NAJWYŻSZA IZBA KONTROLI

Delegatura we Wrocławiu

LWR.410.14.2.2025

Pan
Tadeusz Juska
Burmistrz Góry

Urząd Miasta i Gminy w Górze
ul. Adama Mickiewicza 1
56-200 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	Urząd Miasta i Gminy w Górze, ul. Adama Mickiewicza 1, 56-200 Góra[1].
Kierownik jednostki kontrolowanej	Pan Tadeusz Juska, Burmistrz Góry, od 17 lipca 2024 r. W okresie objętym kontrolą funkcję kierownika jednostki poprzednio pełniła: Irena Krzyszkiewicz, od 6 marca 2008 r. do 17 lipca 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/132/2025 z dnia 19 maja 2025 r.

(akta kontroli: tom I, str. 1-7)

[1] Dalej: Urząd.
[2] Tj. do 22 sierpnia 2025 r.
[3] Dz. U. z 2022 r. poz. 623; dalej: ustawa o NIK.

II. Ocena ogólna[4] kontrolowanej działalności

OCENA OGÓLNA

Gmina Góra[5] w okresie objętym kontrolą podejmowała działania w celu zwiększenia poziomu cyberbezpieczeństwa, w tym w ramach realizacji projektu Cyberbezpieczny Samorząd[6].

W Urzędzie dokonano rozpoznania potrzeb w zakresie cyberbezpieczeństwa oraz zapewniono stabilną i kompetentną obsadę kadrową zaangażowaną w nadzór i realizację Projektu. Wypełniono *Ankietę Dojrzałości Cyberbezpieczeństwa w Jednostkach Samorządu Terytorialnego*[7] i przekazano ją do Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego[8] z zachowaniem terminu i formy, określonych w umowie o powierzenie grantu. W ramach tej umowy Gmina otrzymała dofinansowanie na realizację Projektu w kwocie 849 685,72 zł i w okresie objętym kontrolą poniosła wydatki kwalifikowalne z tego tytułu w wysokości 379 652,24 zł. Dotyczyły one dostaw, instalacji oraz konfiguracji sprzętu informatycznego i oprogramowania, a także świadczenia usług doradczych. Stwierdzono jednak, że zakup komponentów serwera w postaci 14 pamięci RAM o wartości 23 800,00 zł[9], nie mieścił się bezpośrednio w katalogu działań (usług) na jakie można przeznaczyć środki Projektu, określonym w § 3 ust. 2 pkt 3 *Regulaminu Konkursu Grantowego pn. Cyberbezpieczny Samorząd*[10]*.* Pozostałe wydatki zrealizowano zgodnie z wytycznymi dotyczącymi kwalifikowalności wydatków.

Urząd posiadał także ustanowiony System Zarządzania Bezpieczeństwem Informacji[11] spełniający wymogi § 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[12]. Przeprowadzano także wymagane okresowe audyty wewnętrzne w zakresie bezpieczeństwa informacji.

Niezależnie od powyższego stwierdzono, że [1] Urząd nie zabezpieczył właściwie interesów zamawiającego w jednym z prowadzonych postępowań o zamówienie publiczne, nie formułując wymogu posiadania przez wykonawców/oferentów dwuletniego doświadczenia w przygotowaniu i przeprowadzeniu szkoleń budujących oraz wzmacniających świadomość cyberzagrożeń, tj. wymogu dla uznania wydatków za kwalifikowalne wynikającego z § 4 pkt. 7 ppkt d Regulaminu Projektu; [2] brak było adekwatnych zabezpieczeń pomieszczenia serwerowni Urzędu, co stwarzało potencjalne zagrożenie włamania i narażenia na zniszczenie lub nieuprawniony dostęp do aktywów informacyjnych i było niezgodne z § 19 ust. 2 pkt 9

---

[4] Najwyższa Izba Kontroli formułuje ocenę ogólną jako ocenę pozytywną, ocenę negatywną albo ocenę w formie opisowej.
[5] Dalej: Gmina.
[6] Dalej: Projekt.
[7] Dalej: Ankieta.
[8] Dalej: NASK.
[9] Ogółem wydatkowano 29 274,00 zł (w tym 5 474,00 zł wydatków niekwalifikowalnych Projektu - podatek VAT).
[10] Dalej: Regulamin Projektu.
[11] Dalej: SZBI.
[12] Dz. U poz. 773; dalej rozporządzenie KRI.

rozporządzenia KRI; [3] nie odebrano uprawnień do systemów informatycznych osobom, które zakończyły pracę w Urzędzie, co było niezgodne z § 19 ust. 2 pkt 5 rozporządzenia KRI oraz [4] tworzono kopie zapasowe danych w sposób niezgodny z wewnętrznymi procedurami.

