jednostek samorządu terytorialnego. Serwisy samorządowe stanowią atrakcyjny cel zarówno dla cyberprzestępców, jak i podmiotów prowadzących działania hybrydowe, ponieważ ich kompromitacja może prowadzić do dezinformacji, utraty wiarygodności instytucji publicznych oraz ograniczenia zaufania obywateli. Ponadto skuteczne przejęcie kontroli nad publicznie dostępnymi usługami sieciowymi może stanowić punkt wyjścia do dalszej eskalacji uprawnień i penetracji infrastruktury teleinformatycznej urzędu.

Rada wskazuje, iż największym wyzwaniem dla jednostek samorządu terytorialnego w kontekście wdrożenia znowelizowanej ustawy o krajowym systemie cyberbezpieczeństwa jest zbudowanie trwałego systemu zarządzania cyberbezpieczeństwem zgodnego z wymaganiami ustawy. O ile zadania techniczne, takie jak monitorowanie bezpieczeństwa, testy penetracyjne czy usługi SOC, mogą zostać powierzone wyspecjalizowanym podmiotom zewnętrznym, o tyle odpowiedzialność za zarządzanie ryzykiem, organizację procesów bezpieczeństwa, zapewnienie ciągłości działania oraz nadzór nad dostawcami pozostaje po stronie kierownika jednostki.

Dodatkowym wyzwaniem jest znaczne zróżnicowanie potencjału organizacyjnego JST. Znowelizowana ustawa o KSC, implementująca dyrektywę NIS2, uwzględnia zasadę proporcjonalności, różnicując zakres obowiązków m.in. w zależności od wielkości urzędu, jednak nawet najmniejsze gminy są zobowiązane do wdrożenia podstawowych

mechanizmów zarządzania cyberbezpieczeństwem. W praktyce oznacza to konieczność rozwijania kompetencji zarządczych, budowania świadomości kadry kierowniczej oraz wdrożenia procesów organizacyjnych, które dotychczas w wielu jednostkach funkcjonowały w ograniczonym zakresie lub nie były sformalizowane. To właśnie osiągnięcie odpowiedniej dojrzałości organizacyjnej, a nie pozyskanie zaawansowanych technologii, będzie decydować o skuteczności wdrożenia nowych przepisów.

Rada wskazuje, że najczęściej powtarzające się słabości JST obejmują:

- brak mechanizmów skutecznego finansowania cyberbezpieczeństwa w JST;
- braki kadrowe;
- brak świadomości procesowej;
- brak zarządzania ryzykiem i umiejętności jego oceny;
- brak testów odtworzeniowych;
- brak planów ciągłości działania;
- brak zarządzania systemami dostępnymi z sieci Internet;
- ujawnianie informacji technicznych w odpowiedziach na wnioski o informację publiczną i zamówieniach publicznych;
- rozproszenie zakupów, licencji, narzędzi i usług bezpieczeństwa;
- brak systemu podnoszenia kompetencji oraz wymiany doświadczeń między zespołami IT w JST.

Rekomendacje Rady

1. Wypracowanie trwałego mechanizmu finansowania cyberbezpieczeństwa JST

Rada rekomenduje stworzenie trwałego i przewidywalnego mechanizmu finansowania obowiązków wynikających ze znowelizowanej ustawy o krajowym systemie cyberbezpieczeństwa. Dotychczasowe wsparcie, oparte głównie na programach i konkursach grantowych, umożliwia realizację jednorazowych inwestycji, jednak nie zapewnia finansowania kosztów bieżącego utrzymania systemu cyberbezpieczeństwa, które mają charakter ciągły.

Szczególnym wyzwaniem jest fakt, że cyberbezpieczeństwo jednostek samorządu terytorialnego nie stanowi odrębnego zadania własnego ani zadania zleconego z zakresu administracji rządowej, lecz jest elementem zapewnienia prawidłowego funkcjonowania urzędu oraz realizacji wszystkich zadań publicznych. W konsekwencji wydatki na cyberbezpieczeństwo są finansowane przede wszystkim z dochodów własnych JST jako koszty funkcjonowania administracji samorządowej. Jednocześnie obowiązki wynikające ze znowelizowanej ustawy o KSC mają charakter ustawowy i służą realizacji celów o znaczeniu ogólnopaństwowym, związanych z zapewnieniem bezpieczeństwa krajowego systemu cyberbezpieczeństwa.

