NAJWYŻSZA IZBA KONTROLI
Departament Administracji Publicznej

KAP.410.2.7.2025

Pani Barbara Gąsiorowska
Burmistrz Miasta i Gminy
Nowe Miasto nad Pilicą

Urząd Miasta i Gminy
Nowe Miasto nad Pilicą
Plac O.H. Koźmińskiego 1/2
26-420 Nowe Miasto nad Pilicą

WYSTĄPIENIE POKONTROLNE

P/25/003 Realizacja projektu Cyberbezpieczny Samorząd

NAJWYŻSZA IZBA KONTROLI
Departament Administracji Publicznej
ul. Filtrowa 57, 02-056 Warszawa
tel. 48224445308, kap@nik.gov.pl

I. Dane identyfikacyjne

Jednostka kontrolowana	Urząd Miasta i Gminy Nowe Miasto nad Pilicą[1], Plac O. H. Koźmińskiego 1/2, 26-420 Nowe Miasto nad Pilicą
Kierownik jednostki kontrolowanej	Barbara Gąsiorowska, Burmistrz Miasta i Gminy Nowe Miasto nad Pilicą (dalej: Burmistrz), od 7 maja 2024 r. W okresie objętym kontrolą funkcję kierownika jednostki poprzednio pełnili: Mariusz Dziuba, Burmistrz Miasta i Gminy Nowe Miasto nad Pilicą, od 22 listopada 2018 r. do 6 maja 2024 r.
Zakres przedmiotowy kontroli	Realizacja przez Miasto i Gminę Nowe Miasto nad Pilicą działań w celu zwiększenia poziomu cyberbezpieczeństwa.
Okres objęty kontrolą	Od 1 stycznia 2023 r. do dnia zakończenia czynności kontrolnych, tj. 5 września 2025 r.
Podstawa prawna podjęcia kontroli	Art. 2 ust. 2 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli[2]
Jednostka przeprowadzająca kontrolę	Najwyższa Izba Kontroli Departament Administracji Publicznej
Kontroler	Łukasz Hertel, główny specjalista kontroli państwowej, upoważnienie do kontroli nr KAP/64/2025 z 25 czerwca 2025 r.

(akta kontroli str. 1-8)

[1] Dalej: Urząd.
[2] Dz. U. z 2022 r. poz. 623, dalej: ustawa o NIK.

II. Ocena ogólna[3] kontrolowanej działalności

OCENA OGÓLNA

Gmina Nowe Miasto nad Pilicą[4] w latach 2023 – 2025 podejmowała działania na rzecz zwiększenia poziomu cyberbezpieczeństwa realizując projekt pn. *Wzmocnienie cyberbezpieczeństwa w Urzędzie Miasta i Gminy Nowe Miasto nad Pilicą* (dalej: Projekt) na potrzeby Urzędu. W ramach Projektu m.in. przeprowadzono postępowanie przetargowe oraz zawarto umowę na zakup urządzeń i oprogramowania zwiększających odporność na cyberataki, a także zawarto umowy na przeprowadzenie audytów z zakresu diagnozy cyberbezpieczeństwa oraz przygotowania dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (dalej: SZBI). Ponadto, podjęto działania informacyjne dotyczące otrzymania dofinansowania i realizacji Projektu. Stwierdzone w trakcie kontroli nieprawidłowości nie miały istotnego wpływu na realizację Projektu.

Uzasadnienie oceny ogólnej

W okresie objętym kontrolą w Urzędzie rozpoznano potrzeby w zakresie zwiększenia poziomu cyberbezpieczeństwa, m.in. dokonano analizy stanu zabezpieczeń infrastruktury informatycznej funkcjonujących w Urzędzie. W latach 2023-2024 przeprowadzono okresowy audyt z zakresu bezpieczeństwa informacji oraz wdrażano rekomendacje w nim zawarte. W związku z przystąpieniem do Projektu wypełniono *Ankietę Dojrzałości Cyberbezpieczeństwa w Jednostkach Samorządu Terytorialnego* (dalej: Ankieta) i przekazano ją do Operatora[5] z zachowaniem terminu i form określonych w umowie o powierzenie grantu[6] (dalej: umowa grantowa) zawartej 16 lipca 2024 r. z Centrum Projektów Polska Cyfrowa (dalej: CPPC lub Grantodawca). W ramach tej umowy przyznano Grantobiorcy dofinansowanie na realizację Projektu w kwocie 555 119,78 zł[7]. Wydatki poniesione przez Grantobiorcę w ramach Projektu w okresie objętym kontrolą wyniosły 448 953,53[8] i dotyczyły w szczególności zakupu urządzeń i oprogramowania zwiększających odporność na cyberataki, przeprowadzenia audytu z zakresu diagnozy cyberbezpieczeństwa oraz przygotowania dokumentacji SZBI. Z otrzymanego dofinansowania wykorzystano dotychczas 76,02% środków. Zostały one zrealizowane zgodnie z wytycznymi dotyczącymi kwalifikowalności wydatków oraz w ramach limitów zatwierdzonych we Wniosku[9].

