WOJEWODA PODKARPACKI
ul. Grunwaldzka 15
35-959 Rzeszów

OA-IV.431.1.2026

Rzeszów, 2026-04-20

Pan
Andrzej Rychel
Burmistrz Miasta i Gminy
Nowa Sarzyna

Na podstawie art. 46 ust. 1 ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej, w związku ze zrealizowaną w dniach 10 i 12 luty 2026 r. u Burmistrza Miasta i Gminy Nowa Sarzyna (Urząd Miasta i Gminy w Nowej Sarzynie, 37-310 Nowa Sarzyna, ul. Mikołaja Kopernika 1) kontrolą problemową[1], której przedmiotem była ocena działania systemów teleinformatycznych używanych do realizacji zadań zleconych z zakresu administracji rządowej z minimalnymi wymaganiami dla systemów teleinformatycznych - przekazuję niniejsze **wystąpienie pokontrolne.**

Kontrolę przeprowadził zespół kontrolerów: Alicja Trygar (starszy inspektor wojewódzki), Tomasz Szmigiel (zastępca kierownika) na podstawie imiennych upoważnień do kontroli (pisma z dnia 03.02.2026 roku, znak OA-IV.431.1.2026) udzielonych przez działającego z upoważnienia Wojewody Podkarpackiego – Dyrektora Wydziału Organizacyjno-Administracyjnego.

Ustalenia kontrolne dokonane zostały w oparciu o stan faktyczny istniejący od 1 stycznia 2025 roku do dnia realizacji czynności kontrolnych włącznie.

W toku kontroli - w oparciu o kontrolowane dokumenty (przy zastosowaniu metody niestatystycznej, losowy dobór próby) - ustalono, iż pracownicy Urzędu Miasta i Gminy w Nowej Sarzynie prawidłowo realizowali swoje zadania. Stwierdzone uchybienia w swych skutkach nie miały charakteru kluczowego (strategicznego) dla funkcjonowania kontrolowanej jednostki. W dużej mierze miały one charakter formalny, przejawiając się odstępstwami od stanu pożądanego, nie powodując jednak negatywnych następstw dla kontrolowanej działalności.

Kontrola nie wykazała okoliczności wskazujących na popełnienie przestępstwa, wykroczenia, naruszenia dyscypliny finansów publicznych lub innych czynów, za które ustawowo przewidziana jest odpowiedzialność prawna.

[1] W oparciu o zatwierdzony w dniu 7 stycznia 2026 r. „Plan zewnętrznej działalności kontrolnej Podkarpackiego Urzędu Wojewódzkiego w Rzeszowie na 2026 rok").

W oparciu o poczynione ustalenia, stosownie do skali ocen przyjętej w „Programie kontroli problemowej realizowanej u Burmistrza Miasta i Gminy Nowa Sarzyna”[2], **działalność w ww. zakresie należy ocenić pozytywnie z uchybieniami**.

Na podstawie analizy dokumentacji źródłowej zespół kontrolny sformułował następującą ocenę kontrolowanych obszarów:

1. Wymiana informacji w postaci elektronicznej, w tym współpraca z innymi systemami/rejestrami informatycznymi i wspomaganie świadczenia usług drogą elektroniczną – pozytywnie;
2. Wdrożenie systemu zarządzania bezpieczeństwem informacji w systemach teleinformatycznych – pozytywnie z uchybieniami;
3. Dostosowanie systemów informatycznych do standardu WCAG 2.0 – pozytywnie.

Kontekst organizacyjny

Funkcję kierownika w Urzędzie Miasta i Gminy Nowa Sarzyna pełnił Burmistrz: Pan Andrzej Rychel.

Funkcję Inspektora Ochrony Danych (IOD) powierzono wykonawcy zewnętrznemu Panu Danielowi Panek, na podstawie umowy na świadczenie kompleksowej usługi (outsorcing) w zakresie RODO i SZBI oraz pełnienia funkcji Inspektora ochrony danych osobowych i Pełnomocnika ds. SZBI z dnia 15 stycznia 2026 roku z MP LEGAL MIELECH, PANEK I WSPÓLNICY Sp. Komandytowa oraz Zarządzenia nr 5/2026 Burmistrza Miasta i Gminy Nowa Sarzyna.

