WOJEWODA PODKARPACKI
ul. Grunwaldzka 15
35-959 Rzeszów

OA-IV.431.2.2026

Rzeszów, 2026-07-02

Pan

Marek Rączka
Wójt Gminy
Żyraków

Na podstawie art. 46 ust. 1 ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej, w związku ze zrealizowaną w dniach 28 i 29 kwietnia 2026 r. u Wójta Gminy Żyraków 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 22.04.2026 r., znak OA-IV.431.2.2026) 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 Gminy Żyraków 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 Wójta Gminy Żyraków”[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 Urzędu Gminy Żyraków pełnił Wójt Gminy Żyraków – Pan Marek Rączka.

Funkcję Inspektora Ochrony Danych (IOD) pełnił Pan Adam Pryga, pracownik Urzędu Gminy, wyznaczony na podstawie Zarządzenia nr 59/2018 Wójta Gminy Żyraków z dnia 25 maja 2018 r. w sprawie wyznaczenia Inspektora Ochrony Danych w Urzędzie Gminy w Żyrakowie oraz jednostkach organizacyjnych Gminy Żyraków.

Obsługa informatyczna była realizowana przez pracownika Urzędu Gminy, pełniącego jednocześnie funkcję Administratora Systemów Informatycznych (ASI), zgodnie z przypisanym zakresem obowiązków. Do jego zadań należało w szczególności utrzymanie środowiska sprzętowo-programowego, sieci lokalnej, infrastruktury serwerowej oraz systemów i aplikacji – zarówno centralnych, jak i lokalnych – wspierających działalność Urzędu oraz jednostek organizacyjnych Gminy.

Zgłoszenia osoby kontaktowej do CSIRT NASK – Pana Krzysztofa Lipińskiego – dokonano w dniu 23 lutego 2021 r.

Ponadto Zarządzeniem nr AO.0050.134.2025 Wójta Gminy Żyraków z dnia 31 grudnia 2025 r. wyznaczono osobę odpowiedzialną za kontakty z CSIRT w zakresie obsługi incydentów bezpieczeństwa – Pana Krzysztofa Lipińskiego.

Systemy teleinformatyczne

W Urzędzie Gminy Żyraków funkcjonowały zarówno systemy teleinformatyczne centralne, jak i systemy własne lub zakupione, w szczególności:

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), obejmujący m.in. rejestr PESEL, rejestr dowodów osobistych oraz rejestr stanu cywilnego,
- Elektroniczna Platforma Usług Administracji Publicznej (ePUAP),
- Centralna Ewidencja i Informacja o Działalności Gospodarczej (CEIDG),
- system e-Doręczeń;

b) systemy własne lub zakupione:

- Technika IT PB_EWID3 – system do prowadzenia Rejestru Mieszkańców oraz obsługi wyborów samorządowych, wraz z modułem odpowiedzialnym za transmisję danych z Systemu Rejestrów Państwowych do Rejestru Mieszkańców (producent: TECHNIKA IT Sp. z o.o.),
- moduł ewidencji zwrotów podatku akcyzowego w ramach zintegrowanego systemu informatycznego „Sprawny Urząd" (producent: Biuro Usług Komputerowych SOFTRES Sp. z o.o.),
- system poczty elektronicznej,
- strona internetowa Urzędu,
- Biuletyn Informacji Publicznej (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 Gminy Żyraków udostępniał elektroniczną skrzynkę podawczą (dalej: ESP) na platformie ePUAP oraz adres do e-Doręczeń, co umożliwiało wymianę danych i świadczenie usług drogą elektroniczną.

Na stronie internetowej Urzędu oraz w Biuletynie Informacji Publicznej (BIP) zamieszczono informacje o adresie ESP na platformie ePUAP oraz adresie do e-Doręczeń, co ułatwiało interesantom składanie pism ogólnych, skarg i wniosków w formie elektronicznej.