W toku kontroli stwierdzono nieprawidłowości polegające na:

- niewdrożeniu Systemu Zarządzania Bezpieczeństwem Informacji, o którym mowa w § 20 ust. 1 w związku z ust. 3 starego rozporządzenia KRI[10] oraz § 19 ust. 1 w związku z ust. 3 rozporządzenia KRI[11],

---

[3] Najwyższa Izba Kontroli formułuje ocenę ogólną jako ocenę pozytywną, ocenę negatywną albo ocenę w formie opisowej.

[4] Dalej: Gmina lub Grantobiorca.

[5] Tj. do Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego.

[6] Umowa nr FERC.02.02-CS.01-001/23/1703/FERC.02.02-CS.01-001/23/2024.

[7] Tj. w kwocie wskazanej we Wniosku o przyznanie grantu nr 7073bfb9-dac1-4fc2-acd2-e24d01f7d503 (dalej: Wniosek), z tego budżet państwa (dalej: BP) – 94 370,29 zł, budżet środków europejskich (dalej: BŚE) – 460 749,47 zł.

[8] Według stanu na 5 września 2025 r., w tym BŚE – 350 273,5 zł, BP – 71 742,8 zł, wkład własny – 26 937,2 zł.

[9] Stanowiącym załącznik nr 3 do umowy grantowej.

[10] Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie 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 2017 r. poz. 2247, dalej: stare rozporządzenie KRI).

[11] Rozporządzenie Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji

- nieoznaczeniu miejsca realizacji Projektu plakatem informującym o dofinansowaniu, a także niezamieszczeniu opisu Projektu w mediach społecznościowych oraz nieprzestrzeganiu niektórych obowiązków informacyjnych i promocyjnych w zakresie stosowania oznaczeń: znakiem Unii Europejskiej i Funduszy Europejskich, i barw Rzeczypospolitej Polskiej - w publikowanych informacjach na stronie internetowej i części dokumentacji projektowej, co było niezgodne z postanowieniami § 11 ust. 3 umowy grantowej,
- przechowywaniu w serwerowni, tj. pomieszczeniu podlegającemu szczególnej ochronie materiałów łatwopalnych, tj. kartonów i wyeksploatowanego sprzętu komputerowego, co zwiększało ryzyko utraty danych bądź zakłócenia ciągłości działania Urzędu na skutek pożaru i było niezgodne z § 19 ust. 2 pkt 9 rozporządzenia KRI.

III. Opis ustalonego stanu faktycznego oraz oceny cząstkowe[12] kontrolowanej działalności

OBSZAR

1. Realizacja przez Miasto i Gminę Nowe Miasto nad Pilicą działań w celu zwiększenia poziomu cyberbezpieczeństwa.

Opis stanu faktycznego

1. *Strategia Rozwoju Miasta i Gminy Nowe Miasto nad Pilicą na lata 2022-2028*[13] (dalej: Strategia) jest obowiązującym dokumentem określającym obszary działań, cele oraz rekomendacje w zakresie kształtowania i prowadzenia polityki przestrzennej w gminie. W dokumencie tym wskazano cele strategiczne, operacyjne m.in. *Wdrożenie i upowszechnienie nowoczesnych e- usług wśród mieszkańców*, natomiast nie zawarto zagadnień dotyczących zwiększenia poziomu cyberbezpieczeństwa. Sekretarz Gminy wyjaśniła[14], że *w Strategii Rozwoju Miasta i Gminy Nowe Miasto nad Pilicą na lata 2022-2028 nie uwzględniono zagadnień związanych z cyberbezpieczeństwem, ponieważ na etapie przystępowania do prac nad dokumentem strategicznym tj. w 2021 roku, nie przeprowadzono analizy w tym zakresie. Stosowne analizy zostały wykonane dopiero na potrzeby opracowania wniosku o dofinansowanie projektu Cyberbezpieczny Samorząd*.

(akta kontroli str. 61-125, 138-143, 152-157)

2. W okresie objętym kontrolą w Urzędzie rozpoznano potrzeby w zakresie zwiększenia cyberbezpieczeństwa w związku z przygotowaniem wniosku dotyczącego realizacji Projektu oraz potrzeb zakupowych poprzez m.in. wewnętrzne analizy stanu infrastruktury informatycznej, w tym stosowanych systemów zabezpieczeń. Ponadto Sekretarz Gminy wskazała, że stosowano również *zalecenia oraz dobre praktyki publikowane przez instytucje państwowe*

---

w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U poz. 773, dalej: rozporządzenie KRI). Rozporządzenie uchylało stare rozporządzenie KRI.

