NAJWYŻSZA IZBA KONTROLI

Delegatura we Wrocławiu

LWR.410.14.1.2025

Pani
Małgorzata Krzyszkowska
Starosta Kamiennogórski

Starostwo Powiatowe
w Kamiennej Górze
ul. Broniewskiego 15
58-400 Kamienna Góra

WYSTĄPIENIE POKONTROLNE

P/25/003–„Realizacja projektu Cyberbezpieczny Samorząd”

NAJWYŻSZA IZBA KONTROLI
Delegatura we Wrocławiu
ul. marsz. Józefa Piłsudskiego 15-17, 50-044 Wrocław
tel. 48717118301, lwr@nik.gov.pl

I. Dane identyfikacyjne

Jednostka kontrolowana	Starostwo Powiatowe w Kamiennej Górze, ul. Broniewskiego 15, 58-400 Kamienna Góra[1].
Kierownik jednostki kontrolowanej	Małgorzata Krzyszkowska, Starosta Kamiennogórski, od 7 maja 2024 r. W okresie objętym kontrolą funkcję kierownika jednostki poprzednio pełnił: Jarosław Gęborys, od 20 listopada 2018 r. do 7 maja 2024 r.
Zakres przedmiotowy kontroli	Realizacja przez gminy i powiaty działań w celu zwiększenia poziomu cyberbezpieczeństwa.
Okres objęty kontrolą	Od 1 stycznia 2023 r. do dnia zakończenia czynności kontrolnych w 2025 r.[2]
Podstawa prawna podjęcia kontroli	Artykuł 2 ust. 2 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli[3].
Jednostka przeprowadzająca kontrolę	Najwyższa Izba Kontroli Delegatura we Wrocławiu
Kontroler	Cezary Mazik, główny specjalista kontroli państwowej, upoważnienie do kontroli nr LWR/133/2025 z dnia 19 maja 2025 r.

(akta kontroli: tom I, str. 1-3)

[1] Dalej: Starostwo.
[2] Czynności kontrolne zakończono 21 sierpnia 2025 r.
[3] Dz. U. z 2022 r. poz. 623; dalej: ustawa o NIK.

II. Ocena ogólna[4] kontrolowanej działalności

OCENA OGÓLNA

Powiat Kamiennogórski[5] w okresie objętym kontrolą podejmował działania w celu zwiększenia poziomu cyberbezpieczeństwa, w tym w ramach realizacji projektu Cyberbezpieczny Samorząd[6].

W Starostwie zapewniono stabilną i kompetentną obsadę kadrową zaangażowaną w nadzór i realizację Projektu. Przeprowadzano także wymagane okresowe audyty wewnętrzne w zakresie bezpieczeństwa informacji. Dla Starostwa oraz Powiatowego Centrum Wspierania Rodziny w Kamiennej Górze[7] ustalono adekwatne wskaźniki produktu i rezultatu. Wypełniono *Ankiety Dojrzałości Cyberbezpieczeństwa w Jednostkach Samorządu Terytorialnego*[8] i przekazano je do Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego[9] z zachowaniem terminu i formy, określonych w umowie o powierzeniu grantu. W ramach tej umowy Powiat otrzymał dofinansowanie na realizację Projektu w kwocie 850 000,00 zł. w okresie objętym kontrolą wydatki kwalifikowalne poniesione przez grantobiorcę w ramach Projektu, wyniosły 30 520,00 zł i dotyczyły zakupu oprogramowania antywirusowego. Wydatki te zrealizowano zgodnie z wytycznymi dotyczącymi kwalifikowalności wydatków oraz w ramach limitów zatwierdzonych we wniosku o przyznanie grantu. NIK wskazuje, przez prawie rok od otrzymania pełnych środków finansowych nie ogłoszono, do dnia zakończenia czynności kontrolnych, postępowania o zamówienie publiczne obejmującego zakup sprzętu oraz szkoleń przewidzianych we wniosku o przyznaniu grantu.