W związku z tym zasadne jest wprowadzenie stabilnego mechanizmu współfinansowania tych obowiązków ze środków budżetu państwa, uwzględniającego zróżnicowanie potencjału organizacyjnego i finansowego jednostek samorządu terytorialnego. Mechanizm ten powinien zapewniać finansowanie nie tylko inwestycji, ale przede wszystkim kosztów operacyjnych, obejmujących m.in. zarządzanie cyberbezpieczeństwem, usługi monitorowania bezpieczeństwa (SOC), audyty, testy bezpieczeństwa, zarządzanie podatnościami, utrzymanie kopii zapasowych, szkolenia pracowników, usługi chmurowe, wsparcie poincydentowe oraz rozwój kompetencji organizacyjnych.

Szczególnego wsparcia wymagają małe jednostki samorządu terytorialnego, których potencjał kadrowy i finansowy jest niewystarczający do samodzielnego spełnienia wymagań wynikających z ustawy o KSC. Brak stabilnego finansowania może prowadzić do sytuacji, w której jednostki będą w stanie sfinansować zakup infrastruktury technicznej, jednak nie będą posiadały środków na jej bezpieczne utrzymanie, aktualizację oraz zapewnienie odpowiednich kompetencji organizacyjnych, co w dłuższej perspektywie obniży poziom cyberodporności administracji samorządowej.

2. Budowa wielopoziomowego modelu wsparcia jednostek samorządu terytorialnego poprzez współpracę instytucjonalną, centra usług wspólnych i mechanizmy wymiany informacji

Rada rekomenduje rozwój wielopoziomowego modelu wsparcia jednostek samorządu terytorialnego w realizacji obowiązków wynikających ze znowelizowanej ustawy o krajowym systemie cyberbezpieczeństwa. Model ten powinien opierać się na wykorzystaniu istniejących instrumentów współpracy przewidzianych w ustawach ustrojowych samorządu terytorialnego, w szczególności możliwości zawierania porozumień między jednostkami samorządu terytorialnego, tworzenia związków JST, stowarzyszeń oraz organizowania wspólnej obsługi jednostek organizacyjnych w formule centrów usług wspólnych.

W związku z tym rekomenduje się rozwój trójpoziomowego modelu wsparcia:

1. Centra usług wspólnych w obszarze cyberbezpieczeństwa (CUW-CYBER)

Model oparty na powołaniu centrów usług wspólnych pozwala na wspólną obsługę organizacyjną i ekspercką wielu jednostek, przy zachowaniu odpowiedzialności kierowników poszczególnych JST za bezpieczeństwo realizowanych zadań publicznych.

CUW-CYBER mogłyby świadczyć na rzecz gmin, powiatów oraz ich jednostek organizacyjnych m.in.:

- wsparcie w przygotowaniu i aktualizacji dokumentacji bezpieczeństwa,
- prowadzenie analiz ryzyka,
- wsparcie w realizacji wymagań ustawy o KSC,
- koordynację procesów zarządzania incydentami,
- organizację szkoleń i podnoszenie świadomości pracowników,

- wsparcie w nadzorze nad dostawcami usług IT,
- koordynację korzystania z usług technicznych, takich jak SOC, monitoring bezpieczeństwa czy audyty.

Takie rozwiązanie odpowiada rzeczywistym potrzebom JST, ponieważ wzmacnia przede wszystkim kompetencje zarządcze i organizacyjne, które są obecnie największą słabością wielu jednostek.

2. *Wojewódzkie centra kompetencyjne cyberbezpieczeństwa*

Na poziomie regionalnym zasadne jest rozwijanie struktur pełniących funkcję centrów kompetencyjnych wspierających JST. Ich rolą powinno być zapewnienie wiedzy eksperckiej, koordynacja działań między jednostkami oraz pomoc w sytuacjach wymagających specjalistycznych kompetencji.

Struktury wojewódzkie mogłyby wspierać JST w szczególności w:

- przygotowaniu do realizacji obowiązków wynikających z KSC,
- ocenie poziomu dojrzałości cyberbezpieczeństwa,
- organizacji ćwiczeń i testów ciągłości działania,
- koordynacji współpracy z podmiotami krajowego systemu cyberbezpieczeństwa,
- organizacji wspólnych zakupów lub usług specjalistycznych.