[12] Oceny cząstkowe to oceny działalności w poszczególnych obszarach badań kontrolnych. Ocena cząstkowa może być sformułowana jako ocena pozytywna, ocena negatywna albo ocena w formie opisowej.

[13] Przyjęta Uchwałą nr XXXII/215/2021 Rady Miejskiej w Nowym Mieście nad Pilicą z dnia 20 maja 2021 r. W okresie objętym kontrolą dokument nie był aktualizowany.

[14] Na podstawie Zarządzenia Nr 134/2024 Burmistrza Miasta i Gminy Nowe Miasto nad Pilicą z dnia 7 sierpnia 2024 roku, w sprawie upoważnienia Sekretarza Miasta i Gminy do wykonywania w imieniu Burmistrza Miasta i Gminy niektórych zadań.

zajmujące się tematyką cyberbezpieczeństwa oraz rozeznanie rynku i zapoznanie się z ofertami dostępnych rozwiązań technicznych oraz usług zwiększających odporność na cyberataki.

(akta kontroli str. 152-157)

3. Zgodnie z § 4 ust. 1 pkt 4 umowy grantowej w terminie 30 dni od dnia jej zawarcia, Urząd przekazał[15] do Operatora za pośrednictwem skrzynki ePUAP Ankietę.

(akta kontroli str. 126-143)

4. Projekt *Wzmocnienie cyberbezpieczeństwa w Urzędzie Miasta i Gminy Nowe Miasto nad Pilicą* był realizowany w ramach programu Fundusze Europejskie na Rozwój Cyfrowy (dalej: FERC), Priorytet II Zaawansowane usługi cyfrowe, Działanie 2.2 Wzmocnienie krajowego systemu cyberbezpieczeństwa. Powierzenie grantu nastąpiło na podstawie umowy grantowej, której przedmiotem było przyznanie Grantobiorcy dofinansowania na realizację Projektu w kwocie 555 119,78 zł. Zakres przedmiotowy grantu wskazany we Wniosku o dofinansowanie obejmował realizację zadań w trzech obszarach określonych w Regulaminie Konkursu Grantowego pn. „Cyberbezpieczny Samorząd"[16] – organizacyjnym, technicznym oraz kompetencyjnym. Projekt miał być realizowany w okresie maksymalnie 24 miesięcy od dnia wejścia w życie umowy grantowej, tj. do 16 lipca 2026 r.

(akta kontroli str. 583-612)

Głównym celem Projektu, jak wskazano we Wniosku o dofinansowanie, było wzmocnienie cyberbezpieczeństwa w Urzędzie Miasta i Gminy Nowe Miasto nad Pilicą. Realizacja Projektu została podzielona na trzy zadania, tj.:

- Zadanie 1 – polegało na: doradztwie w zakresie określenia poziomu cyberbezpieczeństwa wraz z audytem wstępnym i końcowym, przygotowaniu dokumentacji SZBI wraz z przeprowadzeniem analizy ryzyka.
- Zadanie 2 – polegało na: zakupie oraz wdrożeniu systemów i urządzeń podnoszących bezpieczeństwo informacji w Urzędzie, takich jak m.in.: system NAC[17], system SIEM[18], oprogramowanie do zarządzania infrastrukturą IT, system do zbierania i analizy logów, system zarządzania podatnościami, centralny zasilacz awaryjny, agregat zasilający oraz nowy serwer.
- Zadanie 3 – polegało na przeprowadzeniu szkoleń dla pracowników Urzędu w zakresie cyberbezpieczeństwa.

(akta kontroli str. 574-582)

5. Zgodnie z § 5 ust. 1 umowy grantowej, dofinansowanie udzielone Grantobiorcy miało zostać wypłacone w przypadku pierwszej transzy w terminie 60 dni kalendarzowych od dnia zawarcia umowy, natomiast

[15] 14 sierpnia 2024 r.
[16] https://www.gov.pl/web/cppc/cyberbezpieczny-samorzad
[17] System NAC (Network Access Control) to rozwiązanie bezpieczeństwa, które kontroluje dostęp do sieci, zapewniając, że tylko autoryzowani użytkownicy i urządzenia mogą się do niej dostać.
[18] System SIEM (Security Information and Event Management) to rozwiązanie, które pomaga organizacjom w zarządzaniu bezpieczeństwem poprzez zbieranie, analizowanie i korelowanie danych z różnych źródeł w czasie rzeczywistym.