System Zarządzania Bezpieczeństwem Informacji[10] nie spełniał wymogów § 19 ust. 1 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[11]. Kopie zapasowe danych były przechowywane w niewłaściwym pomieszczeniu. Wbrew regulacjom wewnętrznym nie sporządzano wniosków o odebranie pracownikom uprawnień w systemach informatycznych. Ponadto, w związku z planowanymi w ramach Projektu zakupami, w Starostwie nie zapewniono aktualności „Planu postępowań o udzielenie zamówień na 2025 r.", co było niezgodne z art. 23 ust. 4 ustawy z 11 września 2019 r. – Prawo zamówień publicznych[12].

---

[4] Najwyższa Izba Kontroli formułuje ocenę ogólną jako ocenę pozytywną, ocenę negatywną albo ocenę w formie opisowej.
[5] Dalej: Powiat.
[6] Dalej: Projekt.
[7] Dalej: PCPR.
[8] Dalej: Ankiety.
[9] Dalej: NASK.
[10] Dalej: SZBI.
[11] Dz. U poz. 773; dalej rozporządzenie KRI.
[12] Dz. U. z 2024 r. poz. 1320, ze zm.; dalej PZP.

III. Opis ustalonego stanu faktycznego

OBSZAR **Realizacja przez gminy i powiaty działań w celu zwiększenia poziomu cyberbezpieczeństwa**

Opis stanu faktycznego

1. W okresie objętym kontrolą brak było dokumentów o charakterze strategicznym lub planistycznym Powiatu, jak i Starostwa, w których zostały uwzględnione zagadnienia dotyczące zwiększenia poziomu cyberbezpieczeństwa. Według wyjaśnień Wicestarosty brak opracowania takich dokumentów wynikał z faktu, że nie jest to wymóg prawny.

(akta kontroli: tom I, str. 6; tom II, str. 12)

2. Określenie potrzeb w zakresie zwiększenia poziomu cyberbezpieczeństwa nastąpiło na podstawie bieżącej analizy infrastruktury informatycznej, doświadczenia i praktyk w zakresie bezpieczeństwa oraz audytów bezpieczeństwa informacji przeprowadzonych w Starostwie przez firmę zewnętrzną. Na podstawie powyższych elementów, określenia tych potrzeb dokonał Naczelnik Wydziału Informatyzacji i Ochrony Danych. Dodatkowo w zakresie realizacji Projektu posiłkowano się pomocą firmy doradczej, której zadaniem było m.in. weryfikowanie dokumentacji zamówień publicznych realizowanych w ramach Projektu, udzielanie odpowiedzi na pytania wykonawców w trakcie postępowań, delegowanie eksperta na potrzeby etapu oceny ofert, udzielanie konsultacji na etapie realizacji umowy oraz uczestniczenie w odbiorach dostaw i usług realizowanych w ramach Projektu.

(akta kontroli: tom I, str. 6; tom II, str. 89-115)

3. Starostwo w dniu 2 sierpnia 2024 r. przekazało do NASK wypełnione Ankiety. Dokumenty dotyczące Starostwa i PCPR przesłano za pośrednictwem wskazanej w umowie o powierzeniu grantu skrytki ePUAP należącej do NASK. Ankiety te z powodu błędów były korygowane i ponownie składane w dniach: 29 sierpnia 2024 r.[13] oraz 2 września 2024 r.[14].

(akta kontroli: tom I, str. 437-484; tom II, str. 16)

4. W dniu 4 lipca 2024 r. Powiat podpisał z Centrum Projektów Polska Cyfrowa[15] umowę o powierzeniu grantu o numerze FERC.02.02-CS.01-001/23/1983/FERC.02.02-CS.01-001/23/2024[16]. Przedmiotem umowy było dofinansowanie na realizację Projektu w wysokości 850 000,00 zł, z czego 82% pochodziło ze środków Unii Europejskiej, a 18% ze środków budżetu państwa[17]. Całkowitą kwotę dofinansowania pozyskano 19 września 2024 r., kierując do CPPC w dniu 29 sierpnia 2024 r. wniosek o jednorazową wypłatę dofinansowania[18]. Jako uzasadnienie tego wniosku wskazano na chęć optymalizacji wykorzystania środków finansowych i kompleksowej realizacji zadań Projektu, argumentując, że fragmentaryczne wdrażanie rozwiązań mogłoby ograniczyć ich skuteczność i opóźnić ich natychmiastowe ich