1.2. Współpraca systemów teleinformatycznych z innymi systemami

Pracownicy Urzędu Gminy Żyraków posiadali dostęp do rejestrów publicznych, w szczególności do Systemu Rejestrów Państwowych (SRP – Źródło) oraz Centralnej Ewidencji i Informacji o Działalności Gospodarczej (CEIDG), co umożliwiało efektywne przetwarzanie danych.

System Technika IT PB_EWID3 integrował się z SRP poprzez mechanizm subskrypcji, automatyzując import danych do Rejestru Mieszkańców oraz ograniczając ryzyko błędów wynikających z ręcznego wprowadzania danych.

Dostęp do SRP (rejestr PESEL, rejestr dowodów osobistych, rejestr stanu cywilnego) oraz CEIDG umożliwiał weryfikację i aktualizację danych w czasie zbliżonym do rzeczywistego, zgodnie z wymaganiami interoperacyjności określonymi w przepisach o informatyzacji działalności podmiotów realizujących zadania publiczne.

1.3. Obieg dokumentów

W Urzędzie Gminy Żyraków nie było wdrożonego Systemu Elektronicznego Zarządzania Dokumentacją umożliwiający zarządzanie dokumentami i wykonywanie czynności kancelaryjnych w postaci elektronicznej.

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.

Spełnienie powyższych wymagań wiąże się z koniecznością opracowania i utrzymywania dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), obejmującej regulacje wewnętrzne oraz ich bieżącą aktualizację w związku ze zmieniającym się otoczeniem organizacyjnym i technologicznym. Dokumentacja ta stanowi podstawę skutecznego zarządzania bezpieczeństwem informacji.

W Urzędzie Gminy Żyraków System Zarządzania Bezpieczeństwem Informacji został ustanowiony na podstawie Zarządzenia nr AO.0050.125.2025 Wójta Gminy Żyraków z dnia 2 grudnia 2025 r. wraz z kompleksową dokumentacją obejmującą załączniki.

Kluczowe dokumenty składające się na SZBI:

- Polityka Bezpieczeństwa Informacji,
- Polityka Ochrony Danych Osobowych (załącznik nr 1 do Polityki Bezpieczeństwa Informacji),
- Polityka Zarządzania Ciągłością Działania wraz z zestawem Planów Ciągłości Działania (załącznik nr 2 do Polityki Bezpieczeństwa Informacji),
- Polityka Zarządzania Incydentami Cyberbezpieczeństwa (załącznik nr 3 do Polityki Bezpieczeństwa Informacji),
- Polityka Zarządzania Systemami Teleinformatycznymi – PZST, (załącznik nr 4 do Polityki Bezpieczeństwa Informacji),
- Polityka Bezpieczeństwa Informacji dla SRP – szczególne wymagania dla Systemu Rejestrów Państwowych (załącznik nr 5 do Polityki Bezpieczeństwa Informacji),
- Regulamin pracy zdalnej dla pracowników Urzędu Gminy w Żyrakowie (załącznik do Zarządzenia nr AO.120.7.2025 Kierownika Urzędu z dnia 31 grudnia 2025 r.),
- Lista dopuszczonego oprogramowania do użytkowania w Urzędzie Gminy Żyraków (załącznik nr 1 do Zarządzenia nr AO.0050.44.2026 Wójta Gminy Żyraków z dnia 5 maja 2026 r.),
- Zarządzenie nr AO.0050.137.2025 Wójta Gminy Żyraków z dnia 31 grudnia 2025 r. w sprawie zasad prowadzenia inwentaryzacji sprzętu i oprogramowania informatycznego,
- Ewidencja sprzętu komputerowego wykorzystywanego do przetwarzania danych osobowych (stan na dzień 15 kwietnia 2026 r.).

2.2. Analiza zagrożeń związanych z przetwarzaniem informacji

Warunkiem skutecznego funkcjonowania Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) jest systematyczne i udokumentowane prowadzenie analiz ryzyka.

Analiza zagrożeń w ramach SZBI obejmuje ocenę ryzyka utraty poufności, integralności oraz dostępności informacji, w tym identyfikację zagrożeń i podatności, szacowanie ryzyka, określenie sposobu postępowania z ryzykiem oraz dobór adekwatnych zabezpieczeń, zgodnie z § 19 Rozporządzenia KRI.