Wsparcie informatyczne zapewnione było przez dwóch informatyków, pracowników Urzędu Miasta i Gminy. Pod ich opieką znajdowały się środowiska sprzętowo-programowe, sieć lokalna, serwerownie, systemy i aplikacje centralne oraz własne, usprawniające pracę pracownikom Urzędu Miasta i Gminy w Nowej Sarzynie i jednostek podległych.

Funkcja Administratora Systemów Informatycznych (ASI) na podstawie zakresu obowiązków została powierzona osobie zatrudnionej na stanowisku kierownika referatu ds. Informatyki. Nie uzyskano informacji o wyznaczeniu osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa Zgłoszenia takiej osoby należy dokonać jak najszybciej do CSIRT NASK.

W okresie objętym kontrolą w Urzędzie Miasta i Gminy Nowa Sarzyna funkcjonowały systemy teleinformatyczne własne - zakupione przez urząd oraz centralne m.in.:

a) systemy centralne:

[2] Stosownie do § 37 ust. 2 zarządzenia Nr 1/14 Wojewody Podkarpackiego z dnia 2 stycznia 2014 r. w sprawie szczegółowych warunków i trybu prowadzenia kontroli (z późn. zm.) w ramach realizacji czynności kontrolnych stosowana była 4-stopniowa skala ocen, tj. ocena pozytywna, pozytywna z uchybieniami, pozytywna z nieprawidłowościami, negatywna.

- System Rejestrów Państwowych (SRP) - dane o obywatelach zgromadzonych w poszczególnych rejestrach (rejestr PESEL, rejestr Dowodów Osobistych, rejestr Stanu Cywilnego);
- Elektroniczna Platforma Usług Administracji Publicznej (ePUAP);
- Centralna Ewidencja Działalności Gospodarczej (CEIDG);
- eDoręczenia.

b) systemy własne lub zakupione:
- EWIDENCJA.NET – Lokalny Rejestr Mieszkańców i obsługi wyborów samorządowych wraz z modułem odpowiedzialnym za transmisję danych z SRP do LRM – firmy Clanet sp. z o.o.,
- Ewidencja zwrotów podatku akcyzowego – w ramach zintegrowanego systemu informatycznego „Sprawny Urząd" - firmy Biuro Usług Komputerowych SOFTRES sp. z o.o.,
- Proton - Elektroniczny Obieg Dokumentów firmy Sputnik wdrożony w ramach projektu PSeAP (Podkarpacki System E-Administracji Publicznej) – obecnie serwis firma Nefeni,
- poczta elektroniczna,
- strona www,
- BIP.

Podstawą oceny są następujące ustalenia kontroli:

1. Wymiana informacji w postaci elektronicznej, w tym współpraca z innymi systemami/rejestrami informatycznymi i wspomaganie świadczenia usług drogą elektroniczną

1.1. Usługi elektroniczne

Urząd Miasta i Gminy Nowa Sarzyna udostępniał elektroniczną skrzynkę podawczą (dalej: ESP) na platformie ePUAP oraz adres do eDoręczeń co umożliwiało wymianę danych i świadczenie usług elektronicznych.

Na stronie www Urzędu oraz na BIP znajdowała się informacja o adresie **elektronicznej skrzynki podawczej** ESP na ePUAP oraz adres eDoręczeń, co ułatwiało klientom składanie pism ogólnych, skarg czy wniosków drogą elektroniczną.

Udostępnienie ESP i eDoręczeń na stronie/BIP spełnia minimalne wymogi Ustawy o informatyzacji, umożliwiając interakcje bez wizyty w urzędzie.

1.2. Współpraca systemów teleinformatycznych z innymi systemami

Pracownicy Urzędu Miasta i Gminy Nowa Sarzyna mieli dostęp do rejestrów publicznych, takich jak SRP Źródło i CEIDG, co umożliwiało efektywne przetwarzanie danych. System EWIDENCJA.NET integrował się z SRP poprzez moduł ImportSRP, automatyzując import danych do Lokalnego Rejestru Mieszkańców i minimalizując błędy ręcznego wprowadzania.

Dostęp do SRP Źródło (rejestr PESEL, dowody, stan cywilny) i CEIDG pozwalał na weryfikację i aktualizację danych w czasie rzeczywistym, zgodnie z wymogami interoperacyjności z Ustawy o informatyzacji.

1.3. Obieg dokumentów

W Urzędzie Miasta i Gminy Nowa Sarzyna był wdrożony System Elektronicznego Zarządzania Dokumentacją PROTON umożliwiający zarządzanie dokumentami i wykonywanie czynności kancelaryjnych. Obecnie każda wpływająca korespondencja była rejestrowana i dekretowana w systemie PROTON.