w przypadku drugiej i trzeciej transzy – w terminie do 60 dni kalendarzowych od zaakceptowania przez Operatora wniosku o wypłatę kolejnej transzy.
W dniu 12 sierpnia 2024 r. Burmistrz zwróciła się do CPPC z wnioskiem o wypłatę pełnej przyznanej kwoty w ramach Projektu w jednej transzy w wysokości 100% grantu, argumentując m.in. *że realizacja projektu w sposób całościowy umożliwi przeprowadzenie kompleksowych działań w sposób szybki i zapewniający wsparcie na każdym etapie wdrożenia*. Środki ostatecznie zostały przekazane w dwóch zaliczkach, tj. 6 września 2024 r. oraz 21 października 2024 r. W ramach pierwszej zaliczki przekazano kwotę 166 535,93 zł (BŚE – 138 224,84 zł BP-28 311,09 zł), a w ramach drugiej zaliczki przekazano 388 583,85 zł (BŚE – 322 524,65 zł, BP – 66 059,2 zł).

(akta kontroli str. 198-205, 230-232, 627-629)

W celu realizacji Projektu, Urząd 24 lutego 2024 r. zawarł z firmą zewnętrzną umowę na *Świadczenie usług doradczych w aspektach technicznych i merytorycznych w ramach konkursu Cyberbezpieczny Samorząd* w ramach której przewidziano: określenie poziomu cyberbezpieczeństwa i opracowanie raportu z audytu przed wdrożeniem Projektu oraz po zakończeniu realizacji zadań niezbędnych do osiągnięcia jego celu. Łączna wartość zamówionych usług w ramach tej umowy wyniosła 33 702zł, w ramach dofinansowania stanowiła 5,7% wartości grantu (z BŚE 26 294,3 zł, z BP – 5385,58 zł, wkład własny – 2002,12 zł). Do dnia zakończenia kontroli Wykonawca zrealizował pierwszą część umowy[19] na kwotę 16 851 zł (z BŚE 13 147,15 zł, z BP – 2692,79 zł, wkład własny – 1001,06 zł). Ustalono, że po zleconym w ramach Projektu audycie sformułowane zostały wnioski/rekomendacje, z których część została wdrożona, a część została zaplanowana do realizacji w późniejszym okresie.

(akta kontroli str. 576-59, 807-821, DVD-1 pliki: 081-085)

W dniu 15 kwietnia 2025 r. Urząd zawarł z firmą zewnętrzną umowę na *Świadczenie usług doradczych w aspektach technicznych i merytorycznych w ramach konkursu Cyberbezpieczny Samorząd* w ramach której przewidziano: przygotowanie i wdrożenie dokumentacji SZBI. Łączna wartość poniesionych wydatków na zamówione usług w ramach tej umowy wyniosła 23 985 zł, co stanowiło 4,06% wartości grantu (z BŚE 18 713,1 zł, z BP – 3832,8 zł, wkład własny – 1439,1 zł). Zgodnie z protokołem wykonania przedmiotowej umowy, opracowane dokumenty zostały przekazane w terminie, a umowa została wykonana zgodnie z jej zakresem i postanowieniami. Opracowana dokumentacja SZBI przygotowywana jest do formalnego wdrożenia[20].

(akta kontroli str. 801-821, DVD-1 pliki: 086-089)

Urząd w dniu 22 maja 2025 r. wszczął postępowanie[21] na *Zakup, dostawę i wdrożenie systemów i nowych urządzeń podnoszących bezpieczeństwo informacji w urzędzie oraz przeszkolenie pracowników urzędu w zakresie*

[19] *Raport z oceny zgodności z Krajowymi Ramami Interoperacyjności oraz Krajowym Systemem Cyberbezpieczeństwa* przekazano w dniu 18 marca 2025 r.
[20] Tj. po uruchomieniu wszystkich rozwiązań technicznych przewidzianych w ramach realizacji Projektu oraz dokonaniu aktualizacji dokumentacji uwzględniającej końcowe zmiany w infrastrukturze teleinformatycznej.
[21] Oznaczenie sprawy INF.271.1.2025.RD.