Wyniki analizy ryzyka powinny być skutecznie wykorzystywane do podejmowania decyzji w zakresie podnoszenia poziomu bezpieczeństwa, w szczególności poprzez wdrażanie odpowiednich mechanizmów kontrolnych, zapewnienie ciągłości działania (np. poprzez system zastępstw na kluczowych stanowiskach) oraz realizację szkoleń pracowników w obszarach szczególnie narażonych na zagrożenia związane z eksploatacją systemów teleinformatycznych. Analiza powinna obejmować wszystkie informacje przetwarzane w jednostce.

W Urzędzie Gminy Żyraków zasady zarządzania ryzykiem zostały określone w Polityce Bezpieczeństwa Informacji. Proces szacowania ryzyka był koordynowany przez Inspektora Ochrony Danych, natomiast identyfikacja zagrożeń i podatności oraz ocena skutków i prawdopodobieństwa ich wystąpienia były realizowane przez właścicieli aktywów, pełniących jednocześnie rolę właścicieli ryzyka.

Analiza ryzyka bezpieczeństwa informacji została przeprowadzona w Urzędzie Gminy Żyraków w listopadzie 2025 r., a jej wyniki stanowiły podstawę do wdrożenia działań ograniczających zidentyfikowane ryzyka.

2.3. Inwentaryzacja sprzętu i oprogramowania informatycznego

Zarządzanie infrastrukturą informatyczną wymaga zapewnienia aktualnej i kompletnej inwentaryzacji sprzętu oraz oprogramowania wykorzystywanego do przetwarzania informacji, obejmującej ich rodzaj, konfigurację oraz sposób wykorzystania. W praktyce oznacza to prowadzenie rejestru zasobów teleinformatycznych zawierającego informacje o wszystkich zidentyfikowanych aktywach, w tym dane dotyczące urządzeń, ich parametrów technicznych, aktualnej konfiguracji, zainstalowanego oprogramowania, środków komunikacji, a także relacji pomiędzy elementami infrastruktury oraz ich użytkownikami.

Prowadzenie takiej inwentaryzacji stanowi istotny element Systemu Zarządzania Bezpieczeństwem Informacji i wynika z § 19 ust. 2 pkt 2 Rozporządzenia KRI.

W Urzędzie Gminy Żyraków regulacje wewnętrzne przewidywały obowiązek utrzymywania aktualnej inwentaryzacji sprzętu i oprogramowania w zakresie ich rodzaju i konfiguracji, na podstawie Zarządzenia nr AO.0050.137.2025 Wójta Gminy Żyraków z dnia 31 grudnia 2025 r. w sprawie zasad prowadzenia inwentaryzacji sprzętu i oprogramowania informatycznego. Inwentaryzacja prowadzona była w formie arkusza kalkulacyjnego.

Dodatkowo ewidencja zasobów była wspierana przez system ESET Protect, umożliwiający identyfikację urządzeń oraz zainstalowanego oprogramowania w sieci teleinformatycznej.

2.4. Zarządzanie uprawnieniami do pracy w systemach informatycznych

Istotnym elementem polityki bezpieczeństwa informacji jest zarządzanie dostępem do systemów teleinformatycznych, w których przetwarzane są informacje. Celem zarządzania dostępem jest zapewnienie, że osoby uczestniczące w przetwarzaniu informacji posiadają odpowiednie uprawnienia, adekwatne do realizowanych zadań i obowiązków, a zmiany zakresu obowiązków skutkują odpowiednią modyfikacją uprawnień.
Zasady zarządzania uprawnieniami dostępu w Urzędzie Gminy Żyraków zostały określone w Polityce Zarządzania Systemami Teleinformatycznymi.
Dostęp do zasobów informatycznych był nadawany pracownikom po przypisaniu zakresu obowiązków oraz utworzeniu indywidualnego konta użytkownika, zabezpieczonego unikalnym identyfikatorem i hasłem.