System umożliwiał cyfrowy obieg dokumentów, automatyzując rejestrację każdej korespondencji wpływowej.

2. Wdrożenie systemu zarządzania bezpieczeństwem informacji w systemach teleinformatycznych

2.1. Dokumenty z zakresu bezpieczeństwa informacji

Zgodnie z § 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, zwanego dalej Rozporządzeniem KRI - podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność.

Wymaga to opracowania dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), w tym szeregu regulacji wewnętrznych oraz zapewnienia aktualizacji tych regulacji w zakresie dotyczącym zmieniającego się otoczenia. Dokumentacja jest warunkiem niezbędnym dla możliwości skutecznego zarządzania bezpieczeństwem informacji.

W Urzędzie Miasta i Gminy Nowa Sarzyna ustanowiono Systemu Zarządzania Bezpieczeństwem Informacji na podstawie Zarządzenia Nr 34/2025 z 24 kwietnia 2025 roku, wraz kompleksową dokumentacją (12 załączników) opracowaną zewnętrznie przez firmę SEQMA Security Management, pod nadzorem Pełnomocnika Systemu Zarządzania Bezpieczeństwem Informacji.

Kluczowe dokumenty stanowiące SZBI to:

- System Zarządzania Bezpieczeństwem Informacji ustanowiony Zarządzeniem Nr 34/2025 Burmistrza Miasta i Gminy Nowa Sarzyna z dnia 24 kwietnia 2025 roku;
- Polityka Bezpieczeństwa Informacji (załącznik nr 1 do Zarządzenia);
- Procedura Zarządzania Ryzykiem (załącznik nr 2 do Zarządzenia);
- Procedura Zarządzania Incydentami (załącznik nr 3 do Zarządzenia);
- Procedura Klasyfikacji Informacji (załącznik nr 4 do Zarządzenia);
- Procedura Zarządzania Podatnościami i Poprawkami (załącznik nr 5 do Zarządzenia);
- Procedura Zarządzania Systemem Informatycznym (załącznik nr 6 do Zarządzenia);
- Procedura Zarządzania Bezpieczeństwem w Relacjach z Dostawcami Zewnętrznymi (załącznik nr 7 do Zarządzenia);
- Procedura Zarządzania Bezpieczeństwem Fizycznym (załącznik nr 8 do Zarządzenia);

- Procedura Audytu Wewnętrznego (załącznik nr 9 do Zarządzenia);
- Procedura Zarządzania Bezpieczeństwem w Procesach Kadrowych (załącznik nr 10 do Zarządzenia);
- Polityka Ciągłości Działania (załącznik nr 11 do Zarządzenia);
- Procedura Nadzoru nad Dokumentacją (załącznik nr 12 do Zarządzenia);
- Regulamin Organizacji i Przetwarzania Danych Osobowych w Urzędzie Miasta i Gminy w Nowej Sarzynie wraz z załącznikami, stanowiący Załącznik do zarządzenia Nr 71/2018 ;
- Zarządzenie Nr 119/2024 Burmistrza Miasta i Gminy Nowa Sarzyna z dnia 12 listopada 2024 r. w sprawie programów dopuszczonych do używania na komputerach Urzędu Miasta i Gminy w Nowej Sarzynie.

2.2. Analiza zagrożeń związanych z przetwarzaniem informacji

Wymogiem skuteczności SZBI jest przeprowadzanie okresowych analiz ryzyka.
Analiza zagrożeń w ramach SZBI wymaga ocen ryzyka utraty poufności, integralności lub dostępności informacji, obejmujących identyfikację, szacowanie, plan i deklarację zabezpieczeń zgodnie z §19 Rozporządzenia KRI.
W Urzędzie Miasta i Gminy Nowa Sarzyna zarządzanie ryzykiem opierało się na Procedurze zarządzania ryzykiem i jego ocenie w 2025 roku, realizowanej przez Zespół ds. Zarządzania Ryzykiem, co spełniało wymogi. Należy jednak systematycznie dokonywać weryfikacji aktualności i wdrożenia działań.

Wyniki analizy ryzyka mają wpływać na decyzje odnośnie podniesienia bezpieczeństwa funkcjonowania jednostki, np. poprzez wzmocnienie kontroli zarządczej, system zastępstw na strategicznych stanowiskach, szkolenia pracowników w stosunku do zagrożonych obszarów eksploatacji systemów informatycznych. Dokonując analizy ryzyka warto wziąć pod uwagę utratę integralności, dostępności lub poufności wszystkich informacji.