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 Gminy, jak i Urzędu, w których zostały uwzględnione zagadnienia dotyczące zwiększenia poziomu cyberbezpieczeństwa. Według wyjaśnień Sekretarza Miasta i Gminy brak opracowania takich dokumentów wynikał z faktu, że nie jest to wymóg prawny, co nie oznacza jednak według niego, że w działalności samorządu Gminy sprawy cyberbezpieczeństwa były marginalizowane.

(akta kontroli: tom I, str. 11-12)

2. Wskazówką dla określenia potrzeb w zakresie zwiększenia poziomu cyberbezpieczeństwa w Urzędzie były wyniki audytu bezpieczeństwa informatycznego przeprowadzonego w maju 2022 r. przez firmę zewnętrzną w ramach grantu Cyfrowa Gmina. Natomiast konkretne potrzeby i działania w tym zakresie zostały określone przez Urząd przy wsparciu zewnętrznej firmy doradczej, która pomagała w ich analizie i rekomendowaniu odpowiednich do nich technologii, usług oraz systemów, a także miała za zadanie wspierać go w zakresie realizacji Projektu.

(akta kontroli: tom I, str. 14, 143-237, 375-417)

3. Urząd przekazał do NASK wypełnioną Ankietę. Dokument ten przesłano 8 sierpnia 2024 r. za pośrednictwem, wskazanej w umowie udostępnienia grantu, skrytki ePUAP należącej do NASK.

(akta kontroli: tom I, str. 233-245)

4. W dniu 17 lipca 2024 r. Gmina podpisała z Centrum Projektów Polska Cyfrowa[13] umowę o powierzeniu grantu o numerze FERC.02.02-CS.01-001/23/2182/FERC.02.02-CS.01-001/23/2024[14]. Przedmiotem umowy było dofinansowanie na realizację Projektu w wysokości 849 685,72 zł, z czego 82% pochodziło ze środków Unii Europejskiej, a 18% ze środków budżetu państwa[15]. Pierwszą transzę grantu w wysokości 254 905,72 zł pozyskano w dniu 30 sierpnia 2024 r. Następnie, celem przyspieszenia realizacji Projektu, Gmina wystąpiła 11 września 2024 r. o wypłatę całości dofinansowania. Wniosek ten został pozytywnie rozpatrzony i w dniu 25 października 2024 r. wpłynęła kwota 594 780,00 zł, zgodnie z możliwością wynikającą z § 2 ust. 8 umowy o powierzeniu grantu. Okres kwalifikowalności wydatków w ramach Projektu rozpoczął się 1 czerwca 2023 r. i zakończy się 30 czerwca 2026 r. Przewidziano

[13] Dalej: CPPC.
[14] Dalej: umowa o powierzeniu grantu.
[15] Bez udziału własnego Gminy. Urząd w trakcie realizacji Projektu dokonał korekty oświadczenia VAT, w którym wskazał, że podatek ten stanowi koszty niekwalifikowalne tego Projektu.

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 zaplanowano 113 768,72 zł, na usługi przygotowania Projektu oraz usługi wspierające jego realizację, audyt zgodności z KRI[16], audyt zgodności z ustawą z 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa[17], audyt systemu bezpieczeństwa informacji oraz opracowanie i wdrożenie dokumentacji SZBI,
- kompetencyjnym, na który przeznaczono 79 124,20 zł, na przeprowadzenie szkoleń z cyberbezpieczeństwa dla kadry administracyjnej i kadry informatycznej, szkoleń specjalistycznych z cyberbezpieczeństwa dla kadry zarządzającej oraz szkoleń specjalistycznych dla informatyków z wybranych rozwiązań technicznych,
- technicznym, na który przeznaczono 656 792,80 zł, na zakup: serwera do połączenia w klaster z istniejącym serwerem, komponentów serwera w celu rozbudowy istniejącego klastra serwerów, rozwiązań Network Access Control[18], dysków twardych do macierzy dyskowej, zasilaczy UPS[19], urządzeń UTM[20], zarządzanych urządzeń sieciowych, oprogramowania do zarządzania i aktualizacji systemów operacyjnych i oprogramowania na stacjach roboczych, serwerach, urządzeniach sieciowych, oprogramowania do zarządzania podatnościami, wdrożenia systemów teleinformatycznych, wykonania audytów bezpieczeństwa i szkoleń powiązanych z testami socjotechnicznymi.

