NAJWYŻSZA IZBA KONTROLI

Delegatura w Kielcach

LKI.410.6.1.2025

Pan Paweł Wójcik
Burmistrz
Miasta i Gminy Chmielnik
Plac Kościuszki 7
26-020 Chmielnik

WYSTĄPIENIE POKONTROLNE

P/25/003 – Realizacja projektu Cyberbezpieczny Samorząd

NAJWYŻSZA IZBA KONTROLI
Delegatura w Kielcach
ul. gen. T. Kościuszki 6, 25-310 Kielce
tel. 48412499100, lki@nik.gov.pl

I. Dane identyfikacyjne

Jednostka kontrolowana	Urząd Miasta i Gminy w Chmielniku,26-020 Chmielnik, Plac Kościuszki 7 (dalej także: Urząd lub UMiG)
Kierownik jednostki kontrolowanej	Paweł Wójcik, Burmistrz Miasta i Gminy Chmielnik (dalej także: Burmistrz), od 10 grudnia 2014 r. do dnia zakończenia niniejszej kontroli.
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.
Podstawa prawna podjęcia kontroli	Art. 2 ust. 2 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli[1]
Jednostka przeprowadzająca kontrolę	Najwyższa Izba Kontroli Delegatura w Kielcach
Kontroler	Tadeusz Mikołajewicz, doradca prawny, upoważnienie do kontroli nr LKI/51/2025 z 05.05.2025 r.

(akta kontroli str. 1-2; 3-5)

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

II. Ocena ogólna[2] kontrolowanej działalności

OCENA OGÓLNA

W okresie objętym kontrolą Gmina nie posiadała dokumentów strategicznych, które uwzględniały zagadnienia dotyczące zwiększenia poziomu cyberbezpieczeństwa. Działania mające zmienić ten stan, zostały podjęte w związku z pracami nad nową „Strategią Rozwoju Miasta i Gminy Chmielnik do 2030 r." Rozpoznawanie potrzeb w zakresie zwiększenia poziomu bezpieczeństwa informatycznego podjęto w Urzędzie w 2023 r. w związku z planowanym udziałem w projekcie „Cyberbezpieczny Samorząd" (dalej także: Projekt) poprzez ustalenie potrzeb zakupu usług i sprzętu, w celu podniesienia bezpieczeństwa cyfrowego jednostek organizacyjnych. W ramach realizacji umowy o powierzenie grantu (dalej także: Umowa), podpisanej w dniu 2 lipca 2024 r. ze Skarbem Państwa, w imieniu którego działało Centrum Projektów Polska Cyfrowa (dalej: CPPC), Urząd przekazał Ankietę Dojrzałości Cyberbezpieczeństwa w jednostkach Samorządu Terytorialnego (dalej także: Ankieta lub Ankieta Dojrzałości) na skrzynkę ePUAP do Naukowej i Akademickiej Sieci Komputerowej – Państwowy Instytut Badawczy (dalej także: NASK). Nastąpiło to z zachowaniem określonego w Umowie terminu. Realizacja Umowy obejmującej Urząd oraz jednostki podległe, tj. Miejsko-Gminny Ośrodek Pomocy Społecznej w Chmielniku – dalej także: MGOPS oraz Środowiskowy Dom Pomocy dla Osób z Zaburzeniami Psychicznymi i Niepełnosprawnych Intelektualnie w Chmielniku – dalej także: Środowiskowy Dom Pomocy, przebiegała prawidłowo i terminowo z zachowaniem zasady uzyskiwania najlepszych efektów z danych nakładów, a także zasady optymalnego doboru metod i środków służących osiągnięciu założonych celów. Urząd prowadził wyodrębnioną ewidencję księgową oraz posiadał wyodrębniony rachunek bankowy umożliwiający identyfikację wszystkich transakcji oraz poszczególnych operacji bankowych związanych z Projektem. Wyznaczeni przez Burmistrza do realizacji Projektu pracownicy Urzędu, posiadali stosowne do tego zadania kompetencje i umiejętności. Ich wyznaczenie nastąpiło ustnie, zaś zakres obowiązków, uprawnień i odpowiedzialności nie ujmował zagadnienia realizacji grantu. Stan ten został zmieniony w trakcie trwania kontroli. Środki pozyskane z grantu, wynoszące 850 000, 00 zł., były wydatkowane gospodarnie, a dotychczas poniesione przez Urząd wydatki na szkolenia, zakupy sprzętu i oprogramowanie były kwalifikowalne i zgodne z zawartą Umową. Zakupione urządzenia i oprogramowanie zostało zainstalowane i uruchomione. Stopień zaawansowania działań Urzędu, nie stwarzał zagrożeń w terminowej realizacji całości Umowy. Przyjęte przez Urząd mierniki wskaźników produktu i rezultatu były zgodne z Regulaminem Konkursu Grantowego (dalej także: Regulamin Grantowy) i zostały w pełni osiągnięte. Pomimo, iż do czasu zakończenia niniejszej kontroli Projekt nie został zakończony, Burmistrz podjął działania celem wprowadzenia procedury monitorowania utrzymania osiągniętego poziomu cyberbezpieczeństwa, w tym efektów projektu „Cyberbezpieczna Gmina Chmielnik" po jego zakończeniu. Urząd opracował, ustanowił i wdrożył System Zarządzania Bezpieczeństwem Informacji, na który składało się kilka zarządzeń, w tym Polityka Bezpieczeństwa Informacji. Ww. dokumenty zostały opublikowane i przedstawione do zapoznania się oraz stosowania wszystkim

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

pracownikom Urzędu. Obowiązująca dokumentacja SZBI i PIB była poddana okresowym przeglądom, dokonanym przez upoważnionych do tego - Inspektora Ochrony Danych oraz Administratora Systemów Informatycznych. Z przeglądów tych sporządzono sprawozdania. Urząd nie przeprowadził w 2024 r. obowiązkowego, corocznego audytu z zakresu bezpieczeństwa informacji. Prawidłowo realizował, wynikający z zawartej Umowy, obowiązek informowania obywateli o fakcie otrzymania dofinansowania na realizację Projektu.

III. Opis ustalonego stanu faktycznego oraz oceny cząstkowe[3] kontrolowanej działalności

OBSZAR **Realizacja przez Gminę działań w celu zwiększenia poziomu cyberbezpieczeństwa**

Opis stanu faktycznego

1. W okresie objętym kontrolą, w Mieście i Gminie Chmielnik obowiązywał Statut Miasta i Gminy Chmielnik (dalej także: Statut), uchwalony w dniu 22 lutego 2003 r. Uchwałą nr IV/44/2003 Rady Miejskiej w Chmielniku (dalej także: Rada Miejska) w sprawie uchwalenia Statutu Miasta i Gminy Chmielnik[4]. Statut ten, od daty jego uchwalenia, zmieniany był piętnastokrotnie uchwałami Rady Miejskiej (jeden raz w okresie objętym kontrolą[5]). W Urzędzie obowiązywał Regulamin Organizacyjny nadany przez Burmistrza w dniu 27 lutego 2018 r. zarządzeniem nr 455/2018[6]. Określał on strukturę Urzędu, organizację oraz zasady i zakres funkcjonowania poszczególnych komórek organizacyjnych. Regulamin ten został dziewięciokrotnie zmieniony zarządzeniami Burmistrza (dwukrotnie w okresie objętym kontrolą[7]).