[13] Wysłano obie ankiety.
[14] Wysłano ankietę dotyczącą Starostwa.
[15] Dalej: CPPC.
[16] Dalej: umowa o powierzeniu grantu.
[17] Bez udziału własnego Powiatu. Podatek VAT był kosztem niekwalifikowalnym, ponoszonym przez Powiat.
[18] Zgodnie z możliwością wynikającą z § 2 ust. 8 umowy o powierzeniu grantu.

wykorzystanie. Okres kwalifikowalności wydatków w ramach Projektu rozpoczął się 1 czerwca 2023 r. i zakończy się 30 czerwca 2026 r. Przewidziano także utrzymanie środków trwałych i usług nabytych w ramach Projektu przez okres minimum dwóch lat od jego zakończenia.

Środki pozyskane w ramach tego grantu, według wniosku o jego przyznanie, mają zostać przeznaczone na realizację zadań w następujących obszarach:

- organizacyjnym, na który przeznaczono 19 000,00 zł, na usługi doradcze w celu wsparcia procesu zamówień publicznych, realizowanych w ramach Projektu ,
- kompetencyjnym, na który przeznaczono 77 800,00 zł, na przeprowadzenie Ankiet w Starostwie oraz PCPR, audytu KRI[19] w PCPR, szkolenia podstawowego dla pracowników Starostwa i PCPR podnoszącego świadomość cyberzagrożeń i przedstawiającego sposoby ochrony oraz na szkolenia specjalistyczne kadry informatycznej Starostwa,
- technicznym, na który zaplanowano 753 200,00 zł, na zakup i wdrożenie serwerów z oprogramowaniem CAL[20], rozwiązań Network Access Control[21], macierzy, oprogramowania do kategoryzacji i archiwizacji logów, rozwiązań do utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania, rozwiązań do ochrony przed wyciekiem danych DLP[22], rozbudowę oprogramowania antywirusowego, zakup serwera poczty z mechanizmem uwierzytelniania dwuskładnikowego oraz zakup zasilacza UPS[23].

(akta kontroli: tom I, str. 485-542)

NIK wskazuje, że do dnia 21 sierpnia 2025 r. wykorzystano jedynie 3,59%[24] otrzymanego grantu na Projekt, mimo otrzymania całości środków na konto Starostwa w dniu 20 września 2024 r. Ponadto przez prawie rok od otrzymania pełnych środków finansowych nie ogłoszono, do dnia zakończenia czynności kontrolnych NIK, postępowania o zamówienie publiczne, obejmującego zakup sprzętu oraz szkoleń przewidzianych we wniosku o przyznaniu grantu. Według wyjaśnień Starosty umowa o powierzenie grantu nie określa dokładnej kolejności ani terminu wydatkowania środków, a Projekt trwa do dnia 30 czerwca 2026 r. Starosta wskazał również, że kwota dofinansowania została wypłacona na wniosek Starostwa w całości, aby można było przeprowadzić pełne i kompleksowe zakupy i wdrożenie elementów systemu zwiększających cyberbezpieczeństwo.

---

[19] Audyt sprawdzający spełnianie wymogów określonych w rozporządzeniu KRI.

[20] Oprogramowanie CAL (Client Access License) to licencje dostępowe, które umożliwiają użytkownikom lub urządzeniom korzystanie z usług systemów serwerowych firmy Microsoft.

[21] Systemy bezpieczeństwa, które kontrolują dostęp do sieci, uwierzytelniają urządzenia i użytkowników, a także zapewniają, że spełniają one określone wymagania bezpieczeństwa.

[22] DLP (Data Leak/Leakage/Loss Protection/Prevention) – ogólna nazwa technologii informatycznych wspomagających ochronę danych w postaci elektronicznej przed kradzieżą lub przypadkowymi wyciekami.

[23] zasilacz UPS (uninterruptible power supply) – urządzenie lub system, którego funkcją jest utrzymanie zasilania innych urządzeń elektrycznych lub elektronicznych w przypadku zaniku lub nieprawidłowych parametrów zasilania sieciowego.