(akta kontroli: tom I, str. 20-74, 418-453; tom II, str. 3-4, 9-10)

Do dnia 22 sierpnia 2025 r. poniesiono wydatki kwalifikowalne w wysokości 379 652,24 zł[21], co stanowiło 44,68% otrzymanego grantu na ten cel[22]. Według wyjaśnień złożonych przez Sekretarza Miasta i Gminy, wcześniejsze wpłynięcie całości dofinansowania pozwoliło na podjęcie efektywnych działań prowadzących do organizacji dużego zamówienia publicznego, które przygotowano pod koniec 2024 r., a zakończono 14 marca 2025 r. podpisaniem umowy o wartości 725 204,26 zł. Podkreślił również, że umowa ta jest obecnie realizowana i została częściowo opłacona w zakresie dostarczonego sprzętu informatycznego oraz oprogramowania.

---

[16] Audyt sprawdzający spełnianie wymogów określonych w rozporządzenia KRI.

[17] Dz. U z 2024 r., poz. 1077, ze zm.

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

[19] 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.

[20] UTM (Unified Threat Management) - zintegrowane rozwiązanie do zarządzania zagrożeniami, które umożliwia ochronę sieci.

[21] Ogółem wydatkowano 466 972,26 zł, z czego 87 320,02 zł stanowiły wydatki niekwalifikowalne Projektu (podatek VAT) .

[22] 379 652,24 zł z 849 685,72 zł.

Realizowane według stanu na 22 sierpnia 2025 r. działania w ramach przyznanego grantu polegały na:

a) świadczeniu usług doradczych, w zakresie rozeznania potrzeb, wsparcia w przygotowaniu, realizacji i zarządzaniu Projektem. Wykonawca został wybrany w wyniku rozstrzygnięcia postępowania >>Usługa doradcza w ramach programu „Cyberbezpieczny Samorząd"<<. Zostało ono przeprowadzone zgodnie z wewnętrznymi regulacjami dotyczącymi wydatkowania środków budżetowych poniżej 130 000,00 zł[23]. Postępowanie to wszczęto 23 sierpnia 2023 r., a zakończyło się zawarciem umowy z wykonawcą o wartości 39 430,89 zł netto[24] w dniu 22 września 2023 r. Urząd poniósł dotąd wydatki kwalifikowalne z tytułu realizacji tej umowy w wysokości 24 390,24 zł[25],
b) dostawie i częściowym wdrożeniu sprzętu informatycznego oraz oprogramowania, a także prowadzeniu szkoleń, opracowywaniu dokumentacji SZBI i przeprowadzeniu testów penetracyjnych. Wykonawca został wybrany w wyniku rozstrzygnięcia postępowania o zamówienie publiczne „Dostawy i usługi służące poprawie cyberbezpieczeństwa w Urzędzie Miasta i Gminy w Górze". Postępowanie to zostało przeprowadzone w trybie w trybie art. 275 ust. 1 ustawy z 11 września 2019 r. – Prawo zamówień publicznych[26], zgodnie z obowiązującymi przepisami PZP. Postępowanie to wszczęto 30 stycznia 2025 r., a zakończyło się zawarciem umowy z wykonawcą o wartości 604 762,00 zł netto[27] w dniu 14 marca 2025 r. Dotąd zrealizowano dostawę sprzętu informatycznego i oprogramowania, a wydatki kwalifikowalne z tego tytułu wyniosły 355 262,00 zł[28]. Trwały ponadto szkolenia[29] oraz opracowywano dokumentację SZBI.

   W postępowaniu tym, w specyfikacji warunków zamówienia[30] i umowie nie wskazano wymagania posiadania dwuletniego doświadczenia w przygotowaniu i przeprowadzeniu szkoleń budujących oraz

---

[23] Regulamin udzielania zamówień publicznych przez Urząd Miasta i Gminy w Górze, których wartość jednostkowa nie przekracza wyrażonej w złotych równowartości 130 000,00 złotych (Załącznik nr 1 do zarządzenia nr 3/2021 Burmistrza Góry z dnia 15 stycznia 2021 r.)

[24] 48 500,00 zł brutto.

[25] Wydatkowano łącznie 30 000,00 zł, z czego 5 609,76 zł stanowiły wydatki niekwalifikowalne Projektu (podatek VAT).

[26] Dz. U z 2024 r. poz.1320, ze zm.; dalej: PZP.