W przypadku konieczności nadania, zmiany lub cofnięcia uprawnień do systemów informatycznych, informacja o użytkowniku była najczęściej przekazywana w sposób ustny, pomimo opracowania formularza wniosku o przyznanie/zmianę/cofnięcie uprawnień użytkownika (załącznik nr 1 do PZST).
Monitorowanie dostępu do zasobów informatycznych było realizowane na bieżąco, zgodnie z § 19 ust. 2 pkt 4 Rozporządzenia KRI. Według wymogów Polityki Zarządzania Systemami Teleinformatycznymi za weryfikację zgodności uprawnień z zakresem obowiązków oraz stanem faktycznym odpowiadał Sekretarz Gminy.
Zakres uprawnień użytkowników w badanych systemach był ograniczony w sposób uniemożliwiający wykonywanie operacji zastrzeżonych dla administratorów systemów.
W okresie objętym kontrolą konta byłych pracowników były sukcesywnie blokowane w systemach informatycznych.

2.5. Szkolenia pracowników zaangażowanych w proces przetwarzania informacji

Istotnym elementem Systemu Zarządzania Bezpieczeństwem Informacji jest zapewnienie odpowiedniego poziomu świadomości pracowników w zakresie współodpowiedzialności za bezpieczeństwo informacji, identyfikacji zagrożeń oraz znajomości konsekwencji wynikających z naruszeń bezpieczeństwa.
Szkolenia z zakresu bezpieczeństwa informacji powinny obejmować wszystkie osoby uczestniczące w procesie przetwarzania informacji oraz zapewniać aktualną wiedzę dotyczącą zagrożeń, stosowanych zabezpieczeń oraz skutków potencjalnych incydentów bezpieczeństwa.
Dokumentacja wewnętrzna Urzędu Gminy Żyraków regulowała zasady podnoszenia świadomości pracowników poprzez realizację szkoleń wstępnych oraz cyklicznych, prowadzonych co najmniej raz w roku, zgodnie z postanowieniami Polityki Zarządzania Systemami Teleinformatycznymi.
W toku kontroli przedstawiono informacje potwierdzające realizację szkoleń z zakresu cyberbezpieczeństwa przeprowadzonych w grudniu 2024 r. w ramach projektu „Cyberbezpieczny Samorząd". Kompetencje pracowników zostały dodatkowo uzupełnione szkoleniem zrealizowanym w marcu 2026 r.
Ponadto pracownikom zapewniono dostęp do dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji poprzez udostępnienie obowiązujących regulacji w wewnętrznym zasobie informacyjnym.

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.

W obowiązujących dokumentach były zawarte zasady zarządzania bezpieczną pracą na komputerach przenośnych i sposoby zabezpieczenia tych urządzeń (Procedura ochrony danych osobowych przy pracy zdalnej stanowiąca załącznik nr 16 do Polityki ochrony danych osobowych oraz Regulamin pracy zdalnej dla pracowników Urzędu Gminy w Żyrakowie stanowiący załącznik do Zarządzenia nr AO.120.7.2025 Kierownika Urzędu z dnia 31 grudnia 2025 r.).

Dyski zewnętrzne wykorzystywane w laptopach były zaszyfrowane. Niektóre osoby świadczyły pracę poza siedzibą Urzędu, co wiązało się z koniecznością konfiguracji służbowego sprzętu mobilnego w sposób umożliwiający bezpieczną pracę z zasobami Urzędu.
W toku audytu ustalono również, że w pojedynczym przypadku do łączenia się z zasobami Urzędu podczas służbowych czynności wykorzystywany był prywatny sprzęt, przy zastosowaniu bezpiecznego kanału komunikacji. Praktyka ta, choć incydentalna, generuje podwyższone ryzyko naruszenia bezpieczeństwa informacji, w szczególności w zakresie kontroli dostępu, aktualności zabezpieczeń oraz możliwości nadzoru nad przetwarzanymi danymi.