2.3. Inwentaryzacja sprzętu i oprogramowania informatycznego

Zarządzanie infrastrukturą informatyczną wymaga utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację. W praktyce oznacza to zapewnienie funkcjonowania rejestru zasobów teleinformatycznych zawierającego informacje o wszystkich zidentyfikowanych aktywach informatycznych, w tym: szczegółowe dane o urządzeniach technicznych, parametrach, aktualnej konfiguracji, oprogramowaniu, środkach komunikacji, a także rodzaju relacji między elementami konfiguracji oraz użytkownikiem. Inwentaryzacja sprzętu i oprogramowania informatycznego jest kluczowym elementem zarządzania infrastrukturą w ramach SZBI, wymagając aktualnego rejestru zasobów z danymi o rodzajach, konfiguracjach, relacjach i użytkownikach zgodnie z §19 ust. 2 pkt 2 Rozporządzenia KRI.
W UMiG Nowa Sarzyna regulacje wewnętrzne częściowo przewidywały utrzymywanie aktualności inwentaryzacji sprzętu, co do rodzaju i konfiguracji, jednak bez wskazania sposobu inwentaryzacji. Ewidencjonowanie odbywało się przez narzędzie eAuditor oraz ESET Protect.
eAuditor rejestruje podzespoły i oprogramowanie, a ESET Protect identyfikuje urządzenia i aplikacje w sieci.

Sposób zabezpieczenia systemu informatycznego został opisany w Procedurze Zarządzania Systemem Informatycznym (załącznik nr 6 do Zarządzenia 34/2025).

2.4. Zarządzanie uprawnieniami do pracy w systemach informatycznych

Istotnym elementem polityki bezpieczeństwa informacji jest zarządzanie dostępem do systemów teleinformatycznych przetwarzających informacje. Zarządzanie dostępem ma zapewnić, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków, a w przypadku zmiany zadań następuje również zmiana ich uprawnień.

Zarządzanie uprawnieniami dostępu w Urzędzie Miasta i Gminy Nowa Sarzyna, regulowała ogólnie Procedura Zarządzania Systemem Informatycznym (załącznik nr 6 do Zarządzenia 34/2025).

Pracownicy uzyskiwali dostęp do zasobów informatycznych po przyznaniu zakresu obowiązków i nadaniu unikalnego identyfikatora i hasła w systemie teleinformatycznym.

W przypadku konieczności zmiany i odbioru uprawnień w systemach informatycznych informacja o danym użytkowniku przekazywana była przy pomocy wniosku o nadanie/zmianę/odebranie uprawnień w systemie informatycznym podpisanym przez bezpośredniego przełożonego. Monitorowanie dostępu odbywało się na bieżąco, co spełniało wymogi rozliczalności i audytu.

Zakres uprawnień użytkowników badanych systemów uniemożliwiał wykonywanie przez nich działań zastrzeżonych dla administratorów systemów. Podczas logowania przez informatyków na niektóre urządzenia było używane wspólne konto administratora, bez separacji ról administratora od kont codziennego użytku.

W okresie objętym badaniem konta byłych pracowników Urzędu były sukcesywnie blokowane w systemach informatycznych. Na bieżąco odbywało się monitorowanie dostępu do zasobów informatycznych zgodnie z wymaganiami § 19 ust. 2 pkt 4 rozporządzenia KRI. W ramach dokumentacji SZBI został przygotowany do wprowadzenia wzór Rejestru uprawnień użytkowników.

2.5. Szkolenia pracowników zaangażowanych w proces przetwarzania informacji

Istotnym elementem SZBI jest świadomość pracowników współodpowiedzialności za bezpieczeństwo informacji, zagrożeń i konsekwencji zaistnienia incydentów związanych z naruszeniem bezpieczeństwa.

Szkolenia z zakresu bezpieczeństwa informacji powinny obejmować wszystkie osoby uczestniczące w procesie przetwarzania informacji oraz dostarczać aktualnej wiedzy o nowych zagrożeniach, adekwatnych zabezpieczeniach oraz skutkach ewentualnych incydentów związanych z bezpieczeństwem informacji.

