WOJEWODA PODKARPACKI
ul. Grunwaldzka 15
35-959 Rzeszów

OA-IV.431.4.2025 Rzeszów, 2025-12-30

Pan
Daniel Krawiec
Wójt Gminy Przeworsk

Na podstawie art. 46 ust. 1 ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej, w związku ze zrealizowaną w dniach 4 i 6 listopada 2025 r. u Wójta Gminy Przeworsk (Gmina Przeworsk, ul. Bernardyńska 1A, 37-200 Przeworsk) 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 28.10.2025 r., znak OA-IV.431.4.2025) udzielonych przez działającego z upoważnienia Wojewody Podkarpackiego – Dyrektora Wydziału Organizacyjno-Administracyjnego.

Ustalenia kontrolne dokonane zostały w oparciu o stan faktyczny istniejący od 1 stycznia 2024 r. 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 w Przeworsku 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 2025 r. „Planu zewnętrznej działalności kontrolnej Podkarpackiego Urzędu Wojewódzkiego w Rzeszowie na 2025 rok").

W oparciu o poczynione ustalenia, stosownie do skali ocen przyjętej w „Programie kontroli problemowej realizowanej u Wójta Gminy Przeworsk”[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 Gminy Przeworsk pełnił Wójt: Pan Daniel Krawiec.

Funkcję Inspektora Ochrony Danych (IOD) powierzono wykonawcy zewnętrznemu Panu Pawłowi Dzień, na podstawie umowy z dnia 01.01.2025 r. zawartą z firmą ARTEMIDA SECURITY DATA sp. z o.o.

Wsparcie informatyczne zapewnione było przez informatyka, pracownika Urzędu Gminy Przeworsk. Pod jego opieką znajdowały się: środowiska sprzętowo-programowe, sieć lokalna, serwerownia, systemy i aplikacje centralne oraz własne, usprawniające pracę pracownikom Urzędu Gminy Przeworsk.

Została wyznaczona osoba odpowiedzialna za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa na podstawie Zarządzenia Nr 121/2021 Wójta Gminy Przeworsk z dnia 30 grudnia 2021 r. oraz zostało dokonane zgłoszenie tej osoby do CSIRT NASK w dniu 28 września 2022 r.

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

a) systemy centralne:

- 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.

[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.

b) systemy własne lub zakupione:
- Lokalny Rejestr Mieszkańców wraz z modułem transmisyjny (EPLUS, ImportSRP) – firmy CLANET sp. z o.o.;
- Zwrot podatku akcyzowego – firmy VENDIS;
- Ewidencja środków trwałych i przedmiotów użytkowania - firmy Biuro Usług Komputerowych SOFTRES sp. z o.o.;
- 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 Gminy Przeworsk udostępniał elektroniczną skrzynkę podawczą (dalej: ESP) na platformie ePUAP oraz adres do eDoręczeń. Na stronie BIP kontrolowanej jednostki znajdowała się informacja o **elektronicznej skrzynce podawczej i adresie do eDoręczeń,** które pozwalały na przesłanie drogą elektroniczną pism skierowanych do Urzędu, w tym pism ogólnych, skarg, wniosków, zapytań itp.
Na stronie BIP znajdowała się informacja o adresie eDoręczeń i **elektronicznej skrzynki podawczej**.

1.2. Współpraca systemów teleinformatycznych z innymi systemami

Pracownicy Urzędu Gminy Przeworsk posiadali dostęp do rejestrów publicznych takich jak: SRP Źródło, CEIDG.

System Lokalnego Rejestru Mieszkańców komunikował się z usługami sieciowymi Systemu Rejestrów Państwowych w celu pobierania danych dzięki modułowi ImportSRP odpowiadającemu za transmisję danych z SRP do Lokalnego Rejestru Mieszkańców.

1.3. Obieg dokumentów

W Urzędzie Gminy Przeworsk nie było wdrożonego Systemu Elektronicznego Zarządzania Dokumentacją umożliwiającego zarządzanie dokumentami i wykonywanie czynności kancelaryjnych. Obecnie każda wpływająca korespondencja była rejestrowana i dekretowana ręcznie.