W dniu 28 czerwca 2018 r. zarządzeniem nr 500/2018 Burmistrz powołał, bezpośrednio mu podlegającego, Inspektora Ochrony Danych Osobowych. Określił jego zakres obowiązków wynikających z zapewnienia bezpieczeństwa informacji w Urzędzie[8]. Zagadnienia z zakresu cyberbezpieczeństwa nie zostały wyodrębnione i przypisane ww. Inspektorowi. Także, powołany zarządzeniem Burmistrza nr 233/2020, Administrator Systemu Informatycznego w Urzędzie, nie miał wyodrębnionych i przypisanych tych zagadnień. Zobowiązany był do: *„dokonywania przeglądu i analizowania danych przyjętych w Urzędzie Miasta*

---

[3] 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.

[4] Dz. Urz. Woj. Świętokrzyskiego z 2003 r. nr 89, poz. 896.

[5] Uchwała nr II/6/2024 Rady Miejskiej w Chmielniku z dnia 27 maja 2024 r. - *(Dz. Urz. Woj. Świętokrzyskiego z dnia 31 maja 2024 r. poz. 2179).*

[6] https://www.chmielnik.com/asp/regulamin-organizacyjny-urzędu,524,,1

[7] Zarządzenie nr 627/2023 z 27 stycznia 2023 r. w sprawie wprowadzenia zmian do Regulaminu Organizacyjnego Urzędu Miasta i Gminy w Chmielniku (obowiązuje od 1 lutego 2023 r.); Zarządzenie nr 692/2023 z 17 lipca 2023 r. w sprawie wprowadzenia zmian do Regulaminu Organizacyjnego Urzędu Miasta i Gminy w Chmielniku.

[8] Zgodnie z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) i innych przepisów ochrony danych osobowych (RODO).

i Gminy w Chmielniku polityk bezpieczeństwa danych osobowych i współpracę w tym zakresie z Inspektorem Danych Osobowych".

Zagadnienia dotyczące cyberbezpieczeństwa, ze szczególnym uwzględnieniem jego zwiększenia, nie były ujęte w strategicznych dokumentach Urzędu. W okresie objętym kontrolą Miasto i Gmina Chmielnik nie posiadała aktualnej Strategii Rozwoju. W ostatnio obowiązującym (obecnie nieaktualnym) dokumencie pn. „Aktualizacja Strategii Rozwoju Miasta i Gminy Chmielnik na lata 2016-2020 z perspektywą do roku 2022" zagadnienia cyberbezpieczeństwa nie były zapisane. Jak wyjaśnił Burmistrz*: W związku ze zmieniającą się sytuacją międzynarodową (wojna w Ukrainie) i przyspieszonym rozwojem usług realizowanych za pomocą Internetu w szczególnie okresie pandemii Covid-19, Gmina podjęła działania wpisania do obecnie przygotowywanej Strategii Rozwoju Miasta i Gminy Chmielnik do 2030 r., sprawy dotyczące wsparcie rozwoju zaawansowanych kompetencji cyfrowych, w tym również w obszarze cyberbezpieczenstwa dla samorządu i zapewnienie cyberbezpieczeństwa (w ramach nowego dedykowanego obszaru interwencji). W związku z powyższym Burmistrz Miasta i Gminy Chmielnik zarządzeniem nr 628/2023 z dnia 27 stycznia 2023 r. wprowadził Politykę Bezpieczeństwa Informacji w Urzędzie Miasta i Gminy w Chmielniku, w której zapisano, że jednym z głównych celów Urzędu Miasta i Gminy w Chmielniku jest zapewnienie ochrony przetwarzania danych z zachowaniem gwarancji należytego bezpieczeństwa i poufności powierzonych informacji.*

(akta kontroli str. 6-7; 8; 9-15; 16-18; 19-38; 39-40; 41-44; 45-46)

2. Urząd rozpoznawał zagrożenia i wynikające z nich potrzeby w zakresie cyberbezpieczeństwa. Na stronie internetowej Urzędu[9] znajdowała się zakładka poświęcona temu zagadnieniu. Informowała ona m.in. o takich zagadnieniach jak: zasady dot. dbałości o bezpieczeństwo danych, poradnik bezpiecznego korzystania z Internetu podłączonego do urządzeń mobilnych, ogólne informacje na czym polega bezpieczeństwo w sieci, ostrzeżenie o wysyłaniu SMS przez oszustów, listę ostrzeżeń oraz tzw. Akademię NASK[10]w tym „ABC cyberbezpieczeństwa".

Jak wyjaśnił Naczelnik Wydziału Administracji*: W związku z rosnącą falą zagrożeń jakie czekają na użytkowników w sieci (...), w lipcu 2023 r. i we wrześniu 2023 r. Urząd Miasta i Gminy w Chmielniku przeprowadził telefoniczne rozmowy z kierownikami jednostek organizacyjnych dotyczące potrzeb zakupu usług i sprzętu w celu podniesienia bezpieczeństwa cyfrowego. Analizując założenia projektu „Cyberbezpieczny Samorząd" postanowiono objąć wsparciem te jednostki które można było, w celu poprawienia bezpieczeństwa pracy użytkowników z tych jednostek pracujących w sieci. Dlatego finalnie w projekcie oprócz Urzędu Miasta i Gminy Chmielnik w znalazł się również Miejsko-Gminny Ośrodek Pomocy Społecznej w Chmielniku i Środowiskowy Dom Samopomocy. Pozostałe jednostki, które nie mogły być ujęte projektem we własnym zakresie starają się podnieść swój poziom bezpieczeństwa. Informatyk Urzędu (...) przekazał te informacje kierownictwu Urzędu, które „dało zielone światło" do przystąpienia do projektu. W dniu 14 marca 2024 r. na sali ślubów w Urzędzie Miasta i Gminy w Chmielniku w obecności*

[9] https://www.chmielnik.com/asp/cyberbezpieczenstwo,836,,1
[10] Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy.

Sekretarza[11] odbyło się spotkanie z przedstawicielami jednostek organizacyjnych dotyczące zagrożeń i problemów związanych z cyberbezpieczeństwem. Na spotkaniu poruszane były problemy dotyczące braku wyspecjalizowanej kadry w jednostkach, braku urządzeń i środków finansowych na poprawę bezpieczeństwa. Pracownicy Urzędu mają świadomość, rosnącego zagrożenia informatycznego. Wzięli udział w indywidualnych szkoleniach z cyberbezpieczństwa organizowanego przez NASK BIP, w dniach 3,4,5 lipca 2024 r[12]. O cyberzagrożeniach na bieżąco byli i są informowani pracownicy Urzędu za pośrednictwem wewnętrznego komunikatora np.:

o fałszywych e-mailach m.in.: z Ministerstwa Finansów i Krajowej Administracji Skarbowej, o zakazie stosowania zewnętrznych nośników (pamięci zewnętrznych). Urząd na bieżąco, informował mieszkańców o obowiązywaniu stopni alarmowych: Bravo, Charlie - CRP wydawanych przez Prezesa Rady Ministrów. W dniu 24 lutego 2022 r. Informatyk Urzędu kierował zapytania do usługodawców czy ze zwiększającą się falą cyberataków nie występują problemy z działaniem usług na rzecz Urzędu i czy są one odpowiednio chronione. W związku z wybuchem wojny w Ukrainie oraz zwiększonymi atakami cyberprzestępców na różne serwisy w okresie od 24 lutego do 31 maja 2022 r. w celu zwiększenia bezpieczeństwa informatycznego po godzinach pracy Urzędu oraz w weekendy został wyłączany dostęp do sieci Internet. Raportowaliśmy do Cert Polska incydenty cyberbezpieczeństwa: w dniu 23-02-2023 r. i w dniu 24-02-2023 r. Na bieżąco blokowane są fałszywe e-maile, które wpływają na skrzynki pocztowe służbowe Urzędu. Te wszystkie okoliczności i zdarzenia, zagrożenia z otaczającego świata w powiązaniu z wiedzą i zaangażowaniem Informatyka Urzędu, który jest Administratorem Systemów Informatycznych pozwoliły na przygotowanie wniosku o uzyskanie grantu „Cyberbezpieczny samorząd" w celu podniesienia stopnia bezpieczeństwa naszej infrastruktury i jednostek, którymi objęto projekt.