Dokumentacja wewnętrzna Urzędu Miasta w Nowej Sarzynie regulowała zakres podnoszenia świadomości pracowników poprzez szkolenia wstępne i cykliczne z zakresu bezpieczeństwa (Procedura Zarządzania Bezpieczeństwem w Procesach Kadrowych - załącznik nr 10 do Zarządzenia 34/2025) oraz Regulamin Organizacji i Przetwarzania Danych Osobowych). Kontrolującym przedstawiono informację o szkoleniach pracowników zrealizowanych w ramach projektu Cyberbezpieczny Samorząd w marcu 2025 roku, z zakresu cyberbezpieczeństwa i SZBI.

2.6. Praca na odległość i mobilne przetwarzanie danych

Wobec możliwości technicznych związanych z telepracą (pracą poza siedzibą podmiotu publicznego z wykorzystaniem urządzeń mobilnych takich jak laptopy, tablety, smartfony) pojawiają się nowe zagrożenia bezpieczeństwa informacji.

Zarządzanie bezpieczeństwem urządzeń mobilnych jest istotnym elementem SZBI, wymagającym regulacji zasad ochrony przed kradzieżą, nieautoryzowanym dostępem i zagrożeniami sieci Wi-Fi, szczególnie w kontekście przetwarzania danych publicznych. Konieczne jest więc opisanie zasad określających sposoby zabezpieczenia urządzeń mobilnych i danych w nich zawartych.

Ogólne zasady zarządzania bezpieczną pracą na komputerach przenośnych i sposoby zabezpieczenia tych urządzeń były zawarte w Podstawowych Zasadach Bezpieczeństwa, Rozdział: Bezpieczna praca zdalna (załącznik do Polityki Bezpieczeństwa Informacji).

Niemniej praca zdalna nie występowała. Pracownicy nie wynosili sprzętu poza siedzibę Urzędu, co eliminuje ryzyka zewnętrzne jak kradzież czy publiczne sieci, minimalizując potrzebę zaawansowanych środków.

2.7. Serwis sprzętu informatycznego i oprogramowania

W przypadku systemów informatycznych o znaczeniu istotnym dla jednostki niezbędne jest objęcie tych systemów (w zakresie oprogramowania użytkowego, systemowego, sprzętu i rozwiązań telekomunikacyjnych) stosownymi umowami serwisowymi, gwarantującymi odpowiednio szybkie uruchomienie pracy systemu w przypadku awarii. Umowy powinny posiadać klauzule prawne zabezpieczające ochronę informacji w przypadku wejścia w ich posiadanie przez firmy serwisujące.

Serwis sprzętu i oprogramowania w systemach kluczowych dla jednostki publicznej wymaga umów z SLA, klauzulami poufności i regulacjami dostępu, aby zapewnić szybką reakcję na awarie i ochronę danych.

Procedura Zarządzania Bezpieczeństwem w Relacjach z Dostawcami Zewnętrznymi (załącznik nr 7 do Zarządzenia 34/2025) określała ramy współpracy oraz konieczność podpisania z Dostawcami umowy o zachowaniu poufności w przypadku dostępu do informacji chronionych.

Procedura wskazywała również, że udzielanie dostępu fizycznego i logicznego do zasobów teleinformatycznych także należy określić w zawieranych umowach z Dostawcami.

Niemniej w sprawdzanych umowach o asystę i opiekę autorską lub serwisową z firmami zewnętrznymi powyższe zapisy Procedury nie były stosowane. Nie we wszystkich umowach z wykonawcami zostały określone zasady i czas dostępu, zwłaszcza zdalnego oraz nie określono SLA (Service Level Agreement), czyli gwarantowanego poziomu świadczenia usług oraz czasu i sposobów reakcji na zgłaszane problemy (udostępniono umowę licencyjną z Biurem Usług komputerowych SOFTRES sp. z o.o. – 2025 r.) na Zintegrowany System Informatyczny „Sprawny Urząd”.

W przypadku tego systemu nie została przedstawiona umowa powierzenia przetwarzania danych osobowych.