[24] Wydatki kwalifikowalne30 520,00 zł z 850 000,00 zł otrzymanego grantu.

Realizowane według stanu na 21 sierpnia 2025 r. działania w ramach przyznanego grantu polegały na:

- zakupie licencji oprogramowania antywirusowego na 100 stanowisk z ważnością do 30 czerwca 2026 r. Oprogramowanie to zostało pozyskane w postępowaniu „Rozbudowa oprogramowania antywirusowego w ramach Projektu Cyberbezpieczny Samorząd realizowanego w ramach Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane technologie cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu bezpieczeństwa". Postępowanie to zostało przeprowadzone zgodnie z wewnętrznymi regulacjami dotyczącymi wydatkowania środków budżetowych poniżej 130 000,00 zł[25]. Zostało one wszczęte w dniu 27 lutego 2025 r., a zakończyło się zawarciem umowy z wykonawcą o wartości 30 520,00 zł netto[26] w dniu 17 marca 2025 r.,
- wyłonieniu firmy doradczej w celu wsparcia procesu zamówień publicznych, realizowanych w ramach Projektu, realizacji i rozliczenia umów zawartych w ramach postępowań o zamówienie publiczne oraz rozliczenia całego Projektu. Wykonawca został wybrany w ramach postępowania „Usługa wsparcia w ramach projektu Cyberbezpieczny Samorząd realizowanego w ramach Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane technologie cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu bezpieczeństwa". Postępowanie to zostało przeprowadzone zgodnie z wewnętrznymi regulacjami dotyczącymi wydatkowania środków budżetowych poniżej 130 000,00 zł. Zostało one wszczęte w dniu 22 lipca 2025 r., a zakończyło się zawarciem umowy z wykonawcą o wartości 15 900 zł netto[27] w dniu 30 lipca 2025 r.,
- przygotowywaniu postępowania o zamówienie publiczne w trybie art. 275 PZP na zakup sprzętu oraz szkoleń przewidzianych we wniosku o przyznanie grantu.

  Postępowanie to zostało ujęte w Planie postępowań o udzielenie zamówień Starostwa dopiero 3 lipca 2025 r., co opisano w sekcji *Stwierdzone nieprawidłowości.*

Zgodnie z § 7 umowy o powierzeniu grantu, w dniu 1 sierpnia 2025 r. Starostwo przekazało do CPPC, za pośrednictwem udostępnionego systemu teleinformatycznego, informację o postępie rzeczowym realizacji Projektu.

(akta kontroli: tom I, str. 379-436, 485-542; tom II, str. 1-8, 12-15, 89-123)

5. W realizacji Projektu przewidziano także udział PCPR. Podstawowym kryterium dołączenia tej jednostki do Projektu była jej lokalizacja w jednym z dwóch budynków wykorzystywanych przez Starostwo oraz chęć podniesienia w tej jednostce świadomości i cyberbezpieczeństwa. Analizę zapotrzebowania

[25] Regulamin wydatkowania środków budżetowych w Starostwie Powiatowym w Kamiennej Górze o wartości 130 000,00 złotych (załącznik nr 1 do Uchwały Nr 175/2021 Zarządu Powiatu Kamiennogórskiego z dnia 13 kwietnia 2021 r.).

[26] 37 539,60 zł brutto.

[27] 19 557,00 zł brutto. Pierwsza płatność wynagrodzenia w wysokości 50% wartości umowy, zgodnie z jej postanowieniami, ma zostać dokonana po zakończeniu postępowania dotyczącego dostaw i usług.

w tym zakresie przeprowadził Naczelnik Wydziału Informatyki i Ochrony Danych Starostwa po konsultacji z ówczesnym Dyrektorem PCPR.

W ramach Projektu dla PCPR zakupiono i przekazano 20 licencji programu antywirusowego oraz zaplanowano przeprowadzenie szkoleń dla pracowników oraz zakup dwóch serwerów NAS[28].

(akta kontroli: tom I, str. 379-436; tom II, str. 13)

6. Do realizacji zadań związanych z realizacją Projektu w Starostwie wyznaczony został Naczelnik Wydziału Informatyki i Ochrony Danych. Wynikało to z wewnętrznych ustaleń i miało odzwierciedlenie w aktualnym zakresie czynności tego pracownika.