[27] 725 204,26 zł brutto.

[28] Wydatkowano łącznie 436 972,26 zł, z czego 81 710,26 zł stanowiły wydatki niekwalifikowalne Projektu. Dostarczono: macierz dyskową, serwer, komponenty serwera w postaci 14 pamięci RAM (DDR4) oraz 24 dysków twardych SSD, switch, serwer plików NAS, 24 dyski twarde do serwera plików NAS, dwa urządzenia UTM, kontroler Wifi, punkt dostępowy Wifi, dwa urządzenia UPS, dwie licencje na oprogramowanie serwerowe, oprogramowanie do zarządzania i aktualizacji systemów operacyjnych na stacjach roboczych, serwerach, urządzeniach sieciowych oraz monitorowania infrastruktury informatycznej.

[29] Szkolenia dla pracowników IT z zakresu obsługi nabywanego sprzętu i oprogramowania; szkolenie dla pracowników administracyjnych w zakresie cyberbezpieczeństwa, szkolenia powiązane z testami socjotechnicznymi, szkolenia dla pracowników IT w zakresie cyberbezpieczeństwa, szkolenia specjalistyczne dla informatyków obejmujące szkolenie z zakresu Active Directory, wirtualizacji, bezpieczeństwa kopii zapasowych, systemu SIEM, zarządzania urządzeniami na styku sieci firmowej z Internetem oraz wiedzy o atakach hackerskich i zapobieganiu im.

[30] Dalej: SWZ.

wzmacniających świadomość cyberzagrożeń, co było działaniem nierzetelnym i co opisano w sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli: tom I, str. 246-453; tom II, str. 3-4, 9-10)

Zgodnie z § 7 umowy o powierzeniu grantu, w dniu 11 sierpnia 2025 r. Urząd przekazał do CPPC, za pośrednictwem udostępnionego systemu teleinformatycznego, informację o postępie rzeczowym realizacji Projektu.

(akta kontroli: tom II, str. 113-114)

5. Urząd realizując Projekt nie przewidział udziału podlegających mu jednostek organizacyjnych w realizacji grantu. Według wyjaśnień Sekretarza Miasta i Gminy rozważano włączenie w realizację Projektu gminnych jednostek organizacyjnych, lecz wysokość środków finansowych będących do dyspozycji w jego ramach nie zapewniała zaspokojenia w pełni potrzeb Urzędu w tym zakresie, w związku z czym zrezygnowano z włączenia do Projektu innych jednostek.

(akta kontroli: tom I, str. 20-74; tom II, str. 71)

6. Za realizację Projektu odpowiedzialni byli Sekretarz Miasta i Gminy oraz Informatyk Urzędu. Wynikało to z wewnętrznych ustaleń i miało odzwierciedlenie w aktualnym regulaminie organizacyjnym Urzędu oraz zakresach czynności pracowników. Osoby te we współpracy z firmą doradczą ,odpowiadały także za opracowanie wniosku będącego podstawą realizacji całego Projektu.

(akta kontroli: tom I, str. 17; tom II str. 82)

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

(akta kontroli: tom II, str. 82)

8. We wniosku o przyznanie grantu Urząd sformułował następujące wskaźniki produktu i rezultaty Projektu:

- przeszkolenie z zakresu podniesienia świadomości zagrożeń w obszarze bezpieczeństwa cyfrowego i bezpieczeństwa informacji pracowników administracyjnych oraz kadry zarządzającej,
- przeszkolenie kadry informatycznej z zakresu cyberbezpieczeństwa oraz obsługi i wykorzystania funkcjonalności zakupionych w ramach grantu nowych rozwiązań i technologii,
- zwiększenie bezpieczeństwa informacji, zmniejszenie ryzyka utraty danych oraz zapewnienie ciągłości działania Urzędu.

Przyjęte wskaźniki i rezultaty Projektu są co prawda adekwatne do planowanych działań zapisanych we wniosku o przyznanie grantu, ale nie zostały zwymiarowane zgodnie z wymogami dokumentu „Opis wskaźników projektu Cyberbezpieczny Samorząd”[31], ponieważ nie zawierają wartości liczbowych opisujących ilość osób przeszkolonych i systemów, w których zwiększono bezpieczeństwo.

[31] Załącznik nr 9 do Regulaminu Konkursu Grantowego.

Sekretarz Miasta i Gminy w złożonych wyjaśnieniach wskazał, że wniosek został zaakceptowany i dopuszczony do realizacji, a rzeczywiste wskaźniki zostaną przedstawione przez Gminę na etapie rozliczenia Projektu.