(akta kontroli str. 47-49; 50-51)

3. W Urzędzie funkcjonuje skrzynka ePUAP przy pomocy której Urząd przesyła różnego rodzaju dokumenty, w tym dokumenty wrażliwe.

Zgodnie z § 4 pkt 1 ppkt 4 umowy o powierzenie grantu (dalej także: Umowa), o której szerzej w dalszej części Wystąpienia, Urząd (jako Grantobiorca) był zobowiązany do przekazania do NASK (jako Operatora) uzupełnioną Ankietę Dojrzałości Cyberbezpieczeństwa w jednostkach Samorządu Terytorialnego (dalej także: Ankieta lub Ankieta Dojrzałości). Przekazanie winno nastąpić w terminie 30 dni od dnia zawarcia Umowy, zgodnie z zakresem określonym w dokumentacji konkursowej. Wykonując ten obowiązek, w dniu 26 lipca 2024 r. tj. w ciągu 24 dni od zawarcia Umowy, Urząd przekazał na wskazany w Umowie adres skrytki ePUAP NASK[13] wypełnioną Ankietę Dojrzałości (dotyczącą Urzędu oraz dwóch podmiotów uczestniczących w Projekcie tj. MGOPS oraz Środowiskowego Domu Pomocy. W dniu 06 sierpnia 2024 r. NASK przesłał do Urzędu informację, w której podziękował za przesłaną Ankietę i jednocześnie zwrócił się (na podstawie §5 pkt 3 ust. 2 Regulaminu Konkursu Grantowego –

[11] Sekretarz Urzędu.

[12] Byli to: Burmistrz, Z-ca Burmistrza, Sekretarz Gminy, Skarbnik, Z-ca Skarbnika, Naczelnik Wydziału Administracji, Informatyk, Główna Księgowa jednostek oświatowych, inspektor ds. obsługi sekretariatu.

[13] NASK-PIB:/NASK-Instytut/SkrytkaESP (akronim /temat: cyberbezpieczny.samorzad.ankieta).

dalej także: Regulamin Grantowy) o poprawę błędnie udzielonej odpowiedzi w tejże Ankiecie Dojrzałości. Nazajutrz, tj. 07 sierpnia 2024 r., z zachowaniem terminu pięciu dni, określonego w ww. przepisie Regulaminu Grantowego, Urząd przesłał stosowną korektę na skrzynkę ePUAP NASK.

(akta kontroli str. 52-57; 58-60)

4. W dniu 14 grudnia 2023 r. (godz. 09:31:37) Gmina Chmielnik, za pośrednictwem aplikacji[14], złożyła wniosek o numerze FERC.02.02-CS.01-001/23/1858 (dalej: Wniosek) o dofinansowanie w ramach konkursu „Cyberbezpieczny Samorząd", realizowanego w ramach Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa. Tytuł Projektu brzmiał: „Cyberbezpieczna Gmina Chmielnik". Wniosek przewidywał wydatki w wysokości 850 000,00 zł tj. 100% dofinansowania. Wkład UE wynosił 697 000,00 zł., a wkład BP 153 000,00 zł. Powyższa kwota była, zgodnie z §4 pkt. 4 Regulaminu Grantowego, maksymalną wysokością grantu o jaką mogła się ubiegać JST[15] w przypadku gmin (§4 pkt 3 Regulaminu Grantowego). W uzasadnieniu Wniosku Gmina wskazała, że: *(...) postępująca cyfryzacja stwarza nowe możliwości dla samorządów w zakresie realizacji zadań, projektów i przedsięwzięć oraz obsługi mieszkańców. Możliwościom i udogodnieniom, jakie daje cyfryzacja towarzyszą także zagrożenia dla bezpieczeństwa w sieci. Celem realizacji niniejszego projektu jest wzmocnienie poziomu bezpieczeństwa sieci i systemów.*

Wniosek zawierał ogólne informacje o projekcie; wskazanie miejsca realizacji projektu; informacje o Grantobiorcy (w tym osobę upoważnioną do kontaktu, tj. T.B. - Naczelnika Wydziału Administracji); zakres rzeczowy Projektu; zakres finansowy; źródła finansowania oraz oświadczenia i załączniki.

W dniu 02 lipca 2024 r. zawarta została umowa o powierzeniu grantu[16] pomiędzy Skarbem Państwa, w imieniu którego działało Centrum Projektów Polska Cyfrowa (dalej: CPPC) a Gminą Chmielnik. Środki finansowe przewidziane Umową tj. 850 000,00 zł, zostały udzielone w wyniku rozstrzygnięcia konkursu grantowego w ramach projektu *Cyberbezpieczny Samorząd* nr FERC.02.02-CS.01-001/23 (dalej: Cyberbezpieczny Samorząd). Pochodziły one z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (dalej: FERC). Konkurs grantowy został przeprowadzony i rozstrzygnięty przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy. Zgodnie z postanowieniami Umowy (§2 pkt 1) Gmina otrzymała środki w wysokości 100% kwoty wskazanej we wniosku o przyznanie grantu (850 000,00 zł), w tym dofinansowanie ze środków Unii Europejskiej stanowiące 82% (697 000,00 zł), oraz dofinansowanie z budżetu państwa stanowiące 18% (153 000,00 zł). Miały one zostać wypłacone (§2 pkt 7) w trzech transzach zaliczkowych w wysokości kolejno: 30%, 30% i 40% przyznanej kwoty. Umowa przewidywała (§2 pkt 8) możliwość zmiany wysokości, jak i terminu wypłaty transzy, po otrzymaniu przez NASK (jako Operatora) pisemnej prośby z uzasadnieniem, ww. zmiany ze strony Gminy. Pierwsza transza mogła zostać wypłacona w terminie do 60 dni kalendarzowych po

[14] Aplikacja do składania wniosków dostępna na stronie: www.gov.pl/cppc/cyberbezpiecznysamorzad

[15] Jednostka Samorządu Terytorialnego.

[16] Nr FERC.02.02-CS.01-001/23/1858/FERC.02.02.-CS.01-001/23/2024.

zawarciu umowy, nie wcześniej jednak niż po złożeniu Ankiety Dojrzałości (§2 pkt 7 ust. 1 Umowy). Okres realizacji projektu i okres realizacji Umowy (§3 pkt 1) miał trwać maksymalnie 24 miesiące od dnia wejścia w życie, ale nie dłużej niż do 30 czerwca 2026 r. Natomiast kwalifikowalność poniesionych wydatków (§6 pkt 1) miała rozpocząć się od 1 czerwca 2023 r. i zakończyć maksymalnie w ciągu 24 miesięcy od dnia wejścia w życie, ale nie dłużej niż do 30 czerwca 2026 r. Wydatki poniesione przed, oraz po ww. okresie miały zostać uznane za niekwalifikowalne (§6 pkt 2). Wydatki te, w ramach Projektu, Gmina była zobowiązana pokryć w pełni we własnym zakresie. Warunki realizacji Projektu i obowiązki Gminy (§4) przewidywały zakup sprzętu/usług/ oprogramowania/realizacji szkoleń opisanych we Wniosku o przyznanie grantu, Regulaminie Grantowego oraz w Umowie. Gmina zobowiązana była do przekazania zakupionego sprzętu/usług/oprogramowania nieodpłatnie do podmiotów wskazanych we Wniosku o przyznanie grantu (MGOPS i Środowiskowy Dom Pomocy). Zobowiązana była również do przekazania do NASK (jako do Operatora) wypełnionej Ankiety Dojrzałości Cyberbezpieczeństwa w Jednostkach Samorządu Terytorialnego w terminie 30 dni od dnia zawarcia Umowy (pod rygorem wstrzymania wypłaty dofinansowania) jako obligatoryjnego załącznika do wniosku rozliczającego. Środki przyznane do wykorzystania Gminie, zgodnie z Umową i Wnioskiem o przyznanie grantu, powinny być wydatkowane w trzech obszarach: usług organizacyjno/technologicznych, usług kompetencyjnych i zakupu systemów służących zwiększeniu poziomu bezpieczeństwa informacji w jednostkach.