cyberbezpieczeństwa, w wyniku którego 9 czerwca 2025 r. zawarto z firmą zewnętrzną umowę, która była podzielona na dwa etapy[22]. Do dnia 5 września 2025 r. zrealizowano I etap umowy w ramach którego na potrzeby Urzędu dokonano zakupu m.in.: oprogramowania do zarządzania infrastrukturą IT, jednego Systemu NAC, jednego systemu SIEM, jednego systemu do analizy ruchu sieci Fortianalyzer[23], jednego systemu do zarządzania podatnościami, oprogramowania DLP Protection Suite Protector[24], oprogramowania EDR[25], zasilacza awaryjnego UPS, Licencji dla UTM[26], dwóch dysków NAS[27] oraz przeprowadzono szkolenie z zakresu cyberbezpieczeństwa dla 40 pracowników. Łączna wartość zakupionych urządzeń i zamówionych usług w ramach tej umowy wyniosła 531 023,72 zł i stanowiła 89,91% wartości grantu (z BŚE – 414 304,7 zł, z BP – 84 857,6 zł, wkład własny – 31 861,4 zł). Zgodnie z protokołem odbioru wykonania I etapu przedmiotu umowy zamówienie zrealizowano w dniu 29 lipca 2025 r. Etap II umowy przewidywał dostawę i podłączenie generatora prądu. Sekretarz Gminy wskazała, że *przewidywany termin zakończenia realizacji to koniec października 2025 r., obecnie przygotowywane jest podłoże pod generator oraz zlecenie instalacji elektrycznej w urzędzie – przyłącze do generatora.* Do dnia zakończenia kontroli w ramach zawartej umowy wydatkowano kwotę 408 117,53 zł (z BŚE – 318 413,44 zł, BP – 65 217,21 zł, wkład własny 24 487,06 zł).

(akta kontroli str. 248-572, 807-821 DVD-1 pliki: 091-094)

6. We wniosku o przyznanie grantu wskazano Urząd Miasta i Gminy Nowe Miasto nad Pilicą jako jedyny podmiot korzystający z wnioskowanych rozwiązań. W realizacji Projektu nie przewidziano udziału innych jednostek organizacyjnych Gminy. Sekretarz Gminy wskazała, że *umowa grantowa zawarta w ramach projektu Cyberbezpieczny Samorząd odnosi się wyłącznie do Urzędu Miasta i Gminy Nowe Miasto nad Pilicą jako podstawowej jednostki samorządu terytorialnego realizującej zadania publiczne (...) Projekt dotyczy więc bezpośrednio urzędu jako instytucji odpowiedzialnej za realizację zadań własnych i zleconych, a także jako administratora kluczowych zasobów informatycznych. Podległe jednostki organizacyjne, takie jak szkoły, ośrodek pomocy społecznej czy instytucje kultury, funkcjonują w oparciu o odrębne struktury organizacyjne, posiadają własnych administratorów systemów informatycznych oraz infrastrukturę techniczną (...)*.

(akta kontroli str. 138-143)

7. W ramach struktury organizacyjnej Urzędu zadania związane z wdrażaniem nowych technologii i koordynacją projektów o charakterze informatycznym realizowane były przez pracownika zatrudnionego na stanowisku informatyka.

---

[22] Etap I – do 29 lipca 2025 r., Etap II – do 31 grudnia 2025 r.

[23] FortiAnalyzer to zaawansowane narzędzie do analizy i zarządzania danymi bezpieczeństwa.

[24] Rozwiązania typu DLP (Data Loss Prevention), to narzędzia służące do ochrony danych przed ich przypadkową utratą, wyciekiem lub kradzieżą.

[25] EDR (Endpoint Detection and Response) to oprogramowanie, które służy do wykrywania, monitorowania i reagowania na zagrożenia na urządzeniach końcowych m.in. komputerach, laptopach, serwerach.

[26] Unified Threat Management - to zintegrowany system ochrony sieci komputerowej, który łączy w sobie kilka funkcjonalności, takich jak zapory sieciowe, systemy wykrywania i zapobiegania atakom, serwery poczty elektronicznej, VPN, antywirusy i filtry treści internetowych.

[27] Urządzenia magazynujące dane, podłączone do sieci, umożliwiają centralne przechowywanie, udostępnianie i zabezpieczanie danych.

Sekretarz Gminy wskazała, że *realizacja zadań w ramach projektu wykonywana była zgodnie zakresem obowiązków służbowych oraz poleceń przełożonych.* W realizację Projektu od strony organizacyjnej, technicznej i merytorycznej zaangażowanych było sześć osób. Osoby te zostały wyznaczone na podstawie zakresu przypisanych im zadań, odpowiadających ich kompetencjom i kwalifikacjom zawodowym.

(akta kontroli str. 9-60, 138-143, 798-800)

8. Według stanu na dzień 3 września 2025 r. nie wystąpiła fluktuacja kadr utrudniająca sprawną realizację grantu[28].

(akta kontroli str. 798-800)

9. Zgodnie z § 3 ust. 2 pkt 2 umowy grantowej, zakończenie realizacji Projektu obejmuje m.in. złożenie wniosku rozliczającego z uwzględnieniem osiągnięcia wskaźników Projektu. Sekretarz Gminy wskazała, że *wskaźniki realizacji projektu pn. Cyberbezpieczny Samorząd zostały szczegółowo określone w Załączniku nr 9 do Regulaminu Projektu. Wskaźniki te stanowią podstawę oceny efektywności wdrożonych działań oraz osiągnięcia celów projektu. Zgodnie z postanowieniami regulaminowymi, pomiar wartości wskaźników zostanie przeprowadzony po zakończeniu realizacji przedsięwzięcia, w ramach procesu składania końcowego wniosku o rozliczenie projektu. Weryfikacja wskaźników będzie służyła potwierdzeniu stopnia realizacji założonych rezultatów.*