Natomiast CPPC wskazało, że do udziału w grancie Jednostki Samorządu Terytorialnego nie konkurowały ze sobą wysokością zadeklarowanych wskaźników, więc uznano, że nie ma potrzeby ich oceny w ramach kryteriów formalno-merytorycznych.

(akta kontroli: tom I, str. 20-74; tom II str. 1, 4, 117-119)

9. W ramach realizacji Projektu przez Urząd, do dnia 11 sierpnia 2025 r. pozyskano i zainstalowano/uruchomiono:

- macierz dyskową – jedną sztukę,
- serwer – jedną sztukę,
- komponent serwera – pamięć RAM (DDR4) – 14 sztuk,
- komponent serwera – dyski twarde SSD – 24 sztuki,
- serwer plików NAS – dwie sztuki,
- dyski twarde do macierzy dyskowej – 24 sztuki,
- UPS – jedną sztukę,
- oprogramowanie serwerowe i do zarządzania – trzy elementy,

ponadto pozyskano i w trakcie instalacji/uruchamiania pozostawały:

- switch – jedna sztuka,
- urządzenia sieciowe – trzy sztuki,
- UPS – jedna sztuka,
- urządzenia UTM – dwie sztuki[32].

Zakupienie komponentów serwera w postaci pamięci RAM nie mieściło się jednak bezpośrednio w katalogu działań (usług) na jakie można przeznaczyć środki Projektu, co opisano w sekcji *Stwierdzone nieprawidłowości*.

Ponadto w ramach realizacji umowy zawartej 14 marca 2025 r. przeprowadzono dwa szkolenia: z cyberbezpieczeństwa dla kadry zarządzającej oraz dla informatyków w zakresie Active Directory, wirtualizacji i tworzenia kopii zapasowych[33]. Według wyjaśnień Sekretarza Miasta i Gminy pozostałe szkolenia planowane są do odbycia w miesiącu wrześniu 2025 r. Przygotowany został także projekt zarządzenia Burmistrza wprowadzający SZBI, który ma wejść w życie z dniem 1 września 2025 r.

Natomiast realizacja usług doradczych na podstawie zawartej umowy współpracy z 22 września 2023 r. polegała na określeniu potrzeb Urzędu w zakresie Projektu, przedstawieniu wstępnego kosztorysu Projektu i jego modyfikacji, wsparciu w sporządzeniu wniosku o przyznanie grantu oraz wniosku o przyspieszenie płatności grantu, wsparciu przy wypełnieniu Ankiety oraz opracowaniu merytorycznej dokumentacji do prowadzonych postępowań o zamówienie publiczne w ramach Projektu.

---

[32] W ramach realizacji umowy z wykonawcą z 14 marca 2025 r. na dostawę sprzętu informatycznego, oprogramowania, wdrożenia, przeprowadzenia szkoleń oraz opracowania i wdrożenia dokumentacji SZBI o wartości 725 204.26 zł brutto, za które zapłacono 436 972,26 zł (faktura nr 0039/05/POZ/25 z 13 maja 2025 r.).

[33] Zgodnie z umową z wykonawcą faktura za te szkolenia zostanie wystawiona po przeprowadzeniu kompletu szkoleń.

(akta kontroli: tom I, str. 418-453; tom II, str. 3-4, 71-100)

10. Na dzień zakończenia czynności kontrolnych realizacja Projektu była na etapie przeprowadzania szkoleń i opracowania dokumentacji SZBI oraz przygotowywania postępowań na przeprowadzenie audytów.

Pomimo tego, 11 lipca 2025 r. przyjęto procedury monitorowania utrzymania efektów Projektu[34], które wprowadzały Kartę monitorowania utrzymywania efektów i trwałości Projektu. Na dokumencie tym dokonywana będzie ocena wskaźnikowa, porównująca wartość wskaźników wg wniosku o dofinansowanie ze stanem na chwilę oceny, odnotowywane będą problemy w utrzymaniu trwałości Projektu oraz przebieg monitoringu trwałości Projektu. Monitorowanie trwałości Projektu ma się obywać raz w roku w I kwartale, począwszy od 2027 r.