Zgodnie z §4 ust. 1 pkt 6 Umowy, Gmina wydzieliła w dniu16 listopada 2023 r. księgi rachunkowe z osobnym dziennikiem pn. „Cyberbezpieczna Gmina Chmielnik" oraz otwarła wyodrębniony rachunek bankowy przypisany do Projektu[17]. Prowadzona była odrębna ewidencja księgowa kosztów, wydatków i przychodów umożliwiająca identyfikację wszystkich transakcji oraz poszczególnych operacji bankowych związanych z Projektem. Do prowadzenia ksiąg rachunkowych w ramach ww. Projektu stosowane były zasady określone w zarządzeniu Burmistrza z dnia 02 stycznia 2018 r. w sprawie ustalenia zasad rachunkowości dla budżetu Gminy Chmielnik[18]. W opisach dowodów księgowych (zatwierdzonych pod względem merytorycznym oraz formalnym i rachunkowym) została zapewniona ścieżka audytu poprzez zawarcie w nich informacji o finansowaniu zakupów sprzętu ze środków FERC, w tym również numer umowy i kwota kwalifikowanego wydatku (§4 ust. 1 pkt 8 Umowy).

W dniu 27 sierpnia 2024 r. Gmina Chmielnik, po uprzednim przekazaniu do NASK wypełnionej Ankiety Dojrzałości Cyberbezpieczeństwa w Jednostkach Samorządu Terytorialnego (o czym powyżej w niniejszym wystąpieniu pokontrolnym), otrzymała pierwszą transzę środków przewidzianych w Umowie, wynoszącą 250 000, 00 zł. W dniu 26 września 2024 r. Gmina wystąpiła (na podstawie §2 pkt 8 Umowy) z pisemnym wnioskiem o przekazanie całej kwoty dofinansowania, motywując wniosek możliwością sprawnego przeprowadzenia postępowania zamówień publicznych i optymalnej realizacji Projektu. W dniu 29 listopada 2024 r. Gmina otrzymała drugą (i ostatnią) transzę środków

[17] Bank Spółdzielczy w Chmielniku, rachunek bankowy o numerze: 77848300012001000000130199 pn. „Cyberbezpieczna Gmina Chmielnik".
[18] Zarządzenie nr 439/2018.

w wysokości 595 000,00 zł., stanowiącą uzupełnienie do pełnej wysokości przyznanych Umową środków.

Gmina nie utworzyła osobnego harmonogramu realizacji zakresu rzeczowego Projektu. Jak wyjaśnił Naczelnik Wydziału Administracji: *(...) na podstawie przyjętego Wniosku, i w samym Wniosku o dofinansowanie, w zakresie rzeczowym i finansowym określano zakres zrealizowanych i przyjętych do realizacji działań objętych dofinansowaniem.*

W celu zakupu, dostawy i wdrożenia sprzętu informatycznego i oprogramowania w ramach Projektu, Gmina przeprowadziła przetarg w trybie podstawowym, na podstawie art. 275 pkt 2 ustawy z dnia 11 września 2029 r. Prawo zamówień publicznych[19]. Ogłoszenie o zamówieniu zostało zamieszczone w Biuletynie Informacji Publicznej Gminy Chmielnik i w Biuletynie Zamówień Publicznych[20]. W wyniku przetargu wyłoniony został wykonawca[21], z którym w dniu 17 stycznia 2025 r. zawarta została umowa[22]. Jej przedmiotem była: „*Dostawa sprzętu komputerowego, oprogramowania informatycznego oraz usług szkoleniowo-audytowych w ramach realizacji projektu grantowego „Cyfrowa Gmina".* Realizacja umowy została potwierdzona dokumentacja powykonawczą.

W ramach projektu „Cyberbezpieczna Gmina Chmielnik" zrealizowano:

1.W obszarze usług organizacyjno/technicznych:

- audyt Systemu Zarządzania Bezpieczeństwem Informacji (dalej także: SZBI) oraz Krajowych Ram Interoperacyjności (dalej także: KRI) we wszystkich jednostkach objętych Projektem. Wydatkowano 22 140,00 zł, tj. 26,04% całości środków grantu (SUMA przewidziana w ramach przyznanego grantu: 65 190,00 zł).

2. W obszarze usług kompetencyjnych:

- szkolenia kadry kierowniczej ze wszystkich jednostek objętych Projektem; szkolenia pracowników z cyberbezpieczeństwa ze wszystkich jednostek objętych Projektem; szkolenie Administratorów (2 osoby) z zakupionego urządzenia UTM. Wydatkowano 10 400, zł, tj. 12,23% całości środków grantu (SUMA przewidziana w ramach przyznanego grantu wynosiła 50 430,00 zł).

3. W ramach zakupu systemów służących zwiększeniu poziomu bezpieczeństwa informacji w jednostkach zakupiono i zrealizowano:

W Urzędzie Miasta i Gminy w Chmielniku:

- rozbudowa Serwerów Urzędu o karty komunikacji z Macierzą; serwer Backup-u; macierz Dyskowa; biblioteka taśmowa; deduplikator; centralny UPS; urządzenie typu NAS; urządzenia Access Point; urządzenie UTM; zarządzalne przełączniki sieciowe; oprogramowanie Microsoft Server Datacenter; oprogramowanie do Backup-u dla serwera; upgrade oprogramowania VMvare – w celu utworzenia klastra serwerów; aktualizacja posiadanego oprogramowania do backup-u w celu podłączenia do deduplikatora; oprogramowanie do analizy logów.

W MGOPS:

---

[19] Dz. U. z 2024 r. poz. 1320.
[20] W dniu 23 grudnia 2024 r., nr 2024/BZP 00670728/01.
[21] Tj. ncNETcom Sp. z o.o.
[22] Umowa nr 4/IPS/2025.

- serwer z oprogramowaniem Windows Serwer; urządzenie UTM; zarządzalny przełącznik sieciowy; urządzenie typu NAS.

W Środowiskowym Domu Samopomocy:

- urządzenie UTM.

Wydatkowano 726 252,27 zł, tj. 85,44% całości środków grantu (SUMA przewidziana w ramach przyznanego grantu: 734 380, zł).

Wszystkie zakupione ww. urządzenia oraz oprogramowania spełniały warunki kwalifikowalności określone w Regulaminie Grantowym (§4 ust. 7) i w Umowie (§6). Zostały one skonfigurowane i wdrożone.

Zakupione w ramach Projektu urządzenia dla MGOPS oraz Środowiskowego Domu Pomocy, zostały nieodpłatnie przekazane tym jednostkom (protokołem przekazania[23]). Zgodnie z §4 ust. 1 pkt 3 Umowy. Protokół zawierał informację, iż zakup urządzeń został zrealizowany z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC).