(akta kontroli: tom I, str. 6; tom II, str. 9)

7. W trakcie przygotowania i realizacji Projektu w Starostwie nie doszło do fluktuacji kadr zajmujących się tymi zagadnieniami.

(akta kontroli: tom I, str. 6; tom II, str. 9)

8. We wniosku o przyznanie grantu Starostwo sformułowało następujące wskaźniki produktu i rezultaty Projektu:

- 100 pracowników[29] Starostwa oraz jednostek podległych przeszkolonych z zakresu podnoszenia świadomości zagrożeń w obszarze bezpieczeństwa cyfrowego i bezpieczeństwa informacji,
- dwóch administratorów przeszkolonych z zakresu obsługi i wykorzystania funkcjonalności, zakupionych w ramach grantu, nowych rozwiązań i technologii,
- dwa systemy w zakresie dotyczącym zwiększenia bezpieczeństwa informacji, zmniejszenia ryzyka utraty danych oraz zapewnienia ciągłości działania Starostwa i PCPR.

Przyjęte wskaźniki były adekwatne do planowanych działań zapisanych we wniosku o przyznanie grantu oraz były zgodne z załącznikiem nr 9 do Regulaminu Konkursu Grantowego - Opis wskaźników projektu Cyberbezpieczny Samorząd.

Na dzień zakończenia kontroli wskaźniki te nie zostały jeszcze zrealizowane ze względu na nieogłoszenie postępowania w zakresie dotyczącym zakupu sprzętu informatycznego oraz szkoleń dla administratorów i pracowników.

(akta kontroli: tom I, str. 379-436, 485-542; tom II, str. 13)

9. Zakupione w ramach Projektu oprogramowanie antywirusowe w liczbie 100 licencji zostało dostarczone Starostwu 17 marca 2025 r., a w tym samym dniu, 20 z tych licencji przekazano do PCPR.

Do dnia zakończenia czynności kontrolnych NIK nie ogłoszono postępowania o zamówienie publiczne na zakup sprzętu informatycznego, przeprowadzenie szkoleń, audytów oraz sporządzenie dokumentacji SZBI. Trwała natomiast realizacja umowy na usługi doradcze w zakresie dotyczącym wsparcia

---

[28] NAS (Network Attached Storage) – serwer umożliwiający użytkownikom w łatwy sposób przechowywanie, udostępnianie i zarządzanie danymi z dowolnego miejsca w sieci lokalnej lub zdalnej.

[29] 74 kobiety i 26 mężczyzn.

w przygotowaniu i przeprowadzeniu postępowań o zamówienie publiczne, realizowanych w ramach Projektu.

(akta kontroli: tom I, str. 379-436; tom II, str. 89-123)

We wniosku o przyznanie grantu[30] wskazano, że dwa planowane do zakupu serwery zostaną wykorzystane jako serwery aplikacyjne oprogramowania dziedzinowego. Takie wykorzystanie tych urządzeń nie zawiera się jednak w katalogu działań (usług) na jakie można przeznaczyć środki Projektu określonego w § 3 ust. 2 pkt 3 *Regulaminu Konkursu Grantowego pn. Cyberbezpieczny Samorząd.*

Starosta wyjaśniła, że zrezygnowano z instalacji oprogramowania dziedzinowego na planowanych do zakupu serwerach i zadeklarowała, że na dostarczonym sprzęcie zostanie zainstalowane oprogramowanie wzmacniające cyberbezpieczeństwo, dostarczone w ramach Projektu.

(akta kontroli: tom I, str. 485-534; tom II, str. 87, 89)

10. Na dzień zakończenia czynności kontrolnych realizacja Projektu była w Starostwie na etapie przygotowywania zamówienia publicznego na zakup urządzeń, przeprowadzenie szkoleń, audytów oraz opracowanie dokumentacji SZBI. W związku z powyższym przyjęcie i wdrożenie procedur monitorowania utrzymania efektów Projektu, o których mowa w § 13 umowy o powierzenie grantu, nastąpi po wykonaniu wszystkich umów dotyczących dostaw i usług w ramach Projektu.