2.8. Procedury zgłaszania incydentów naruszenia bezpieczeństwa informacji

Zasady postępowania w przypadku wystąpienia zdarzenia związanego z bezpieczeństwem informacji oraz słabością systemów informacyjnych zostały określone w Procedurze

Zarządzania Incydentami ((załącznik nr 3 do Zarządzenia 34/2025). Procedura umożliwiała szybkie i najbardziej efektywne podjęcie działań korygujących przez wskazanie m.in. osób odpowiedzialnych i kanałów zgłaszania incydentu.
Rejestr incydentów i działań korygujących w Urzędzie Miasta i Gminy Nowa Sarzyna zawierał wpis z 2025 roku. Incydent ransomware związany był z zaszyfrowaniem danych w dniu 27.01.2025 r. Ten atak na infrastrukturę, spowodował konieczność uruchomienia nowych serwerów i przywrócenia danych z kopii zapasowych. Skuteczne przywrócenie wskazuje na działające kopie zapasowe, ale incydent podkreśla potrzebę testów procedur.

2.9. Audyt wewnętrzny z zakresu bezpieczeństwa informacji

Audyt z zakresu bezpieczeństwa informacji nie rzadziej niż raz na rok, w rozumieniu § 19 ust. 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 w Urzędzie Miasta i Gminy był wykonany w 2025 roku pn. Analiza Bezpieczeństwa.

W obowiązującej dokumentacji zawarte zostały ogólne zasady w Procedurze Audytu Wewnętrznego (załącznik nr 9 do Zarządzenia 34/2025) dotyczące konieczności audytowania i sprawdzeń w zakresie bezpieczeństwa informacji. Warto zwrócić uwagę, że celem audytów jest ewentualne ujawnienie słabości systemów, a także słabości zabezpieczeń lub ich stosowania.

Wyniki audytu powinny wpłynąć na doskonalenie tych zabezpieczeń, sposobów ich stosowania, a także na program szkoleń z bezpieczeństwa informacji.

2.10. Kopie zapasowe

Wykonywanie kopii zapasowych zapobiega utracie informacji w wyniku awarii.
Kopie powinny być właściwie tworzone, przechowywane i testowane.
W okresie objętym kontrolą w zakresie wykonywania kopii zapasowych w Urzędzie Miasta i Gminy Nowa Sarzyna obowiązywały wymagania określone w Procedurze Zarządzania Systemem Informatycznym, Rozdział: Kopia bezpieczeństwa (załącznik nr 6 do Zarządzenia 34/2025).
Kopie folderów, maszyn wirtualnych były wykonywane według harmonogramu ustalonego przez ASI oraz przechowywane na serwerze.
Kopie zapasowe były przechowywane w innym miejscu niż serwerownia.
Wykonywanie odtworzenia systemów z kopii zapasowych było testowane oraz odbywało się w razie potrzeby.

2.11. Projektowanie, wdrażanie i eksploatacja systemów teleinformatycznych

W Urzędzie Miasta i Gminy Nowa Sarzyna proces administrowania technicznego i monitorowania określonych obszarów systemów, aplikacji, danych, infrastruktury sieciowej i stacji roboczych był wykonywany przez informatyków, co pozwalało na przewidywanie i zapobieganie ewentualnym problemom związanym z awariami, wyciekami bądź utratą danych.

Systemy centralne, w ramach kontroli podlegały badaniu w ograniczonym zakresie, ze względu na centralne polityki, procedury, wdrożenia i dostępy.

Wybrane systemy własne lub zakupione podlegały sprawdzeniu w zakresie zgodności z rozdz. IV 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.
Najistotniejsze systemy były objęte opieką na podstawie umów opieki autorskiej lub serwisowej.
Pracownicy nie zgłaszali problemów z funkcjonalnością badanych systemów.

2.12. Zabezpieczenia techniczno-organizacyjne dostępu do informacji

Celem zabezpieczeń jest uzyskanie ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, a także np. kradzieżą środków przetwarzania informacji. Zastosowane zabezpieczenia powinny być adekwatne do poziomu ryzyka wynikającego z analizy ryzyka bezpieczeństwa informacji.
Szereg zabezpieczeń techniczno-organizacyjnych dostępu do informacji opisano w Procedurze Zarządzania bezpieczeństwem fizycznym.
Ochrona informacji przed kradzieżą, nieautoryzowanym dostępem, uszkodzeniami czy zakłóceniami w UMiG Nowa Sarzyna realizowana była poprzez wielowarstwowe zabezpieczenia logiczne, fizyczne i monitorujące, zgodne z wymogami SZBI i KRI §19:
a) zabezpieczenie dostępu do informacji poprzez wymuszone logowanie użytkowników za pomocą kart lub poprzez podanie unikalnego hasła do badanych systemów;
b) kontrolę i monitorowanie zabezpieczenia fizycznego dostępu do pomieszczeń oraz zabezpieczenie budynku w system alarmowy;
c) podejmowanie czynności zmierzających do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji poprzez monitorowanie infrastruktury teleinformatycznej, kontrolę wejść i wyjść do pomieszczeń serwerowni uprawnionych osób;
d) zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji poprzez system autoryzacji dostępu do systemów operacyjnych, sieci i aplikacji, stosowania systemów antywirusowych i antyspamowych.