Jak wyjaśnił Naczelnik Wydziału Administracji, realizacja grantu przebiegła zgodnie z podpisaną Umową i brak było zagrożeń nie wykonania wszystkich punktów przewidzianych Wnioskiem o dofinansowanie. Na 31 punktów przyjętych do realizacji, wykonano 24 (co stanowiło 77,42% realizacji Projektu). Do czasu zakończenia kontroli nie wykonano siedmiu punktów (co stanowiło 22,58% Projektu). Pozostało do wykonania:

1. W zakresie usług organizacyjno/technologicznych:

- wdrożenie i aktualizacja dokumentacji SZBI w Urzędzie (do 30 września 2025 r.); przeprowadzenie audytu SZBI we wszystkich jednostkach objętych Projektem (do 31 stycznia 2026 r.); przeprowadzenie audytu Systemu Zarządzania Bezpieczeństwa Informacji wdrożonego w Urzędzie (do 30 kwietnia 2026 r.).

SZBI został ustanowiony i wdrożony w Urzędzie, jednakże jak wyjaśnił Naczelnik Wydziału Administracji*: w związku ze zmieniającą się sytuacją prawną, wzrostem zagrożeń informatycznych, postępem technologicznym i z nowymi uregulowaniami prawnymi dot. cyberbezpieczeństwa tj.: Dyrektywą Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) stosowany w jednostce SZBI wymaga aktualizacji, co zostanie wykonane w ramach projektu „Cyberbezpieczny Samorząd". Urząd jest obecnie w trakcie opracowywania nowego dokumentu.*

2. W zakresie usług kompetencyjnych:

- szkolenia kadry kierowniczej w 2026 r. ze wszystkich jednostek objętych Projektem; szkolenia dla pracowników z cyberbezpieczeństwa w 2026 r. ze wszystkich jednostek objętych Projektem; szkolenia Administratora z Windows Serwer, AD oraz vMware. (do 30 września 2025 r.).

3. W zakresie zakupu systemów służących zwiększeniu poziomu bezpieczeństwa informacji w jednostkach:

- wdrożenie logowania domeną do programów dziedzinowych (do końca 2025 r.).

[23] Z dnia 17 marca 2024 r.

Naczelnik Wydziału Administracji wyjaśnił ponadto, że ostatnie zadanie zostanie wykonane do 30 kwietnia 2026 r., a więc na dwa miesiące przed końcem terminu wynikającego z umowy o przyznanie grantu.

Do dnia 14 maja 2025 r. Urząd wydatkował na realizację Programu kwotę 758 792,27 zł. tj. 89,27% całości Projektu, w tym łączna wartość urządzeń wyniosła 532 455,14 zł., co stanowiło 62,64% całości Projektu.

Nie poniesiono wydatków przed 1 czerwca 2023 r. (§6 pkt 2 Umowy), zaś wszystkie poniesione wydatki spełniały wymogi kwalifikowalności, zarówno zgodnie z Regulaminem Konkursu Grantowego (§4 pkt 7), jak i Umową (§6). Realizacja Umowy obejmującej Urząd oraz jednostki podległe, tj. Miejsko-Gminny Ośrodek Pomocy Społecznej w Chmielniku – dalej także: MGOPS oraz Środowiskowy Dom Pomocy dla Osób z Zaburzeniami Psychicznymi i Niepełnosprawnych Intelektualnie w Chmielniku – dalej także: Środowiskowy Dom Pomocy, przebiegała prawidłowo i terminowo z zachowaniem zasady uzyskiwania najlepszych efektów z danych nakładów, a także zasady optymalnego doboru metod i środków służących osiągnięciu założonych celów.

(akta kontroli str. 61-85; 86-88; 89-101; 102-117; 118-119; 120-123; 124-131; 132-138; 139-168; 169-200; 201-205; 206-208; 209-226; 227-234; 235-236; 237-239; 240-241; 242; 243-248; 249-275; 276-277; 511-512)

5. W ramach realizacji grantu przewidziany był także udział dwóch jednostek Urzędu tj. Miejsko-Gminnego Ośrodka Pomocy Społecznej w Chmielniku i Środowiskowego Domu Samopomocy dla Osób z Zaburzeniami Psychicznymi i Niepełnosprawnych Intelektualnie w Chmielniku. Jak wyjaśnił Informatyk, Urząd i podległe mu jednostki, w tym MGOPS i Środowiskowy Dom Opieki (uczestniczące w Projekcie) nie korzystały ze wspólnej sieci teleinformatycznej. Każda z tych jednostek posiadała swoją odrębną sieć teleinformatyczną.

Wniosek grantowy przewidywał:

- doposażenie Miejsko-Gminnego Ośrodka Pomocy Społecznej poprzez zakup serwera, firewall-a (UTM), zarządzanego switch-a oraz urządzenia do przechowywania backup-ów (urządzenie typu NAS). Działania te miały znacząco poprawić bezpieczeństwo przetwarzania danych oraz zabezpieczyć sieć lokalną należącą do MGOPS przed zagrożeniami wynikającymi z połączenia z siecią Internet.

- doposażenie Środowiskowego Domu Samopomocy dla Osób z Zaburzeniami Psychicznymi i Niepełnosprawnych Intelektualnie w Chmielniku z siedzibą w Zreczu Dużym w urządzenie sieciowe firewall-a (UTM), co miało znacząco poprawić bezpieczeństwo sieci przed zagrożeniami wynikającymi z połączenia z siecią Internet.

W myśl Wniosku realizacja ww. przedsięwzięć miała przyczynić się do poprawy cyberbezpieczeństwa wśród pracowników i interesantów.

Wszystkie urządzenia przewidziane Wnioskiem zostały zakupione i zainstalowane w wymienionych jednostkach (o czym w poprzednim punkcie niniejszego wystąpienia pokontrolnego).

(akta kontroli str. 89-101; 278; 279-285)

6. W związku z realizacją grantu, Burmistrz wyznaczył w dniu 24 sierpnia 2023 r. pięcioro pracowników Urzędu Miasta i Gminy w Chmielniku, jako

odpowiedzialnych za realizację prac dotyczących Projektu. Byli to: Naczelnik Wydziału Administracji, Informatyk w Wydziale Administracji, Skarbnik, Inspektor ds. księgowości budżetowej i Inspektor ds. projektów strukturalnych. Wszyscy ww. pracownicy posiadali kompetencje niezbędne do udziału w realizacji grantu. W szczególności posiadali oni wykształcenie wyższe magisterskie i brali udział w specjalistycznych szkoleniach (poświadczonych stosownym certyfikatem) w tym m.in.: z zakresu zagadnień cyberbezpieczeństwa, bezpieczeństwa i ochrony informacji, finansów lub finansów U. E. Brali również, jak wyjaśnił Burmistrz, dodatkowo udział w czterech webinarach[24] dotyczących przygotowania wniosku o uzyskanie dofinansowania z grantu „Cyberbezpieczny Samorząd" organizowanych przez Centrum Projektów Cyfrowa Polska" oraz webinarze „System do obsługi grantów" w projekcie „Cyberbezpieczny Samorząd", który odbył się 28 sierpnia 2024 r.

Zakres czynności, tj. obowiązków, uprawnień i odpowiedzialności ww. pracowników, nie ujmowały zagadnienia realizacji grantu, zaś wyznaczenie przez Burmistrza pracowników do jego realizacji nastąpiło ustnie, o czym więcej w sekcji *Stwierdzone nieprawidłowości*.

Burmistrz w trakcie niniejszej kontroli aneksami z dnia 12 maja 2025 r. uzupełnił zakres czynności ww. pracowników. Do zakresu ich obowiązków dodany został zapis dot. realizowania obowiązków (odpowiednio pod kątem finansowym – Skarbnik, informatycznym – Informatyk w Wydziale Administracji, finansowo-księgowym – Inspektor ds. księgowości budżetowej, zamówień publicznych – Inspektor ds. projektów strukturalnych i ogólnego nadzoru – Naczelnik Wydziału Administracji) w ramach Projektu grantowego „Cyberbezpieczny Samorząd" o numerze FERC.02.02-CS.01-001/23; Umowa o powierzenie grantu o numerze FERC.02.02-CS.01-001/23/1858.