(akta kontroli: tom II, str. 89)

11. W Starostwie brak było SZBI spełniającego wymogi § 19 ust. 1 rozporządzenia KRI, co opisano w sekcji *Stwierdzone nieprawidłowości*.

W zakresie bezpieczeństwa informacji obowiązywała Polityka Ochrony Danych Osobowych[31], zawierająca Instrukcję zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych[32]. Właścicielem tego dokumentu ustanowiono Starostę, którego, w zakresie wdrożenia, oceny, przeglądu i aktualizacji dokumentacji, wspomagał Inspektor Ochrony Danych. PODO została także właściwie zatwierdzona i przedstawiona pracownikom Starostwa.

PODO zawierała także dodatkowe dokumenty obejmujące procedury:

- zarządzania naruszeniami ochrony danych osobowych,
- zasady wykorzystywania sprzętu prywatnego,
- regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych, mających zapewnić bezpieczeństwo przetwarzania,
- ochrony danych osobowych przy pracy zdalnej.

Dodatkowo Instrukcja zarządzania zasobami informatycznymi zawierała następujące procedury (zasady):

- zarządzania uprawnieniami,

---

[30] Zadanie 3 – W16 – str. 2 wniosku.

[31] Załącznik nr 1 do Zarządzenia Nr 19/2023 Starosty Kamiennogórskiego z 27 czerwca 2023 r.; dalej: PODO.

[32] Dalej: Instrukcja zarządzania zasobami informatycznymi.

- zabezpieczeń dostępu do systemów informatycznych,
- zarządzania sprzętem elektronicznym i oprogramowaniem,
- wykonywania kopii bezpieczeństwa,
- korzystania z poczty elektronicznej,
- korzystania z Internetu,
- zarządzania pojemnością przestrzeni dyskowej,
- bezpiecznego przydzielania przestrzeni dyskowej,
- komunikacji i czynności serwisowych na odległość,
- pracy z urządzeniem mobilnym,
- zabezpieczania sprzętu elektronicznego i systemu informatycznego,
- korzystania z elektronicznych nośników danych,
- wykonywania przeglądów i konserwacji sprzętu elektronicznego i nośników danych,
- utylizacji i serwisu sprzętu elektronicznego.

(akta kontroli: tom I, str. 274-378)

Oględziny tworzenia, przechowywania oraz testowania kopii zapasowych w Starostwie[33] wykazały nieprawidłowe przechowywania kopii zapasowych, co opisano w sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli: tom II, str. 21-22)

Oględziny postępowania z kontami w systemie informatycznym osób, które zakończyły zatrudnienie w Starostwie[34] wykazały brak sporządzania wymaganych wniosków o odebranie uprawnień w systemach informatycznych, co opisano w sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli: tom II, str. 17-18)

12. Dokumentacja składająca się na PODO była na bieżąco aktualizowana i w razie potrzeby doskonalona. Podstawowymi dokumentami w tym zakresie były corocznie prowadzone audyty bezpieczeństwa informacji oraz wykonane analizy ryzyka[35]. W wyniku tak prowadzonych przeglądów w ostatnich dwóch latach zaktualizowano PODO oraz przystąpiono do Projektu w celu poprawienia elementów infrastruktury i opracowania dokumentacji SZBI spełniającej wymogi rozporządzenia KRI.

(akta kontroli: tom II, str. 27, 38-77)

13. W okresie objętym kontrolą w Starostwie przeprowadzono dwa audyty wewnętrzne w zakresie bezpieczeństwa informacji[36], wypełniając tym samym obowiązek wynikający z § 19 ust. 2 pkt 14 rozporządzenia KRI.

Zadania te wykonywała firma zewnętrzna posiadająca niezbędne kompetencje w tym zakresie. Badanie audytowe obejmowało obszary: wymiany informacji w postaci elektronicznej, w tym współpracę z innymi systemami/rejestrami informatycznymi i wspomaganie świadczenia usług drogą elektroniczną; SZBI w systemach teleinformatycznych oraz redukcji ryzyk wynikających z wykorzystania opublikowanych podatności systemów teleinformatycznych.