(akta kontroli str. 138-143, 613-624)

10. W toku kontroli dokonano oględzin zakupionego sprzętu, oprogramowania i ustalono, że sprzęt został uruchomiony, działa prawidłowo, a systemy: NAC, SIEM, Fortinite zostały skonfigurowane, m.in. monitorują i kontrolują dostęp do sieci, analizują dane w celu wykrywania zagrożeń, zarządzają ruchem sieciowym.
W trakcie oględzin w pomieszczeniu serwerowni stwierdzono obecność elementów niezgodnych z zasadami utrzymania środowiska IT, w tym: kartonów i opakowań, wyeksploatowanych jednostek komputerowych oraz innych elementów niemających związku z eksploatacją infrastruktury serwerowej (dalszy opis w sekcji *Stwierdzone nieprawidłowości*).

(akta kontroli str. 222-227, 238-247,)

11. Zgodnie z § 13 ust. 1 umowy grantowej, Grantobiorca zobowiązany był do utrzymania efektów Projektu, w tym do opracowania oraz wdrożenia procedury monitorowania utrzymania efektów Projektu przez okres minimum dwóch lat od jego zakończenia. Na dzień zakończenia czynności kontrolnych, tj. 5 września 2025 r., Projekt był w trakcie realizacji. Sekretarz Gminy wskazała, że *w celu zapewnienia trwałości rezultatów projektu Cyberbezpieczny Samorząd Urząd Miasta i Gminy Nowe Miasto nad Pilicą planuje podjąć następujące działania: utrzymanie oraz bieżąca eksploatacja zakupionych urządzeń i oprogramowania, zapewnienie regularnych aktualizacji systemów teleinformatycznych (...) Na etapie planowania projektu przewidziano także*

[28] W okresie objętym kontrolą nastąpiła zmiana na stanowisku Burmistrza – Projekt został rozpoczęty przez poprzedniego Burmistrza, a obecny Burmistrz kontynuuje jego realizację.

zapewnienie środków finansowych z budżetu gminy na pokrycie kosztów związanych z serwisem urządzeń oraz aktualizacją oprogramowania po zakończeniu okresu realizacji projektu. Opracowanie procedury monitorowania utrzymania efektów projektu Cyberbezpieczny Samorząd jest obecnie w toku. Trwają pracę nad przygotowaniem dokumentu określającego zasady weryfikacji stanu technicznego urządzeń, aktualizacji oprogramowania oraz monitorowania poziomu bezpieczeństwa systemów informatycznych.

(akta kontroli str. 219-221, 798-800)

12. W Urzędzie do dnia zakończenia czynności kontrolnych nie został wdrożony System Zarządzania Bezpieczeństwem Informacji, o którym mowa w § 20 ust. 1 w związku z ust. 3 starego rozporządzenia KRI oraz § 19 ust. 1 w związku z ust. 3 rozporządzenia KRI (dalszy opis w sekcji *Stwierdzone nieprawidłowości*).
W okresie objętym kontrolą w Urzędzie wdrożona została Polityka Ochrony Danych[29] dotycząca głównie bezpieczeństwa danych osobowych.

(akta kontroli str. 209-218)

13. Zgodnie z § 20 ust. 2 pkt 14 starego rozporządzenia KRI oraz §19 ust. 2 pkt 14 rozporządzenia KRI w Urzędzie przeprowadzano okresowe audyty wewnętrzne z zakresu bezpieczeństwa informacji. W wyniku przeprowadzonych audytów przedstawiono rekomendacje, z czego część została wdrożona natomiast, pozostałe zaplanowano do realizacji po zakończeniu Projektu, w związku z koniecznością zakupu odpowiednich urządzeń i wdrożenia dodatkowych rozwiązań technicznych.

(akta kontroli str. 144-151, 630-797)

14. Na podstawie § 11 ust. 3 umowy grantowej, w zakresie informacji i promocji Projektu Grantobiorca zobowiązany był do stosowania zasad określonych w *Podręczniku wnioskodawcy i beneficjenta programów polityki spójności na lata 2021-2027 w zakresie informacji i promocji* (dalej: Podręcznik). Obowiązek obejmował w szczególności:
    - oznaczenie miejsca realizacji Projektu poprzez umieszczenie plakatu;
    - zamieszczenie znaków Funduszy Europejskich, barw RP i Unii Europejskiej na dokumentach związanych z Projektem, w tym na dokumentacji przetargowej, umowach, stronach internetowych, e-publikacjach;
    - umieszczenie opisu Projektu na stronie internetowej oraz w mediach społecznościowych urzędu.