(akta kontroli str. 286-287; 288-312; 313; 314-318; 319)

7. W okresie objętym kontrolą w Urzędzie nie wystąpiła fluktuacja kadr obejmująca osoby uczestniczące w realizacji grantu. Jak wyjaśnił Burmistrz: *wszystkie osoby, które zostały wskazane do obsługi i realizacji grantu, uczestniczą w nim w dalszym ciągu tj. od momentu ich wskazania do chwili obecnej*.

(akta kontroli str. 286)

8. Urząd określił cele Projektu przy pomocy ośmiu mierzalnych wskaźników rezultatu i produktu zgodnie z załącznikiem nr 9 do Regulaminu Grantowego. Termin realizacji przyjętych wskaźników został wyznaczony na 30 kwietnia 2026 r. Wszystkie wskaźniki zostały zrealizowane w całości w terminie wcześniejszym. Na dzień 15 maja 2025 r. wartości tych wskaźników wynosiły[25]:

- wskaźnik nr 1 - liczba pracowników IT podmiotów wykonujących zadania publiczne objętych wsparciem szkoleniowym – dwie osoby, tj. zero kobiet i dwóch mężczyzn (jeden z UMiG i jeden z MGOPS). Założono dwie osoby tj. zero kobiet i dwóch mężczyzn;

- wskaźnik nr 2 - liczba pracowników podmiotów wykonujących zadania publiczne nie będące pracownikami IT, objętych wsparciem szkoleniowym (nie będących pracownikami UMiG, MGOPS i Środowiskowego Domu Pomocy) – 82

[24] W dniach: 25 sierpnia 2023 r., 25 września 2023 r., 20 października 2023 r. i 22 listopada 2023 r.
[25] Wskaźniki nr 1i 2 z podziałem na mężczyzn i kobiety.

osoby, tj. 73 kobiety i dziewięciu mężczyzn. Założono od 50 do 80 kobiet i od pięciu do dziewięciu mężczyzn;

- wskaźnik nr 3 – liczba systemów służących zwiększeniu poziomu bezpieczeństwa informacji – 11 sztuk[26]. Założono 11 sztuk;

- wskaźnik nr 4 – liczba użytkowników nowych i zmodernizowanych publicznych usług, produktów i procesów cyfrowych – 73 osoby/rok (UMiG, MGOPS i Środowiskowy Dom Pomocy). Założono od 50 do 80 osób;

- wskaźnik nr 5 - liczba podmiotów wspartych w zakresie cyberbezpieczeństwa w ramach JST – trzy podmioty (UMiG, MGOPS i Środowiskowy Dom Pomocy). Założono trzy podmioty;

- wskaźnik nr 6 - liczba JST wspartych w zakresie cyberbezpieczeństwa – jeden podmiot (UMiG). Założono jeden podmiot;

- wskaźnik nr 7 - liczba podmiotów wspartych w zakresie cyberbezpieczeństwa – trzy podmioty (UMiG, MGOPS i Środowiskowy Dom Pomocy). Założono trzy podmioty;

- wskaźnik nr 8 - liczba podmiotów wspartych w zakresie rozwoju usług, lub istotnej modernizacji usług, produktów i procesów cyfrowych w kontekście działań e-administracji – trzy podmioty (UMiG, MGOPS i Środowiskowy Dom Pomocy).Założono trzy podmioty.

Wszystkie ww. wskaźniki mieściły się w pierwotnie założonych wartościach.

(akta kontroli str. 320-325; 326-327; 328-329)

9. Wszystkie zakupione w ramach grantu urządzenia i oprogramowania, zarówno w Urzędzie jak i w dwóch pozostałych podmiotach objętych Projektem, zostały zainstalowane i uruchomione, co zostało potwierdzone przeprowadzonymi oględzinami.

Do czasu zakończenia kontroli zostały przeprowadzone następujące audyty i szkolenia:

- audyt SZBI we wszystkich jednostkach objętych Projektem;

- szkolenia kadry kierowniczej ze wszystkich jednostek objętych Projektem; szkolenia pracowników z cyberbezpieczeństwa ze wszystkich jednostek objętych Projektem; szkolenie Administratorów (2 osoby) z zakupionego urządzenia UTM.

Pozostałe audyty i szkolenia przewidziane Projektem mają być przeprowadzone do czerwca 2026 r. (o czym powyżej w niniejszym Wystąpieniu).

(akt kontroli str. 209-226; 227-234; 240-241; 243-248; 279-285; 385-387; 388)

10. W okresie objętym kontrolą, Projekt grantowy „Cyberbezpieczny Samorząd" nie został zakończony i był w trakcie realizacji (o czym powyżej niniejszego wystąpienia pokontrolnego). Procedury związane z Projektem, a odnoszące się do aktualizacji SZBI, prowadzenia analiz ryzyka dot. bezpieczeństwa informacji, analizy incydentów SZBI oraz prowadzenia audytów i wdrażania sformułowanych rekomendacji, będą mogły być realizowane po zakończeniu tegoż Projektu. W ramach działań mających na celu utrzymanie poziomu cyberbezpieczeństwa po zakończeniu realizacji Projektu, w dniu 30 kwietnia

[26] 1. UTM- ŚDS; 2. UTM – MGOPS; 3. Serwer z oprogramowaniem – MGOPS; 4. NAS – MGOPS; 5. UTM – UMiG; 6. NAS – UMIG; 7. Serwer – UMiG; 8. Macierz – UMiG; 9. Deduplikator – UMiG; 10. Biblioteka taśmowa – UMiG; 11. Oprogramowanie do analizy logów- UMiG.

2025 r. Burmistrz wydał zarządzenie[27]w sprawie wprowadzenia procedury monitorowania utrzymania efektów projektu „Cyberbezpieczna Gmina Chmielnik". Zgodnie z załącznikiem do ww. zarządzenia, celem i zakresem procedury było gromadzenie informacji w zakresie utrzymania środków trwałych i usług nabytych w trakcie Projektu przez okres dwóch lat od jego zakończenia oraz utrzymanie trwałości Projektu grantowego. Dane i informacje na potrzeby monitoringu będą zbierane cyklicznie raz do roku w I kwartale, począwszy od roku 2027.

(akta kontroli str. 330-333)

11. W Urzędzie opracowano, ustanowiono i wdrożono System Zarządzania Bezpieczeństwem Informacji, zgodnie z rozporządzeniem 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[28] (§19 ust. 1 w związku z ust. 3). Podstawowym dokumentem składającym się na SZBI było zarządzenie nr 628/2023 z dnia 27 stycznia 2023 r. w sprawie Polityki Bezpieczeństwa Informacji (dalej także: zarządzenie ws. PBI) w Urzędzie Miasta i Gminy w Chmielniku. Regulowała ona m.in. takie zagadnienia jak: metoda szacowania ryzyka i jego analiza, organizacja bezpieczeństwa informacji, zarządzanie aktywami, bezpieczeństwo zasobów ludzkich, zarządzanie systemami i sieciami, bezpieczeństwo fizyczne i środowiskowe, kontrola dostępu, pozyskiwanie, rozwój i utrzymanie systemów informatycznych, zarządzanie incydentami związanymi z bezpieczeństwem informacji; zarządzanie ciągłością działania. Nadto częścią Systemu Zarządzania Bezpieczeństwem Informacji (w zakresie cyberbezpieczeństwa) były:

1. Zarządzenie nr 554/2022 z dnia 21 października 2022 r. w sprawie stosowania planów awaryjnych w zakresie ciągłości działania w obszarze odtwarzania techniki informatycznej po katastrofie obowiązujące w Urzędzie Miasta i Gminy w Chmielniku, zmienione zarządzeniem Nr 629/2023 z dnia 27 stycznia 2023 r. w sprawie zmian do procedury stosowania planów awaryjnych w zakresie ciągłości działania w obszarze odtwarzania techniki informatycznej po katastrofie obowiązujące w Urzędzie Miasta i Gminy w;

2. Zarządzenie nr 636/2023 z dnia 16 lutego 2023 r. w sprawie wprowadzenia procedury zarządzania incydentami związanymi z bezpieczeństwem informacji i cyberbezpieczeństwem w Urzędzie Miasta i Gminy w Chmielniku;

3. Zarządzenie nr 637/2023 z dnia 16 lutego 2023 r. w sprawie wprowadzenia procedury zarządzania incydentami cyberbezpieczeństwa.