---

[33] Przeprowadzone 27 czerwca 2025 r.
[34] Przeprowadzone 17 czerwca 2025 r.
[35] Analiza ryzyka z maja 2024 r. nie wykazała potrzeby podejmowania działań w zakresie aktualizacji dokumentacji bezpieczeństwa informacji.
[36] 23 marca 2023 r. i 27 sierpnia 2024 r.

W zakresie dotyczącym SZBI w ostatnim audycie sformułowano 22 rekomendacji, z których 12 zrealizowano, a pozostałe 10 ma zostać zrealizowane w ramach Projektu.

(akta kontroli: tom I, str. 7-273; tom II, str. 27, 78-86)

14. Do dnia zakończenia czynności kontrolnych NIK prowadzone działania informacyjne i promocyjne, w związku z realizacją Projektu przez Starostwo, polegały na:

- oznaczeniu znakiem Unii Europejskiej, barwami Rzeczypospolitej Polskiej i znakiem Funduszy Europejskich plakatów w budynkach oraz informacji na stronie internetowej i w mediach społecznościowych, a także dokumentów związanych z realizacją Projektu, dotyczących postępowań o zamówienia publiczne;
- umieszczeniu trzech plakatów w formacie A3[37] oraz jednego plakat w formacie A4[38] w siedzibach Starostwa;
- umieszczeniu opisu Projektu na stronie internetowej[39] i na profilu w mediach społecznościowych Starostwa[40];
- bieżącym dokumentowaniu działań informacyjnych i promocyjnych, prowadzonych w ramach Projektu.

(akta kontroli: tom II, str. 124)

Stwierdzone nieprawidłowości

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

1. Nie zapewniono aktualności „Planu postępowań o udzielenie zamówień na 2025 r." Starostwa, bowiem do dnia 2 lipca 2025 r. nie ujęto w nim postępowania o zamówienie publiczne, związanego z realizacją Projektu, co było niezgodne z art. 23 ust. 4 PZP.

Zamówienie z obszaru technicznego związane z realizacją tego Projektu, według wniosku o przyznanie grantu było szacowane na 753 200,00 zł. Środki finansowe na ten cel Starostwo otrzymało 20 września 2024 r. i zostały one 25 marca 2025 r. wprowadzone do budżetu Powiatu, co wskazuje, że postępowanie to powinno znaleźć się w Planie postępowań o udzielenie zamówień znacznie wcześniej niż 3 lipca 2025 r.

W złożonych wyjaśnieniach Starosta przyznała, że doszło do tego z powodu przeoczenia pracownika komórki merytorycznej, a 3 lipca 2025 r. zaktualizowano Plan postępowań o udzielenie zamówień, dodając przedmiotowe zamówienie.

(akta kontroli: tom II, str. 23, 25, 29-37)

2. Starostwo nie posiadało SZBI spełniającego wymogi wynikające z § 19 rozporządzenia KRI. Obowiązująca PODO tylko częściowo pełniła rolę SZBI, ponieważ odnosiła się tylko do danych osobowych, nie regulując przy tym

---

[37] Budynek główny przy ul. Broniewskiego na parterze dwa plakaty – drzwi i tablica ogłoszeń oraz budynek przy ul. Sienkiewicza jeden plakat na parterze na tablicy ogłoszeń koło Wydziału Komunikacji.

[38] W budynku przy ul. Sienkiewicza na tablicy ogłoszeń na III piętrze koło Wydziału Geodezji.

[39] https://kamienna-gora.pl/cyberbezpieczny-samorzad.html - dostęp 6 sierpnia 2025 r.

[40] Profil Starostwa na facebook.com – post z 23 października 2024 r.

ochrony innych informacji i aktywów. Ponadto w Starostwie nie ustanowiono polityki bezpieczeństwa informacji, spełniającej warunki opisane w pkt. 5.2 normy ISO/EIC 27001[41], a zgodnie z § 19 ust. 3 rozporządzenia KRI, system SZBI spełnia wymogi tego rozporządzenia, jeżeli został opracowany na podstawie normy ISO/IEC 27001.

Starosta przyznała, że SZBI nie jest w zgodna z wymogami rozporządzenia KRI. Dodała jednocześnie, że w ramach Projektu planowane jest przygotowanie prawidłowej dokumentacji w tym zakresie, uwzględniającej zmiany dokonywane w infrastrukturze informatycznej Starostwa.