(akta kontroli: tom II, str. 86, 101-106)

11. W Urzędzie opracowano i wdrożono SZBI, którego podstawowym elementem była Polityka Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta i Gminy w Górze[35], przyjęta Zarządzeniem nr 4/22 Burmistrza Góry z dnia 8 lutego 2022 r.[36]. Została ona właściwie przedstawiona i zakomunikowana pracownikom, którzy potwierdzali zapoznanie się z jej postanowieniami, składając pisemne oświadczenia w tym zakresie.

Zgodnie z postanowieniami PZBI, odpowiadającym za jej opracowanie, nadzór nad stosowaniem, przegląd i modyfikację był Inspektor Ochrony Danych, a osobami odpowiadającymi za jej wdrożenie i nadzór nad przestrzeganiem przez pracowników byli naczelnicy wydziałów.

Częścią składową PZBI, zatwierdzoną i zakomunikowaną pracownikom urzędu odpowiedzialnym za realizację określonych zadań, była Instrukcja zarządzania systemem informatycznym, zawierająca następujące procedury:

- nadawania uprawnień do przetwarzania danych,
- rozpoczęcia, zawieszenia i zakończenia pracy dla użytkowników systemu,
- tworzenia kopii zapasowych i archiwalnych,
- wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych,
- szacowania ryzyka w zakresie bezpieczeństwa informacji,
- bezpieczeństwa informacji w pracy zdalnej,
- zarządzania incydentami bezpieczeństwa informacji,
- zarządzania oprogramowaniem.

Ponadto w Urzędzie funkcjonowała procedura nadawania i odbierania uprawnień do systemów informatycznych pracownikom, stanowiąca załącznik nr 1 i 2 do Regulaminu Pracy Urzędu Miasta i Gminy z dnia 5 czerwca 2025 r.[37]

(akta kontroli: tom I, str. 454-534; tom II, str. 72-73, 75-81)

---

[34] Zarządzenie Nr 22/25 Burmistrza Góry z dnia 18 lipca 2025 r. w sprawie procedury monitorowania utrzymania efektów projektu pn. „Cyberbezpieczny Samorząd dla Gminy Góra".
[35] Dalej: PZBI.
[36] Zmieniona zarządzeniem nr 24/22 Burmistrza Góry z dnia 25 października 2022 r.
[37] Wprowadzonego zarządzeniem nr 15/25 Burmistrza Góry z 5 czerwca 2025 r.

Serwerownia Urzędu zlokalizowana była w odrębnym, nieoznaczonym i klimatyzowanym pomieszczeniu, do którego dostęp mieli informatycy. Posiadała ona wydzieloną instalację elektryczną i nie przechowywano w niej materiałów zagrażających infrastrukturze IT. Niemniej, pomieszczenie to nie posiadało adekwatnych zabezpieczeń, o czym szerzej w sekcji *Stwierdzone nieprawidłowości.*

(akta kontroli: tom II, str. 64-65)

Oględziny postępowania z kontami pracowników w systemie informatycznym, którzy zakończyli pracę w Urzędzie[38] wykazały, że wszyscy trzej badani pracownicy, z którymi rozwiązano umowy o pracę po 1 stycznia 2025 r. nadal posiadali aktywne konta użytkowników, co opisano w sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli: tom II, str. 66-68)

Oględziny tworzenia, przechowywania oraz testowania kopii zapasowych w Urzędzie[39] wykazały sporządzanie kopii zapasowych niezgodnie z PZBI, co opisano w sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli: tom II, str. 66-68)

12. Dokumentacja składająca się na SZBI co roku była przedmiotem audytu wewnętrznego i analizy osób odpowiedzialnych w Urzędzie za bezpieczeństwo informacji. Podstawowym dokumentem z prowadzenia tych działań były coroczne audyty bezpieczeństwa informacji oraz analiza ryzyka[40]. Ich efektem była weryfikacja i aktualizacja PZBI w 2022 r. oraz uwzględnienie w 2024 r. konieczności opracowania nowego dokumentu SZBI w ramach realizowanego Projektu.

(akta kontroli: tom II, str. 7-8, 72)

13. W okresie objętym kontrolą w Urzędzie przeprowadzono dwa[41] audyty wewnętrzne w zakresie bezpieczeństwa informacji, wypełniając tym samym obowiązek wynikający z § 19 ust. 2 pkt 14 rozporządzenia KRI.

Zadania te wykonywał Audytor Wewnętrzny Urzędu posiadający niezbędne kompetencje w tym zakresie. Badanie audytowe obejmowało stopień spełnienia wymogów rozporządzenia KRI w zakresie bezpieczeństwa informacji. W ostatnim audycie sformułowano sześć rekomendacji, z których cztery zrealizowano, a dwie są w trakcie realizacji, w tym jedna w ramach Projektu[42].