Ww. zarządzenia zostały opracowane, opublikowane i przedstawione do zapoznania się oraz stosowania wszystkim pracownikom[29] za pośrednictwem systemu elektronicznego zarządzania dokumentacją SIDAS-EZD.

Zgodnie z pkt 5.1.3. zarządzenia ws. PBI, za bezpieczeństwo informacji odpowiedzialny był każdy pracownik Urzędu na swoim stanowisku pracy. Za całokształt PBI odpowiadał Burmistrz, natomiast za realizację poszczególnych

[27] Zarządzenie Nr 183/2025
[28] Dz. U. poz. 773.
[29] W dniu 14 lutego 2023 r. i 20 lutego 2023 r.

elementów PBI odpowiadali Inspektor Ochrony Danych (IOD) oraz Administrator Systemu Informacji (ASI).

Za aktualizację, opracowywanie, wdrażanie i ocenę stosowanych polityk odpowiedzialny był Inspektor Ochrony Danych oraz Administrator Systemu Informacji.

(akta kontroli str. 334-342; 343-351; 352-372; 373-384)

12. Zgodnie z §19 ust. 2 pkt 1 KRI, zarządzanie bezpieczeństwem informacji realizowane jest w szczególności zapewnieniem przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie działań, które m.in. zapewniają aktualizację regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia. Zapisy dotyczące przeglądów PBI zawierał pkt 16 zarządzenia ws. PBI, zgodnie z którym, w zależności od potrzeb w celu utrzymania odpowiedniego, wysokiego poziomu bezpieczeństwa informacji w Urzędzie *„…dokonuje się regularnych przeglądów niniejszej Polityki i ewentualnie audytów systemu bezpieczeństwa informacyjnego Urzędu"*. Przegląd powinien być dokonany nie rzadziej niż jeden raz w ciągu roku. Inspektor Ochrony Danych miał koordynować realizację przeglądów i w zależności od potrzeb zalecać ich wykonanie wewnątrz Urzędu lub na zewnątrz. Przeprowadzenie przeglądu lub audytu miało być dokumentowane w formie protokołu lub raportu. Dodatkowe przeglądy polityki bezpieczeństwa i stosowanych zabezpieczeń powinny być przeprowadzone w sytuacjach, gdy nastąpiły znaczące zmiany w organizacji mające wpływ na politykę Urzędu lub z nią związane. W szczególności dotyczyło to sytuacji, w której nastąpiło przekazanie do eksploatacji nowego, kluczowego systemu informatycznego, znaczących zmian organizacyjnych w funkcjonowaniu Urzędu lub zmian w obowiązującym prawie.

W celu realizacji ww. obowiązków, w latach 2023, 2024 i 2025[30] Inspektor Ochrony Danych oraz Administrator Systemów Informatycznych przeprowadzili przeglądy obowiązujących w Urzędzie dokumentacji PBI i SZBI. Z przeglądów sporządzono sprawozdania, które zawierały m.in. opis podjętych czynności, najważniejsze wnioski i zalecenia oraz wskazanie terminu następnego przeglądu. W 2023 r. poza przeglądem, m.in. zaktualizowano SZBI funkcjonujący w Urzędzie poprzez dodanie nadrzędnego PBI opartego na Normie (PN-ISO/IEC 27001:2017-06). Stwierdzono, że w UMiG nie nastąpiły istotne zmiany organizacyjne i prawne, które by wpływały na dokonanie kolejnych aktualizacji stosowanej dokumentacji. Wskazano na marzec 2024 r. jako na termin kolejnego przeglądu. W 2024 r. w wyniku przeglądu stwierdzono, że w okresie od 1 marca 2023 r. do 29 lutego 2024 r. w UMiG nie wystąpiły istotne zmiany organizacyjne, prawne i techniczne. Termin następnego przeglądu został wyznaczony na marzec 2025 r. Podczas przeglądu dokonanego w dniu 4 marca 2025 r. stwierdzono, że *w strukturze sieci nastąpiły duże zmiany, które po wdrożeniu logowania domeną w programach dziedzinowych zostaną uwzględnione w dokumentacji.* Ustalono także, że w związku z nowymi uregulowaniami prawnymi dot. Cyberbezpieczeństwa tj: Dyrektywą Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r.[31] Urząd będzie musiał posiadać w pełni opracowaną dokumentację SZBI. W związku z powyższym konieczne

[30] W dniu 1 marca 2023, w dniu 1 marca 2024 i w dniu 4 marca 2025.

[31] W sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii.

będzie opracowanie uzupełnień i dostosowania dokumentacji do nowych przepisów prawa. Termin kolejnego przeglądu został wyznaczony na marzec 2026 r.

Jak wyjaśnił Naczelnik Wydziału Administracji, Urząd Miasta i Gminy podjął działania zmierzające do *opracowania nowej dokumentacji PBI, SZBI i cyberbezpieczeństwa w 2025 r.*

(akta kontroli str. 385-387; 388; 389-395, 513-513)

13. W okresie objętym kontrolą, Urząd przeprowadził w latach 2023 i 2025, okresowy/coroczny audyt bezpieczeństwa informacji określony w § 19 ust. 2 pkt 14 KRI. Audyty miały na celu sprawdzenie wdrożonych zabezpieczeń oraz identyfikację obszarów, które należało usprawnić. Nastawione były na identyfikację ryzyka i ewentualnych skutków jego wystąpienia. Z przeprowadzonych audytów sporządzone zostały raporty.

WW. audyty został przeprowadzony przez audytorów zewnętrznych, posiadających kompetencje w tym zakresie, potwierdzone stosownymi dokumentami[32].

Przedstawione zalecenia zostały przez Urząd wykonane niezwłocznie lub sukcesywnie, a niektóre z nich stały się nieaktualne z powodu upływu czasu (wygaśnięcie umów zawartych na czas oznaczony).

W 2024 r. w Urzędzie nie został przeprowadzony okresowy audyt z zakresu bezpieczeństwa informacji, o czym więcej w sekcji *Stwierdzone Nieprawidłowości*.