Urząd Miasta i Gminy Nowa Sarzyna posiadał pomieszczenia biurowe zlokalizowane w jednym budynku.
Obiekt był objęty systemem alarmowym ochrony fizycznej. Do otwierania głównych drzwi budynku oraz rozbrajania systemu alarmowego byli upoważnieni wyznaczeni pracownicy.
Urząd dysponował jedną główną serwerownią, która znajdowała się w pomieszczeniu przeznaczonym na ten cel. Dostęp do serwerowni był ograniczony i możliwy jedynie dla upoważnionych pracowników urzędu. Ważnym elementem ochrony było asystowanie osobom wchodzącym i wykonującym prace serwisowe.
W serwerowni występowało monitorowanie niektórych parametrów środowiskowych (temperatury, ppoż). Pomieszczenie było klimatyzowane.

Drzwi do serwerowni były wzmocnione.
Bazy danych z kopiami były umieszczone w innej lokalizacji.
W serwerowni znajdował się UPS, który podtrzymywał pracę serwera i urządzeń sieciowych.
W pomieszczeniu nie były przechowywane materiały łatwopalne.
Podstawowe urządzenie infrastruktury informatycznej: serwer, urządzenia sieciowe były zakupione w ramach Projektu.
Monitorowanie ruchu sieciowego wchodzącego i wychodzącego realizowane było przez maszynę sprzętową UTM Fortigate, zakupiony w ramach projektu „Cyberbezpieczny Samorząd" oraz oprogramowanie FortiAnalyzer.
Wszystkie komputery oraz urządzenie sieciowe posiadały oprogramowanie systemowe zaktualizowane do wersji posiadających wsparcie producenta.

2.13. Zabezpieczenia techniczno-organizacyjne systemów informatycznych

Zabezpieczenia techniczno-organizacyjne systemów informatycznych w UMiG Nowa Sarzyna wynikały z analizy ryzyka (maj 2025 r.) i były wdrażane zgodnie z planem postępowania, obejmując aktualizacje oprogramowania oraz środki minimalizujące awarie i nieautoryzowany dostęp.
Poziom bezpieczeństwa systemów teleinformatycznych zapewniono poprzez:
a) aktualizację oprogramowania oraz redukcję ryzyk wynikających z wykorzystywania opublikowanych podatności technicznych systemów teleinformatycznych (w tym oprogramowania antywirusowego);
b) minimalizację ryzyka utraty informacji w wyniku awarii oraz ochronę przed błędami, utratą i nieuprawnioną modyfikacją, a także zapewnienie bezpieczeństwa plików systemowych, zastosowania systemu kopii zapasowych, systemu kontroli dostępu do zasobów informatycznych, systemu monitorowania funkcjonowania systemów teleinformatycznych i sieci.
Była wdrożona usługa katalogowa Active Directory, która pozwalała na zarządzanie tożsamościami i relacjami w sieci, przez co umożliwiała sprawniejszą kontrolę nad całą siecią oraz użytkownikami.

2.14. Rozliczalność działań w systemach informatycznych

Przetwarzanie informacji w systemach teleinformatycznych urzędów publicznych wymaga obowiązkowego logowania działań użytkowników i administratorów, co zapewnia rozliczalność i wykrywanie incydentów zgodnie z polskimi regulacjami, takimi jak RODO (art. 30), KRI oraz Krajowymi Ramami Bezpieczeństwa Cybernetycznego.
Logi muszą rejestrować co najmniej: tożsamość użytkownika, datę, godzinę i rodzaj operacji (kto, kiedy, co), z przeglądem okresowym w celu identyfikacji anomalii oraz przechowywaniem minimum 2 lata w sposób chroniący przed nieautoryzowanym dostępem. Świadomość użytkowników o pełnej traceability podnosi dyscyplinę bezpieczeństwa.