Dodatkowo zgodnie z obowiązującym PZBI, obszar ten raz na pięć lat był objęty audytem wykonanym przez firmę zewnętrzną. Ostatni taki audyt miał miejsce w maju 2022 r.

(akta kontroli: tom I, str. 143-232, 535-546; tom II, str. 6-7)

---

[38] Przeprowadzony w okresie od 15 grudnia 2023 r. do 19 stycznia 2024 r. (za 2023 r.).
[39] Przeprowadzony w okresie od 23 grudnia 2024 r. do 24 stycznia 2025 r. (za 2024 r.).
[40] Analiza ryzyka z 8 stycznia 2025 r. nie wykazała potrzeby podejmowania działań w zakresie aktualizacji dokumentacji bezpieczeństwa informacji.
[41] 23 marca 2023 r. i 28 czerwca 2024 r.
[42] Szkolenia kadry zarządzającej oraz pracowników zwiększające poziom świadomości w zakresie cyberbezpieczeństwa i bezpieczeństwa informacji.

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

- oznaczeniu znakiem Unii Europejskiej, barwami Rzeczypospolitej Polskiej i znakiem Funduszy Europejskich: prowadzonych działań informacyjnych i promocyjnych (plakaty oraz informacje na stronie internetowej, mediach społecznościowych i naklejkach na sprzęcie) oraz dokumentów związanych z realizacją Projektu, podawanych do wiadomości publicznej (dotyczących zamówień publicznych);
- umieszczeniu plakatu w formacie A3 na tablicy ogłoszeń, na parterze budynku Urzędu,
- umieszczeniu opisu Projektu na stronie internetowej Urzędu[43] oraz w mediach społecznościowych,
- umieszczeniu oznaczenia na zainstalowanym sprzęcie informatycznym, zakupionym w ramach Projektu,
- bieżącym dokumentowaniu działań informacyjnych i promocyjnych, prowadzonych w ramach Projektu.

(akta kontroli: tom II, str. 115-116)

Stwierdzone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie stwierdzono następującą nieprawidłowość:

1. Urząd w postępowaniu „Dostawy i usługi służące poprawie cyberbezpieczeństwa w Urzędzie Miasta i Gminy w Górze”[44] nie zabezpieczył właściwie interesów zamawiającego, co było działaniem nierzetelnym. W SWZ i umowie nie wskazano bowiem wymagania posiadania przez wykonawcę dwuletniego doświadczenia w przygotowaniu i przeprowadzeniu szkoleń budujących oraz wzmacniających świadomość cyberzagrożeń, tj. wymogu dla uznania wydatków za kwalifikowalne wynikającego z § 4 pkt 7 ppkt d Regulaminu Projektu.

Sekretarz Miasta i Gminy wyjaśnił, że poinformowano wykonawców o realizacji tego zadania w ramach Projektu, a wykonawcy to podmioty profesjonalnie działające na rynku, z należytą starannością, przy określeniu której uwzględnia się zawodowy charakter tej działalności. W jego opinii chroni to interes prawny Gminy oraz gwarantuje wybór wykonawców dających rękojmię należytego wykonania umowy. Przedstawił także pozyskane dokumenty potwierdzające spełnianie przez wykonawców wymogów w zakresie doświadczenia i kwalifikacji wymaganych do uznania wydatków za kwalifikowalne w tym Projekcie.

NIK wskazuje, że przywoływane zasady kwalifikowalności wydatków Projektu są skierowane do zamawiającego, a nie do wykonawcy. Nie stanowią więc dla niego punktu odniesienia do deklarowania posiadania uprawnień lub kompetencji wynikających z odrębnych przepisów. W przypadku braku wymaganego doświadczenia umowy o zamówienie publiczne mogłyby być

[43] https://gora.com.pl/cyberbezpieczny-samorzad-dla-gminy-gora.html.
[44] Postępowanie BZP.271.5.2025.

wprawdzie wykonane właściwie i z należytą starannością przez wykonawców, lecz ich koszt stanowiłby wydatek niekwalifikowalny Projektu i w całości obciążałby Gminę. Zatem ustanowienie takiego wymogu leżało w interesie Gminy by maksymalnie wykorzystać środki zewnętrzne otrzymane na realizację Projektu i nie angażować własnych.