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.
Polityka Zarządzania Systemem Teleinformatycznym w rozdziale 12 określała konieczność sformułowania w umowach zapisów gwarantujących bezpieczeństwo informacji oraz gwarancję szybkiego uruchomienia i czasów reakcji w przypadku awarii.
Polityka wskazywała również, że udzielanie dostępu fizycznego i logicznego dla firm zewnętrznych do zasobów teleinformatycznych musiało się odbywać bezpiecznymi tunelami VPN wyłącznie za zgodą Administratora Systemów Informatycznych.
W udostępnionej umowie z firmą zewnętrzną Vanona Sp. z o.o. zawartą na 2026 r. o asystę techniczną systemu PB_EWID były określone SLA (Service Level Agreement), czyli gwarantowany poziom świadczenia usług oraz czas i sposób reakcji na zgłaszane problemy.

W przypadku sprawdzanych systemów zostały przedstawione umowy powierzenia przetwarzania danych osobowych (udostępniono m.in. umowę: z Biurem Usług komputerowych SOFTRES sp. z o.o. oraz Vanona Sp. z o.o.).

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: Polityce Zarządzania Systemem Teleinformatycznym (rozdział 15) oraz Polityce Zarządzania Incydentami Cyberbezpieczeństwa. Polityka umożliwiała szybkie i najbardziej efektywne podjęcie działań korygujących przez wskazanie m.in. osób odpowiedzialnych i kanałów zgłaszania incydentu. W przypadku naruszenia ochrony danych osobowych zasady zostały określone w Polityce Ochrony Danych Osobowych.
Rejestr naruszeń w zakresie danych osobowych zawierał wpisy z 2023 i 2024 roku.

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

W obowiązującej dokumentacji zawarte zostały wymogi przeprowadzania audytu informatycznego w jednostce co najmniej raz w roku (Polityka Zarządzania Systemem Teleinformatycznym – rozdział 16). W Polityce Bezpieczeństwa Informacji szczegółowo zostało opisane planowanie i przeprowadzania audytów (rozdział 8). Warto zwrócić uwagę, że celem audytów jest ewentualne ujawnienie słabości systemów, a także słabości zabezpieczeń lub ich stosowania.

W Urzędzie Gminy Żyraków audyt bezpieczeństwa informacji wraz z analizą podatności systemu informatycznego był wykonany w grudniu 2024 r. przez firmę zewnętrzną. Natomiast w ramach nadzoru nad przestrzeganiem przepisów o ochronie danych osobowych oraz wdrożonych procedur bezpieczeństwa, Inspektor Ochrony Danych dokonał sprawdzenia realizacji zasad określonych w Polityce czystego biurka w Urzędzie Gminy Żyraków w kwietniu 2025 r.

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 Gminy Żyraków obowiązywały wymagania co do tworzenia, testowania i przywracania kopii zapasowych określone w rozdziale 9 Polityki Zarządzania Systemem Informatycznym.
Kopie folderów, maszyn wirtualnych były wykonywane według harmonogramu ustalonego przez ASI oraz przechowywane na serwerze typu NAS.

Kopie zapasowe były przechowywane na NAS również w innym miejscu niż serwerownia, w jednostce podległej, w lokalizacji poza Urzędem.
Wykonywanie odtworzenia systemów z kopii zapasowych było testowane oraz dokumentowane.

2.11. Projektowanie, wdrażanie i eksploatacja systemów teleinformatycznych

W Urzędzie Gminy Żyraków proces administrowania technicznego i monitorowania określonych obszarów systemów, aplikacji, danych, infrastruktury sieciowej i stacji roboczych był wykonywany przez informatyka, 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. Jednak należy dokonać analizy umów oraz je uzupełnić o konkretne klauzule i zapisy, aby skutecznie zabezpieczyć systemy informatyczne np. umowę z Biurem Usług komputerowych SOFTRES sp. z o.o. na Zintegrowany System Informatyczny „Sprawny Urząd”.