3. *Mechanizmy wymiany informacji i współpracy środowiskowej*

Wymiana informacji o zagrożeniach, podatnościach i incydentach powinna odbywać się przede wszystkim w ramach mechanizmów przewidzianych ustawą o krajowym systemie cyberbezpieczeństwa, w szczególności zgodnie z art. 46 ustawy o KSC, który określa zasady współpracy i wymiany informacji pomiędzy uczestnikami systemu.

Jednocześnie zasadne jest rozwijanie dobrowolnych form współpracy środowiskowej JST, takich jak ISAC-JST, jako platformy wymiany doświadczeń, dobrych praktyk, rekomendacji oraz wzorcowych rozwiązań organizacyjnych. ISAC-JST nie powinien zastępować ustawowych mechanizmów raportowania i współpracy w ramach KSC, lecz uzupełniać je poprzez budowanie społeczności praktyków oraz zwiększanie odporności całego sektora samorządowego.

Tak zbudowany model pozwoli ograniczyć skutki dużego zróżnicowania potencjału JST, szczególnie pomiędzy dużymi miastami a małymi gminami. Wykorzystanie centrów usług wspólnych i współpracy między jednostkami umożliwi osiągnięcie efektu skali, obniżenie kosztów oraz zapewnienie dostępu do kompetencji, których najmniejsze jednostki nie są w stanie utrzymać samodzielnie.

3. Wzmocnienie kompetencji zarządczych i organizacyjnych w zakresie cyberbezpieczeństwa

Rada rekomenduje opracowanie systemu szkoleń mających na celu rozwój kompetencji jednostek samorządu terytorialnego w zakresie zarządzania cyberbezpieczeństwem, ze szczególnym uwzględnieniem kompetencji kadry kierowniczej, osób odpowiedzialnych za bezpieczeństwo informacji oraz pracowników realizujących zadania związane z organizacją procesów bezpieczeństwa.

Największym wyzwaniem JST nie jest obecnie brak dostępu do specjalistycznych narzędzi technicznych ani niedobór administratorów systemów informatycznych, lecz ograniczona dojrzałość organizacyjna w zakresie zarządzania cyberbezpieczeństwem. Wymogi wynikające ze znowelizowanej ustawy o krajowym systemie cyberbezpieczeństwa oraz dyrektywy NIS2 wymagają przede wszystkim zdolności do identyfikacji ryzyka, zarządzania procesami bezpieczeństwa, zapewnienia ciągłości działania, nadzoru nad dostawcami oraz podejmowania decyzji przez kierownictwo jednostki.

Dlatego działania wzmacniające kadry JST powinny koncentrować się przede wszystkim na:

- rozwoju kompetencji osób odpowiedzialnych za zarządzanie cyberbezpieczeństwem (funkcje CISO, koordynatorów bezpieczeństwa informacji, pełnomocników ds. bezpieczeństwa);
- szkoleniu kadry kierowniczej JST w zakresie odpowiedzialności za cyberbezpieczeństwo, zarządzania ryzykiem i nadzoru nad realizacją obowiązków wynikających z KSC;
- budowaniu kompetencji w zakresie przygotowania polityk bezpieczeństwa, analiz ryzyka, planów ciągłości działania i procedur reagowania na incydenty;
- rozwijaniu umiejętności zarządzania relacjami z dostawcami usług IT i cyberbezpieczeństwa.

Rada rekomenduje stworzenie mechanizmów umożliwiających współdzielenie kompetencji pomiędzy jednostkami samorządu terytorialnego, w szczególności poprzez centra usług wspólnych, porozumienia JST oraz regionalne centra kompetencyjne. Takie rozwiązania pozwolą mniejszym jednostkom uzyskać dostęp do specjalistycznej wiedzy bez konieczności tworzenia własnych rozbudowanych struktur.

Jednocześnie należy rozwijać dostęp do ekspertów technicznych w obszarach wymagających specjalistycznej wiedzy, takich jak analiza podatności, testy bezpieczeństwa, monitoring zagrożeń czy obsługa incydentów. Zadania te mogą być w wielu przypadkach realizowane w formule usług wspólnych lub przez wyspecjalizowane podmioty zewnętrzne.