Na stronie internetowej Urzędu[30] umieszczono informacje dotyczące realizacji Projektu oraz jego dofinansowania ze środków Unii Europejskiej. Urząd nie oznaczył miejsca realizacji Projektu poprzez umieszczenie plakatu informującego o fakcie otrzymania dofinansowania oraz nie zamieścił opisu Projektu w mediach społecznościowych. Ponadto ustalono, że zakres informacji publikowanych na stronie internetowej, a także oznaczenie części dokumentów

---

[29] Wprowadzona Zarządzeniem nr 57/2018 z dnia 30 lipca 2018 r. Burmistrza Miasta i Gminy Nowe Miasto nad Pilicą w sprawie wprowadzenia Polityki Ochrony Danych. Zaktualizowana Zarządzeniem nr 44/2025 z dnia 17 marca 2025r. Burmistrza Miasta i Gminy Nowe Miasto nad Pilicą w sprawie aktualizacji polityki ochrony danych

[30] Cyberbezpieczny samorząd - otrzymano dofinansowanie - Aktualności - UMiG Nowe Miasto nad Pilicą

związanych z realizacją Projektu nie były zgodne z wymaganiami określonymi w Podręczniku (dalszy opis w sekcji *Stwierdzone nieprawidłowości*).

(akta kontroli str. 233-237, 248-259)

Stwierdzone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie stwierdzono następujące nieprawidłowości:

1. Niewdrożenie Systemu Zarządzania Bezpieczeństwem Informacji.
   W okresie objętym kontrolą w Urzędzie nie został wdrożony SZBI, co było niezgodne z § 20 ust. 1 w związku z ust. 3 starego rozporządzenia KRI oraz z § 19 ust. 1 w związku z ust. 3 rozporządzenia KRI. Stosownie do ww. przepisów Urząd zobowiązany był m.in. do opracowania, ustanowienia, wdrożenia, monitorowania i doskonalenia SZBI, zapewniającym poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów jak rozliczalność, autentyczność, niezaprzeczalność i niezawodność.
   Sekretarz Gminy wyjaśniła, że *planowane jest wdrożenie SZBI. Dokument został opracowany i obecnie znajduje się na etapie finalnej weryfikacji. Jego formalne przyjęcie planowane jest na czwarty kwartał 2025 roku, na podstawie zarządzenia Burmistrza Miasta i Gminy Nowe Miasto nad Pilicą. Projekt Polityki Zarządzania Bezpieczeństwem Informacji został przygotowany w ramach realizacji grantu Cyberbezpieczny Samorząd. (...)*
   (akta kontroli str. 209-218, 807-821, DVD-1 pliki: 020-075, 659-707)
2. Nieoznaczenie miejsca realizacji Projektu plakatem informującym o dofinansowaniu, a także niezamieszczenie opisu Projektu w mediach społecznościowych oraz nieprzestrzeganie niektórych obowiązków informacyjnych i promocyjnych w zakresie stosowania oznaczania znakiem Unii Europejskiej i Funduszy Europejskich, i barw Rzeczypospolitej Polskiej w publikowanych informacjach na stronie internetowej i części dokumentacji projektowej, co było niezgodne z postanowieniami § 11 ust. 3 umowy grantowej.
   Obowiązki informacyjne i promocyjne muszą być wypełniane od momentu podpisania umowy (punkt 3 Podręcznika). W toku kontroli ustalono, że nie zamieszczono plakatu informującego o realizacji Projektu oraz żadnych informacji na oficjalnym profilu mediów społecznościowych w zakresie jego realizacji. Część dokumentów[31] nie posiadała oznaczenia, wymaganego umową, tzn. nie zostały oznaczone znakiem Unii Europejskiej, barwami Rzeczypospolitej Polskiej i znakiem Funduszy Europejskich.
   Ustalono także, że Urząd w dniu 10 maja 2024 r. zamieścił informację na stronie internetowej Urzędu o otrzymaniu dofinansowania, natomiast zamieszczone informacje nie spełniały wymogów określonych w Podręczniku, gdyż brak było m.in. informacji o: otrzymaniu wsparcia finansowego z Unii Europejskiej, czyli: znaku Funduszy Europejskich, znaku

[31] M.in.: SWZ, ogłoszenie o zamówieniu, opis przedmiotu zamówienia, odpowiedź na pytania, informacja z otwarcia ofert, zawiadomienie o wyborze najkorzystniejszej oferty, protokół postępowania w trybie podstawowym.

barw Rzeczypospolitej Polskiej i znaku Unii Europejskiej; zadaniach, działaniach, które będą realizowane w projekcie (opis, co zostanie zrobione, zakupione, itp.); efektach, rezultatach projektu (jeśli opis zadań, działań nie zawiera opisu efektów, rezultatów); hasztagi: #FunduszeUE lub #FunduszeEuropejskie.