(akta kontroli: tom I, str. 246-453; tom II, str. 1-2, 5-6, 11-35)

2. Zakupienie komponentów serwera w postaci 14 pamięci RAM o wartości 23 800,00 zł[45], nie mieściło się bezpośrednio w katalogu działań (usług) na jakie można przeznaczyć środki Projektu, określonego w § 3 ust. 2 pkt 3 Regulaminu Projektu. Zakup ten ponadto nie był ujęty we wniosku o przyznanie grantu.

Według wyjaśnień Sekretarza Miasta i Gminy komponenty te zostały zakupione w związku z kończącym się wsparciem dla systemów MS SQL Serwer 2016 oraz Windows Server 2016, a nowe wersje tych systemów wymagają większej pojemności RAM.

NIK nie kwestionuje potrzeby dokonania tego zakupu, ale wskazuje, że systemy te służą zarządzaniu relacyjnymi bazami danych oraz zarządzaniu serwerami i infrastrukturą IT, mają więc charakter dziedzinowy i tym samym nie podnoszą bezpośrednio cyberbezpieczeństwa organizacji. Z tych powodów wydatek taki nie spełnia warunków Projektu i w związku z tym jest wydatkiem niekwalifikowalnym, który nie podlega rozliczeniu.

(akta kontroli: tom I, str. 246-417; tom II, str. 69, 71, 83, 86-87)

3. W pomieszczeniu serwerowni Urzędu brak było adekwatnych zabezpieczeń[46], co stwarzało potencjalne zagrożenie włamania i narażenia na zniszczenie lub nieuprawniony dostęp do aktywów informacyjnych i było niezgodne z § 19 ust. 2 pkt 9 rozporządzenia KRI.

Sekretarz Miasta i Gminy wyjaśnił, że usytuowanie serwerowni i sposoby jej dozoru zmniejszają ryzyko włamania i zniszczenia aktywów informacyjnych.

Należy podkreślić, że wskazane przez Sekretarza Miasta i Gminy zabezpieczenia nie eliminują jednak ryzyka włamania lub narażenia na zniszczenie aktywów informacyjnych do tego pomieszczenia.

(akta kontroli: tom II, str. 64-65, 69, 71-72)

4. Badanie[47] wykazało, że wszystkie trzy osoby, które zakończyły zatrudnienie w Urzędzie po 1 stycznia 2025 r. nadal miały aktywne konta użytkowników w domenie Active Directory, umożliwiające jednocześnie logowanie (i dostęp) do innych systemów dziedzinowych Urzędu. Było to niezgodne z § 19 ust. 2 pkt 5 rozporządzenia KRI.

[45] Ogółem wydatkowano 29 274,00 zł, z czego 5 474,00 zł stanowiły wydatki niekwalifikowalne Projektu (podatek VAT).

[46] O szczegółach Burmistrz został powiadomiony pismem LWR.410.14.2.2025 z 2 lipca 2025 r. (w pkt 3).

[47] Przeprowadzone w dniu 1 lipca 2025 r.

Sekretarz Miasta i Gminy wyjaśnił, że sytuacja ta miała miejsce z powodu nieuwagi informatyków, a konta tych osób nie były używane i zostały zablokowane w trakcie przeprowadzenia oględzin.

(akta kontroli: tom II, str. 66-70, 72)

5. W Urzędzie nie sporządzano kopii zapasowych w chmurze obliczeniowej, co było niezgodne z § 4 i § 9 Procedury tworzenia kopii zapasowych w Urzędzie Miasta i Gminy w Górze[48].

W złożonych wyjaśnieniach Sekretarz Miasta i Gminy przyznał, że w ramach projektu Cyfrowa Gmina przymierzano się do zakupu usług chmurowych i dlatego zapis ten umieszczono w PZBI. Po dokładnej analizie do tego zakupu jednak nie doszło, a dotychczasowa procedura zostanie zastąpiona przez inne skuteczne i bezpieczne rozwiązanie.

(akta kontroli: tom II, str. 66-68, 70, 73-74)

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

1. Poinformowanie Operatora (NASK) o poniesieniu w ramach Projektu wydatku niekwalifikowalnego w kwocie 23 800,00 zł na zakup 14 pamięci RAM oraz poinformowanie NIK o decyzji NASK w tej sprawie.

2. Opracowanie i przyjęcie dokumentacji SZBI dostosowanej do faktycznie realizowanych procesów, w szczególności w zakresie obejmującym sporządzanie kopii zapasowych.

3. Zapewnienie wymaganych zabezpieczeń w pomieszczeniu serwerowni.

[48] Załącznik nr 14 do PZBI.

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/