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 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 zakresie bezpieczeństwa teleinformatycznego w badanej jednostce został ustanowiony System Zarządzania Bezpieczeństwem Informacji (SZBI). System Zarządzania Bezpieczeństwem Informacji wprowadzony został w Polityce Bezpieczeństwa Informacji i Ochrony Danych Osobowych (PBIiODO) na podstawie Zarządzenia nr 152/2018 Wójta Gminy Przeworsk z dnia 28 grudzień 2018 r.;

Ustanowione dokumenty i procedury regulują głównie ochronę danych osobowych. Pomimo, iż dokumentacja była ustanowiona i aktualizowana, nie wszystkie przygotowane wymagania oraz załączniki zostały wdrożone.

Powyższym zarządzeniem w Urzędzie Gminy Przeworsk ustanowiono:

- Politykę Bezpieczeństwa Informacji i Ochrony Danych Osobowych (PBIiODO) Urzędu Gminy Przeworsk wraz z załącznikami;
- Politykę Bezpieczeństwa Systemów Teleinformatycznych (PBST) Urzędu Gminy Przeworsk;
- Regulamin Użytkownika Systemów Teleinformatycznych (RU) Urzędu Gminy Przeworsk;
- Zasady i tryb przeprowadzania analizy ryzyka przetwarzania danych osobowych w Urzędzie Gminy Przeworsk - załącznik do Zarządzania Wójta Gminy Przeworsk nr 157/2024 z dnia 31.12.2024 r. w sprawie powołania zespołu do spraw dokonania analizy ryzyka dla ochrony danych osobowych;
- Procedura zachowania ciągłości działania Urzędu Gminy Przeworsk – załącznik do Zarządzenia Wójta Gminy Przeworsk nr 91/2025 z dnia 30.10.2025 r. w sprawie wprowadzenia Procedury zachowania ciągłości działania;
- Regulamin publikowania w Biuletynie Informacji Publicznej Urzędu Gminy Przeworsk;
- Procedura zarządzania incydentami związanymi z bezpieczeństwem informacji i cyberbezpieczeństwem w Urzędzie Gminy w Przeworsku.

2.2. Analiza zagrożeń związanych z przetwarzaniem informacji

Wymogiem skuteczności SZBI jest przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji. Na analizę ryzyka składają się: identyfikacja, szacowanie a następnie określenie sposobu postępowania z ryzykiem oraz deklaracja stosowania zabezpieczeń będących podstawą podejmowania wszelkich działań minimalizujących ryzyko stosownie do przeprowadzonej analizy.
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.

Zarządzanie bezpieczeństwem przetwarzania danych w Urzędzie Gminy Przeworsk opierało się na zarządzaniu ryzykiem, które polegało na przeprowadzaniu okresowej analizy ryzyka i oceny skutków dla przetwarzania danych osobowych. Identyfikacja, ocena oraz określenie metod przeciwdziałaniu ryzyku przeprowadzana była w 2025 r. przez powołany zespół, w odniesieniu do ochrony danych osobowych.
Dokonując analizy ryzyka warto wziąć pod uwagę utratę integralności, dostępności lub poufności wszystkich informacji, nie tylko tych związanych z danymi osobowymi.
Analiza ryzyka powinna obejmować największe zagrożenia dla cyberbezpieczeństwa oraz stanowić fundament skutecznego cyberbezpieczeństwa.

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.

Regulacje wewnętrzne, w Polityce Bezpieczeństwa Informacji i Ochrony Danych, zawierały zapisy dotyczące identyfikacji i klasyfikacji aktywów informacyjnych. Polityka Bezpieczeństwa Systemów Teleinformatycznych wymagała prowadzenia metryki w formie papierowej lub elektronicznej dla każdego sprzętu komputerowego. Taka metryka nie została przedstawiona. Natomiast informatyk prowadził inwentaryzację wykorzystując specjalistyczne oprogramowanie statlook.
Jednostka dysponowała zakupionym i wdrożonym oprogramowaniem ESET Protect Entry, którego Platforma umożliwiała monitorowanie wszystkich urządzeń w czasie rzeczywistym.