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 Polityce Zarządzania Systemem Teleinformatycznym.
Ochrona informacji przed kradzieżą, nieautoryzowanym dostępem, uszkodzeniami czy zakłóceniami w Urzędzie Gminy Żyraków 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, wejścia i wyjścia 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 Gminy Żyraków 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, do której dostęp był ograniczony i możliwy wyłącznie dla upoważnionych pracowników. Istotnym elementem ochrony było asystowanie osobom wchodzącym do serwerowni oraz wykonującym prace serwisowe.
W serwerowni prowadzono monitoring temperatury, wilgotności i cisnienia, pomieszczenie było klimatyzowane. Drzwi do serwerowni były wzmocnione.
Bazy danych z kopiami zapasowymi były przechowywane w innej lokalizacji niż serwerownia.
W serwerowni znajdował się zasilacz awaryjny UPS, zapewniający podtrzymanie pracy serwera oraz urządzeń sieciowych. W pomieszczeniu nie przechowywano materiałów łatwopalnych.
Podstawowe elementy infrastruktury informatycznej, w tym serwer oraz urządzenia sieciowe, zostały zakupione w ramach projektu.
Monitorowanie ruchu sieciowego wychodzącego i przychodzącego realizowane było przez urządzenie sprzętowe klasy UTM, zakupione w ramach projektu „Cyberbezpieczny Samorząd”.
W ramach projektu zakupiono również oprogramowanie iS Sec, stanowiące narzędzie klasy SIEM (Security Information and Event Management). Wdrożenie zintegrowanego systemu zapewniało monitoring infrastruktury IT oraz automatyzację działań ochronnych przed cyberzagrożeniami. Umożliwiało ono bieżące wykrywanie anomalii na stacjach roboczych i serwerach oraz korelację zdarzeń w całej infrastrukturze.
Wszystkie komputery oraz urządzenia sieciowe posiadały oprogramowanie systemowe zaktualizowane do wersji objętych wsparciem producenta.
Nośniki uszkodzone lub niezdolne do ponownego użycia były trwale niszczone.

2.13. Zabezpieczenia techniczno-organizacyjne systemów informatycznych

Zabezpieczenia techniczno-organizacyjne systemów informatycznych w Urzędzie Gminy Żyraków wynikały z analizy ryzyka przeprowadzonej w listopadzie 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.

Podstawowym dokumentem SZBI w Urzędzie Gminy Żyraków w zakresie zapewnienia ciągłości działania oraz minimalizacji ryzyka utraty informacji była Polityka Zarządzania Ciągłością Działania wraz z zestawem Planów Ciągłości Działania.

Centralne zarządzania tożsamościami w oparciu o Active Directory, należy ocenić jako adekwatne do podstawowych potrzeb zapewnienia bezpieczeństwa środowiska teleinformatycznego i ograniczania ryzyka awarii oraz nieuprawnionego dostępu, tym samym umożliwiające 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 identyfikowalności podnosi dyscyplinę bezpieczeństwa.

Urząd posiadał regulacje wewnętrzne określające zachowanie rozliczalności i zapisywania logów systemowych w szczególności Politykę Zarządzania Systemem Teleinformatyczny (rozdział 14). Systemy użytkowe miały jednak udokumentowaną rozliczalność głównie poprzez logi generowane w systemach takich jak Windows Server oraz w firewall.

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 i BIP poprzez polski walidator dostępny pod adresem: https://validator.utilitia.pl/ badana strona uzyskała wynik 3,2 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 2 czerwca 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 rozdziałem 12 Polityki Zarządzania Systemem Teleinformatycznym.
2. W serwerowni warto wprowadzić Kontrolę Dostępu (rejestr wejść i wyjść) oraz system alarmowy.
3. Zaleca się ograniczenie wykorzystywania prywatnych urządzeń do realizacji obowiązków służbowych wyłącznie do sytuacji uzasadnionych. Dopuszczenie takiego rozwiązania powinno następować pod warunkiem spełnienia minimalnych wymagań bezpieczeństwa określonych w obowiązującej procedurze oraz zapewnienia dostępu jedynie do zasobów niezbędnych do realizacji powierzonych zadań.

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)