Rada odnotowuje znaczenie działań edukacyjnych związanych z rozwojem kształcenia w obszarze cyberbezpieczeństwa, w tym nowych kierunków i kwalifikacji zawodowych. Należy jednak podkreślić, że przygotowanie odpowiednich kadr technicznych jest procesem wieloletnim i nie rozwiąże krótkoterminowo problemu braku zdolności organizacyjnych JST.

Dlatego priorytetem powinno być szybkie zwiększenie kompetencji zarządczych istniejących struktur administracji samorządowej oraz stworzenie mechanizmów współpracy umożliwiających skuteczną realizację obowiązków wynikających z KSC.

4. Wsparcie kompetencji JST w zakresie stosowania Prawa zamówień publicznych dla zapewnienia cyberbezpieczeństwa oraz kompetencji zakupowych

Rada rekomenduje opracowanie i upowszechnienie wytycznych dla jednostek samorządu terytorialnego dotyczących wykorzystania istniejących instrumentów ustawy Prawo zamówień publicznych w procesie pozyskiwania usług i rozwiązań związanych z cyberbezpieczeństwem oraz systemów, usług i produktów IT.

Podstawowym wyzwaniem JST nie jest brak możliwości prawnych realizacji bezpiecznych zamówień, lecz ograniczona zdolność organizacyjna do przygotowania postępowań, które uwzględniają ryzyko cyberbezpieczeństwa, bezpieczeństwo łańcucha dostaw oraz długoterminowe utrzymanie usług. Zakup rozwiązania technicznego bez odpowiedniego określenia wymagań, zasad odpowiedzialności i sposobu zarządzania usługą nie zapewnia rzeczywistej odporności cyfrowej.

Materiały te powinny mieć charakter neutralny technologicznie i wspierać konkurencyjność rynku, umożliwiając mniejszym JST przygotowanie bezpiecznych postępowań bez konieczności posiadania własnych zespołów eksperckich.

Szczególnie istotne jest wykorzystanie możliwości wspólnych zakupów i współpracy między jednostkami samorządu terytorialnego, w tym poprzez porozumienia JST, związki samorządowe oraz centra usług wspólnych. Pozwala to ograniczyć koszty, zwiększyć jakość zamówień oraz zapewnić dostęp do kompetencji, których pojedyncze jednostki nie są w stanie utrzymać.

W przypadku zamówień dotyczących cyberbezpieczeństwa JST oraz systemów, usług czy produktów IT powinny również stosować zasadę ograniczonego ujawniania informacji technicznych, których publikacja mogłaby zwiększać ryzyko ataku, przy jednoczesnym zachowaniu zasad przejrzystości wydatkowania środków publicznych.

5. Wykorzystanie krajowego systemu certyfikacji cyberbezpieczeństwa jako narzędzia wsparcia JST w ocenie dostawców usług bezpieczeństwa

Rada rekomenduje wykorzystanie mechanizmów przewidzianych w ustawie o krajowym systemie certyfikacji cyberbezpieczeństwa jako elementu ograniczania ryzyka związanego z wyborem i nadzorowaniem dostawców usług cyberbezpieczeństwa przez jednostki samorządu terytorialnego.

Krajowy system certyfikacji cyberbezpieczeństwa powinien być wykorzystywany jako jeden z instrumentów wspierających JST w procesach zakupowych i organizacyjnych, w szczególności przy wyborze usług takich jak:

- usługi monitorowania bezpieczeństwa (SOC/MDR);

- audyty bezpieczeństwa i testy bezpieczeństwa;
- usługi reagowania na incydenty;
- rozwiązania chmurowe;
- systemy ochrony danych i kopii zapasowych;
- rozwiązania wspierające zarządzanie podatnościami.

System certyfikacji powinien wspierać budowę zaufania do rynku usług cyberbezpieczeństwa, jednak kluczowym czynnikiem odporności JST pozostaje zdolność organizacyjna do świadomego zarządzania dostawcami, ryzykiem technologicznym oraz bezpieczeństwem świadczonych usług publicznych.

6. Wzmocnienie kompetencji JST w zakresie stosowania przepisów o dostępie do informacji publicznej z uwzględnieniem wymogów cyberbezpieczeństwa

Rada rekomenduje opracowanie wytycznych i rozwój kompetencji jednostek samorządu terytorialnego w zakresie stosowania ustawy o dostępie do informacji publicznej w sposób zapewniający równowagę pomiędzy zasadą jawności działania administracji publicznej a koniecznością ochrony informacji, których ujawnienie mogłoby zwiększyć ryzyko cyberzagrożeń.