Sekretarz Gminy wyjaśniła, że m.in.: *w związku z realizacją działań informacyjno-promocyjnych w ramach Grantu uprzejmie informujemy, iż brak oznaczeń wymaganych postanowieniami umowy wynikał z niezamierzonego przeoczenia. Po zidentyfikowaniu nieprawidłowości, we wszystkich możliwych przypadkach dokonano niezwłocznego uzupełnienia brakujących elementów, zgodnie z wytycznymi zawartymi w Podręczniku wnioskodawcy i beneficjenta programów polityki spójności na lata 2021-2027.*

W związku z usunięciem stwierdzonej nieprawidłowości w trakcie trwania czynności kontrolnych, NIK odstępuje od formułowania wniosku pokontrolnego w tym zakresie.

(akta kontroli str. 233-237, 248-257, 583-612)

3. Umieszczenie w pomieszczeniu podlegającemu szczególnej ochronie, tj. serwerowni elementów niezgodnych z zasadami utrzymania środowiska IT, w tym m.in. materiałów łatwopalnych - kartonów i opakowań, wyeksploatowanych jednostek komputerowych oraz innych elementów niemających związku z eksploatacją infrastruktury serwerowej, co było niezgodne z § 19 ust. 2 pkt 9 rozporządzenia KRI.

   Sekretarz Gminy wyjaśniła, że *obecność wskazanych elementów w pomieszczeniu serwerowni wynikała z czasowego zdeponowania wyeksploatowanych jednostek komputerowych i elementów metalowych w oczekiwaniu na ich przekazanie do utylizacji, oraz czasowe przechowywanie w nim opakowań po nowo zakupionym sprzęcie (...) Po stwierdzeniu nieprawidłowości podjęto działania naprawcze w postaci natychmiastowego usunięcia wszystkich elementów niezwiązanych z eksploatacją infrastruktury serwerowej.*

   Zdaniem NIK, w ramach zapewnienia bezpieczeństwa, w tym ochrony przeciwpożarowej, w serwerowni nie powinny (nawet krótkotrwale) znajdować się materiały łatwopalne, gdyż zwiększa to ryzyko pożaru co może prowadzić do: utraty danych, przerwania działania ważnych operacji, oraz znacznych strat finansowych. W związku z usunięciem stwierdzonej nieprawidłowości, NIK odstępuje od formułowania wniosku pokontrolnego w tym zakresie.

   (akta kontroli str. 222-224, 238-247)

IV. Wnioski

W związku ze stwierdzonymi nieprawidłowościami, Najwyższa Izba Kontroli, na podstawie art. 53 ust. 1 pkt 5 ustawy o NIK, przedstawia następujący wniosek:

Wniosek — Wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji.

V. Pozostałe informacje i pouczenia

Wystąpienie pokontrolne sporządzono w postaci elektronicznej z użyciem kwalifikowanych podpisów elektronicznych.

Prawo zgłoszenia zastrzeżeń

Zgodnie z art. 54 ustawy o NIK kierownikowi jednostki kontrolowanej przysługuje *prawo zgłoszenia* na piśmie umotywowanych zastrzeżeń do wystąpienia pokontrolnego, w terminie 21 dni od dnia jego przekazania. Zastrzeżenia zgłasza się do dyrektora Departamentu Administracji Publicznej. Prawo zgłaszania zastrzeżeń, zgodnie z art. 61b ust. 2 ustawy o NIK, nie przysługuje do wystąpienia pokontrolnego zmienionego zgodnie z treścią uchwały w sprawie zastrzeżeń.

Obowiązek poinformowania NIK o sposobie wykonania wniosku

Zgodnie z art. 62 ustawy o NIK należy poinformować Najwyższą Izbę Kontroli, w terminie 21 od otrzymania wystąpienia pokontrolnego, o sposobie wykonania wniosków pokontrolnych oraz o podjętych działaniach lub przyczynach niepodjęcia tych działań.

W przypadku wniesienia zastrzeżeń do wystąpienia pokontrolnego, termin przedstawienia informacji liczy się od dnia otrzymania uchwały o oddaleniu zastrzeżeń w całości lub zmienionego wystąpienia pokontrolnego.

Warszawa, 11 września 2025 r.

Kontroler

Łukasz Hertel

Główny specjalista kontroli państwowej

/podpisano elektronicznie/

Najwyższa Izba Kontroli

Departament Administracji Publicznej

p.o. Dyrektor

Bogdan Skwarka

/podpisano elektronicznie/