(akta kontroli str. 396-412; 413-431; 432-435; 436-446; 447-472; 473; 474; 475-479)

14. Urząd informował opinię publiczną o fakcie otrzymania dofinansowania na realizację projektu. W szczególności, stosownie do zasad określonych w „Podręczniku wnioskodawcy i beneficjenta programów spójności 2021-2027 w zakresie informacji i promocji”[33] oraz postanowień §11 Umowy, na oficjalnych stronach Urzędu[34], w dniu 8 lipca 2024 r. zamieszczona została informacja o przystąpieniu Gminy Chmielnik do projektu grantowego „Cyberbezpieczny Samorząd”, w ramach którego miał być realizowany projekt o nazwie „Cyberbezpieczna Gmina Chmielnik”. Informacja ta zawierała określenie/tytuł programu, jej zakres rzeczowy, w tym: zakres usług organizacyjno-technologicznych, zakres usług kompetencyjnych, zakup systemów służących zwiększeniu poziomu bezpieczeństwa informacji w jednostkach. Wskazano jednostki organizacyjne uczestniczące w projekcie oraz jego wartość, w tym wkład Unii Europejskiej i wkład Budżetu Państwa. Informacja ta, opatrzona

[32] Maciej Twardowski – Audytor Wiodący Systemu Zarządzania Bezpieczeństwem Informacji wg normy PN-EN ISO/IEC 27001 (Certyfikat TUV Nord Polska Sp. z o.o. z dnia 29 marca 2022 r., ważny do 29 marca 2025 r., Numer rejestracyjny: AC118-AWBI-20220325-C-3838) oraz Mariusz Marek – Audytor Wewnętrzny Systemu Zarządzania Bezpieczeństwem Informacji wg ISO 27001 (Certyfikat nr 1698/05/2013 z dnia 29 maja 2013 r.).

[33] www://funduszeeuropejskie.gov.pl

[34] https://www.chmielnik.com

została znakiem Unii Europejskiej, barwami Rzeczpospolitej Polskiej i znakiem Funduszy Europejskich.

Na tablicy informacyjnej Urzędu umieszczony był plakat o formacie A3, który zawierał informację o przystąpieniu Gminy Chmielnik do projektu grantowego „Cyberbezpieczny Samorząd". Zawierał on także wszystkie informacje zamieszczone na wspomnianej stronie internetowej, w tym także wszystkie ww. wymagane oznaczenia.

Informacja, tożsama w zakresie treści i oznaczeń, znajdowała się również na drzwiach serwerowni Urzędu, w której zainstalowany został serwer zakupiony za środki pozyskane w ramach Programu.

Urząd oznaczył znakami Unii Europejskiej, barwami Rzeczpospolitej Polskiej i znakiem Funduszy Europejskich listy obecności szkoleń pracowników z zakresu bezpieczeństwa informacji i cyberbezpieczeństwa[35]oraz listy obecności szkoleń kadry kierowniczej z zakresu bezpieczeństwa informacji i cyberbezpieczeństwa[36]. Na certyfikatach ukończenia ww. szkoleń zamieszczone zostały wszystkie ww. oznaczenia oraz informacja, że zadanie/Projekt realizowane było z Funduszy Europejskich na Rozwój Cyfrowy2021-2027, w ramach Priorytetu II: Zaawansowane usługi cyfrowe.

Znakami Unii Europejskiej, barwami Rzeczpospolitej Polskiej i znakiem Funduszy Europejskich (wymaganymi Umową) oznaczone zostały faktury zakupów urządzeń, oprogramowania, szkoleń i audytu dokonanych w ramach Projektu[37].

Ww. oznakowaniem opatrzona była korespondencja Burmistrza z kierownikami podmiotów uczestniczących w realizacji Projektu.

(akta kontroli str. 480-484; 485; 486-494; 495-500; 501-505)

Stwierdzone nieprawidłowości

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

1. Urząd nie przeprowadził w 2024 r. corocznego audytu wewnętrznego w zakresie bezpieczeństwa informacji, pomimo iż obowiązek jego przeprowadzenia określony został w § 19 ust. 2 pkt 14, 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. Przepis ten stanowił, iż podmiot realizujący zadania publiczne zapewnia okresowy audyt wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok. Jak wyjaśnił Burmistrz*: (...) miałem świadomość konieczności przeprowadzenia audytu bezpieczeństwa informacji w roku 2024 w Urzędzie Miasta i Gminy w Chmielniku. Jednakże, ze względu na zaangażowanie w przygotowanie i organizację w Mieście i Gminie Chmielnik dwóch akcji wyborczych tj.: wybory władz samorządu terytorialnego na kadencję 2024-2029; radnych do Sejmiku Województwa, radnych do Rady Powiatu w Kielcach, radnych do Rady Miejskiej w Chmielniku, Burmistrza Miasta i Gminy Chmielnik, w tym obsługa administracyjna obwodowych komisji wyborczych, urzędnika wyborczego i Miejskiej*

[35] W dniach 4 i 5 lutego 2025 r.
[36] W dniach 4 i 5 lutego 2025 r.
[37] Faktura 336/03/2025 z dnia 10 marca 2025 r. i Faktura FS 263/03/2025 z dnia 13 marca 2025 r.

Komisji Wyborczej w Chmielniku oraz wybory posłów do Parlamentu Europejskiego, nie udało się przeprowadzić zapytań ofertowych w celu wyboru specjalistycznej firmy do przeprowadzenia w roku 2024 ww. audytu. Ta nieprawidłowość została wyeliminowana i audyt bezpieczeństwa został przeprowadzony z początkiem roku 2025, a kolejny audyt już jest zaplanowany na styczeń 2026 r.

(akta kontroli str. 477)

2. Burmistrz ustnie wyznaczył pracowników odpowiedzialnych za realizację prac dotyczących projektu, nie wskazując w zakresach ich obowiązków zadań związanych z projektem. Było to niezgodne ze Standardem A.3.3. Komunikatu Nr 23 Ministra Finansów Publicznych z dnia 16 grudnia 2009 r. w sprawie standardów kontroli zarządczej dla sektora finansów publicznych[38]. Przepis ten stanowił, że struktura organizacyjna jednostki powinna być dostosowana do aktualnych celów i zadań. Zakres zadań, uprawnień i odpowiedzialności jednostek, poszczególnych komórek organizacyjnych jednostki oraz zakres podległości pracowników powinien być określony w formie pisemnej w sposób przejrzysty i spójny. Aktualny zakres obowiązków, uprawnień i odpowiedzialności powinien być określony dla każdego pracownika. Burmistrz wyjaśnił*: Do przygotowania i realizacji wniosku grantowego „Cyberbezpieczny Samorząd" ustnie wskazałem pracowników Urzędu Miasta i Gminy w Chmielniku (...) gdyż posiadają oni odpowiednie kompetencje, wykształcenie oraz doświadczenie przy realizacji projektów dofinansowanych ze środków Unii Europejskiej i Budżetu Państwa. Ponadto w przydzielonym im zakresom czynności, znajduje się zapis o wykonywaniu innych prac zleconych przez przełożonych. Nie mniej jednak wypełniając zapisy Standardów kontroli zarządczej dla sektora finansów publicznych stanowiących załącznik do Komunikatu nr 23 Ministra Finansów z dnia 16 grudnia 2009 r. w sprawie (poz. 84) A.3. i A.4. dokonano uzupełnienia zakresów czynności ww. pracowników tj. delegowania uprawnień przy realizacji projektu grantowego „Cyberbezpieczny Samorząd".*

(akta kontroli str. 286-287; 288-312; 314-318; 319)

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

NIK nie formułuje uwag.

Wnioski

1. Przeprowadzać coroczny audyt wewnętrzny w zakresie bezpieczeństwa informacji.
2. Określać zadania, uprawnienia i odpowiedzialności pracowników w formie pisemnej, zgodnie ze standardami kontroli zarządczej dla jednostek sektora finansów publicznych.

[38] Dz. Urz. MF Nr 15 poz. 84.

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 w Kielcach. 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 od otrzymania wystąpienia pokontrolnego, o sposobie wykorzystania uwag i 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.

Kielce, 3 lipca 2025 r.

Kontroler

Tadeusz Mikołajewicz

doradca prawny

podpis/podpisano elektronicznie

Najwyższa Izba Kontroli

Delegatura w Kielcach

Dyrektor

Grzegorz Walendzik

podpis/podpisano elektronicznie