Urząd nie posiadał regulacji wewnętrznych określających politykę logów i rozliczalności. Systemy użytkowe miały jednak udokumentowaną rozliczalność (np. logi w systemach jak Windows Server czy firewalle). Jednak zauważono podczas logowania na niektóre urządzenia **w**spólne konto administratora wśród informatyków. Utworzenie

indywidualnych kont administratora dla każdego informatyka jest kluczowe dla zapewnienia rozliczalności działań w systemie IT urzędu.

W ramach projektu zostało zakupione oprogramowanie FortiAnalyzer służące do centralnego zarządzania logami, analizy zagrożeń i raportowania.

3. Zapewnienie dostępności informacji zawartych na stronie BIP oraz internetowej urzędów dla osób niepełnosprawnych

W udostępnianych systemach teleinformatycznych powinny zostać zastosowane rozwiązania techniczne umożliwiające osobom niedosłyszącym lub niedowidzącym zapoznanie z treścią informacji m.in. poprzez powiększenie czcionki, obrazu, zmianę kontrastu, czy też odsłuchanie wyświetlanej treści – zgodnie ze standardem WCAG 2.0.

Zapewnienie dostępności stron BIP i internetowych urzędów dla osób niepełnosprawnych jest obowiązkowe zgodnie z polską Ustawą o dostępności cyfrowej z 4 kwietnia 2019 r., która wymaga zgodności z WCAG 2.1 (lub nowszymi wersjami jak 2.2 od 2025 r.) na poziomie AA. Strony muszą umożliwiać powiększanie czcionki, zmianę kontrastu i odczytywanie treści przez czytniki ekranu, szczególnie dla BIP, danych kontaktowych, formularzy i deklaracji dostępności.
Analizując poprawność kodu strony www poprzez polski walidator dostępny pod adresem: https://validator.utilitia.pl/ badana strona uzyskała wynik 5,0 pkt na 10 możliwych.

Ww. ustalenia, w tym ocena kontrolowanej działalności, zostały udokumentowane w aktach kontroli, na które składają się kopie dokumentów oraz dokumenty przesłane przez urząd drogą elektroniczną.

Przy czym do ww. ustaleń kontrolnych (przekazanych do wiadomości w dniu 31 marca 2026 r.) przysługiwało Panu, na podstawie ww. ustawy o kontroli w administracji rządowej, prawo zgłoszenia umotywowanych pisemnych zastrzeżeń, z którego Pan nie skorzystał.

W związku z powyższym, stosownie do art. 46 ust. 1 ustawy o kontroli w administracji rządowej, sporządzono niniejsze wystąpienie pokontrolne, obejmujące m.in. treść projektu wystąpienia pokontrolnego.

Zgodnie z wymogami § 19 ust. 1-14 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:

1. Dokonać analizy wszystkich umów serwisowych ze stronami trzecimi i w razie potrzeby uzupełnić je o zapisy gwarantujące odpowiedni poziom bezpieczeństwa informacji, w tym określić SLA (Service Level Agreement), czyli gwarantowany poziom świadczenia usług, ciągłość działania, zasady i czas dostępu zdalnego, czas i sposób reakcji na zgłaszane problemy oraz prowadzić nadzór nad wykonawcami w zakresie zgodności z regulacjami i ustaloną Procedurą Zarządzania Bezpieczeństwem w Relacjach z Dostawcami Zewnętrznymi.
2. Niezbędne jest wdrożenie ustanowionej dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji. Do tego potrzebne jest aktywne zaangażowanie

wszystkich pracowników urzędu – nawet jeśli całość koordynuje zewnętrzny Pełnomocnik SZBI. Dokumentację należy połączyć z obowiązującym w urzędzie Regulaminem Przetwarzania Danych Osobowych, tak aby stał się on częścią SZBI.

3. Zgodnie z ustawą o krajowym systemie cyberbezpieczeństwa obowiązkowo zgłosić osoby kontaktowe do CSIRT NASK przez Urząd Miasta i Gminy jako jednostkę samorządu terytorialnego.
4. W celu zapewnienia rozliczalności i możliwości przypisania działań do konkretnej osoby, należy utworzyć indywidualne konta administratorów z separacją ról (admin oraz codzienne konto).

O sposobie wykonania powyższych wniosków pokontrolnych, bądź działaniach podjętych w celu ich realizacji, oczekuję od Pana odpowiedzi na piśmie, w terminie **21 dni** od dnia otrzymania niniejszego wystąpienia.

WOJEWODA PODKARPACKI

(-)

Teresa Kubas-Hul

(Podpisane bezpiecznym podpisem elektronicznym)