Obowiązujące przepisy zapewniają możliwość ochrony informacji, których ujawnienie może naruszać prawnie chronione interesy lub bezpieczeństwo funkcjonowania systemów teleinformatycznych. Kluczowym problemem nie jest zatem brak podstaw prawnych, lecz brak jednolitej praktyki i kompetencji pozwalających JST prawidłowo oceniać charakter informacji.

Ochronie przed nieuprawnionym ujawnieniem powinny podlegać przede wszystkim informacje techniczne i operacyjne, których publikacja może ułatwić przeprowadzenie ataku.

Rada rekomenduje rozwijanie praktyki proporcjonalnej oceny informacji, tak aby ochrona cyberbezpieczeństwa nie była wykorzystywana do ograniczania transparentności działania administracji, lecz służyła ochronie konkretnych zasobów i procesów, których ujawnienie mogłoby realnie zwiększyć ryzyko cyberataku.

7. Opracowanie i wdrożenie pakietu dobrych praktyk cyberbezpieczeństwa dla JST

Rada rekomenduje opracowanie i wdrożenie kompleksowego pakietu dobrych praktyk cyberbezpieczeństwa dla jednostek samorządu terytorialnego, dostosowanego do zróżnicowanego charakteru, wielkości i poziomu dojrzałości organizacyjnej JST.

Celem działania nie powinno być tworzenie kolejnych formalnych obowiązków, lecz zapewnienie samorządom praktycznych narzędzi umożliwiających skuteczną realizację wymagań wynikających ze znowelizowanej ustawy o krajowym systemie cyberbezpieczeństwa oraz podejścia wynikającego z dyrektywy NIS2.

1. **Zarządzanie procesami** - podstawą dobrych praktyk powinno być podejście procesowe obejmujące ocenę mapy procesów z identyfikacją procesów kluczowych dla danego JST, następnie określenie procesów wspierających i zarządczych. Kolejnym krokiem powinno być określenie systemów IT utrzymujących procesy kluczowe, do których następnie wykonana zostanie analiza ryzyka oraz analiza ciągłości działania.
2. **Wzorcowa dokumentacja i narzędzia operacyjne dla JST -** Rada rekomenduje przygotowanie centralnego pakietu wzorcowych dokumentów, procedur, checklist i instrukcji operacyjnych, które JST mogłyby dostosować do własnej struktury organizacyjnej, zasobów i profilu ryzyka. Materiały powinny być przygotowane w sposób praktyczny, zrozumiały również dla osób nietechnicznych. Celem nie powinno być samo posiadanie dokumentacji, lecz zapewnienie, że procedury są znane, aktualne i okresowo testowane.
3. **Katalog dobrych praktyk technicznych cyberbezpieczeństwa -** Rada rekomenduje przygotowanie katalogu dobrych praktyk technicznych, który będzie wspierał JST w planowaniu zabezpieczeń i przygotowaniu zamówień publicznych. Katalog powinien mieć charakter neutralny technologicznie i wskazywać minimalne funkcjonalności, a nie konkretne produkty lub producentów.
4. **Wsparcie wdrożeniowe dla JST w zakresie uKSC/NIS2 -** Rada rekomenduje przygotowanie programu edukacyjnego i wdrożeniowego dla JST, którego celem będzie przełożenie wymagań prawnych na praktyczne działania. Program powinien uwzględniać, że JST różnią się skalą działania, zasobami i zakresem odpowiedzialności.
5. **Wsparcie poprzez centra usług wspólnych i współpracę JST** - pakiet dobrych praktyk powinien być wdrażany z wykorzystaniem istniejących mechanizmów współpracy samorządowej, w szczególności centrów usług wspólnych, porozumień JST oraz regionalnych struktur wsparcia.

Agnieszka Jankowska
Przewodnicząca Rady do Spraw Cyfryzacji
/podpisano elektronicznie/

PODPIS ZAUFANY
AGNIESZKA
JANKOWSKA
19.08.2026 10:41:06 GMT+0200
Dokument podpisany elektronicznie
podpisem zaufanym