(akta kontroli: tom I, str. 274-378; tom II, str. 23-24, 27)

3. W Starostwie nie sporządzano wniosków o odebranie uprawnień w systemach informatycznych, osobom, które zakończyły pracę w Urzędzie, co było niezgodne z art. 20 ust. 2 PODO. Oględziny[42] wykazały brak wniosków o wyrejestrowanie uprawnień dla wszystkich ośmiu sprawdzanych pracowników, którzy zakończyli zatrudnienie po 1 stycznia 2023 r.

Starosta wyjaśniła, że odbieranie uprawnień pracownikom, którzy kończą zatrudnienie, realizowane było na podstawie aktualnej karty rozliczenia pracownika. Przyznała jednak, że praktyka ta nie znalazła odzwierciedlenia w PODO i zadeklarowała, że stosowny zapis zostanie zamieszczony w kolejnej wersji SZBI.

(akta kontroli: tom I, str. 274-378; tom II, str. 17-18, 23, 26)

4. W Starostwie sporządzano kopie zapasowe danych niezgodnie z art. 23 ust. 4 PODO, tj. znajdowały się one w tym samym pomieszczeniu co dane źródłowe. Oględziny[43] wykazały, że kopie zapasowe wykonane automatycznie na zasobach dyskowych (macierzy) znajdowały się w pomieszczeniu serwerowni głównej wraz z podstawowym serwerem produkcyjnym. Natomiast kopie zapasowe wykonywane ręcznie na serwerze NAS zlokalizowanym w serwerowni pomocniczej, były sporządzane z niewystarczającą[44] częstotliwością, przez co nie spełniały one wymogów w zakresie sporządzania i przechowywania kopii zapasowych w innym miejscu niż podstawowy serwer produkcyjny.

Starosta przyznała, że taki stan miał miejsce, informując, że został już uruchomiony skrypt, który automatyzuje proces wykonania kopii zapasowej na serwerze NAS, eliminując problemy związane z częstotliwością ich tworzenia. Pozwala to przechowywać prawidłowo sporządzone kopie w innym pomieszczeniu niż serwer produkcyjny. Przeprowadzone oględziny[45] wykazały, że rozwiązanie to zostało wprowadzone i funkcjonuje poprawnie.

---

[41] Norma ISO/IEC 27001 - Technika informatyczna - Techniki bezpieczeństwa - Systemy zarządzania bezpieczeństwem informacji – Wymagania; dalej: norma ISO/IEC 27001.
[42] Przeprowadzone 17 czerwca 2025 r.
[43] Przeprowadzone 27 czerwca 2025 r.
[44] Kopia sporządzona około miesiąc przed oględzinami, zamiast codzienne/raz w tygodniu.
[45] W dniu 6 sierpnia 2025 r.

(akta kontroli: tom I, str. 274-378; tom II, str. 21-22, 24, 27-28, 124)

IV. Uwagi i wnioski

W związku ze stwierdzonymi nieprawidłowościami, Najwyższa Izba Kontroli, na podstawie art. 53 ust. 1 pkt 5 ustawy o NIK, przedstawia następujące uwagi i wnioski:

Uwagi

Najwyższa Izba Kontroli nie formułuje uwag.

Wnioski

Opracowanie i przyjęcie dokumentacji SZBI, spełniającej wymogi rozporządzenia KRI, dostosowanej do faktycznie realizowanych procesów, w szczególności w zakresie dotyczącym odbierania uprawnień do systemów informatycznych.

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 Delegatury NIK we Wrocławiu. 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 wykorzystania uwag i wykonania wniosków

Zgodnie z art. 62 ustawy o NIK należy poinformować Najwyższą Izbę Kontroli, w terminie 21 dni 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.

Wrocław, 2 września 2025 r.

Kontroler

Cezary Mazik

Główny specjalista kontroli państwowej

/podpisano elektronicznie/

Najwyższa Izba Kontroli

Delegatura we Wrocławiu

p.o. Dyrektor

Radosław Kujawiński

/podpisano elektronicznie/