W urzędzie do pracy bieżącej, użytkowane były komputery stacjonarne oraz laptopy, a do eksploatacji dopuszczone było tylko oprogramowanie autoryzowane przez ASI, które zgodnie z Polityką Bezpieczeństwa Systemów Teleinformatycznych podlegać powinno wpisowi do Ewidencji oprogramowania dopuszczonego do użytkowania. Taka ewidencja nie była prowadzona.

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.
W Urzędzie Gminy, zarządzanie uprawnieniami dostępu do przetwarzania danych regulowały: Regulamin Użytkownika Systemów Teleinformatycznych, Polityka

Bezpieczeństwa Systemów Teleinformatycznych oraz Polityka Bezpieczeństwa Informacji i Ochrony Danych Osobowych.
Dokumentacja powyższa opisywała sposób dostępu do obszarów chronionych, sieci i systemów teleinformatycznych oraz nadawania, zmiany i odbierania uprawnień użytkownikom w systemach informatycznych funkcjonujących w jednostce.
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 dla użytkownika w systemach informatycznych informacja przekazywana była ustnie lub mailowo przez bezpośredniego przełożonego pracownika.
Zakres uprawnień użytkowników badanych systemów uniemożliwiał wykonywanie przez nich działań zastrzeżonych dla administratorów systemów w przypadku komputerów stacjonarnych podłączonych do Active Directory.
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.

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 Gminy Przeworsk (Regulamin Użytkownika Systemów Teleinformatycznych, Polityka Bezpieczeństwa Systemów Teleinformatycznych oraz Polityka Bezpieczeństwa Informacji i Ochrony Danych Osobowych) regulowała zakres przeszkolenia osób przed dopuszczeniem do pracy. Również w zakresie zwiększenia świadomości pracowników przynajmniej raz w roku powinno być organizowane szkolenie przypominające zasady ochrony informacji.
Przedstawiono informację o ostatnim takim szkoleniu z 2025 roku.
W Urzędzie Gminy Przeworsk podejmowane były działania podnoszące świadomość pracowników, w tym celu został udostępniony folder na zasobie dyskowym zawierający dokumenty w zakresie ochrony danych osobowych i informacji.

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. Konieczne jest opisanie zasad określających sposoby zabezpieczenia urządzeń mobilnych i danych w nich zawartych przed kradzieżą i nieuprawnionym dostępem poza siedzibą jednostki, a także zasady korzystania z ogólnodostępnych sieci.
W obowiązujących dokumentach były zawarte ogólne zasady zarządzania bezpieczną pracą na komputerach przenośnych i sposoby zabezpieczenia tych urządzeń (Polityka

Bezpieczeństwa Systemów Teleinformatycznych). W Urzędzie Gminy nie funkcjonował Regulamin pracy zdalnej.

Laptopy nie były szyfrowane. Pracownicy nie wynosili przenośnych komputerów poza siedzibę jednostki.

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.
W procedurach wewnętrznych m.in. w: Polityce Bezpieczeństwa Systemów Teleinformatycznych zostały określone zasady dopuszczenia podmiotów zewnętrznych na wykonanie usług.
Dodatkowo poziom bezpieczeństwa regulowały umowy zawierane z firmami zewnętrznymi, w przypadku serwisowania sprzętu lub oprogramowania (udostępniono umowę serwisową z firmą: CLANET sp. z o.o. na 2025 rok, ZONEO Oleksiewicz Spółka Komandytowo-Akcyjna, INTERmedi@ Ł. Czekała T. Frąckowiak sp. j. oraz licencje z Biurem Usług komputerowych SOFTRES Sp. z o.o., z VENDIS, Data Security Software Solutions sp. z o.o.
W przypadku systemów informatycznych istotnych dla jednostki zostały zawarte także umowy powierzenia przetwarzania danych osobowych.

2.8. Procedury zgłaszania incydentów naruszenia bezpieczeństwa informacji

Zostały określone zasady postępowania w przypadku stwierdzenia naruszenia bezpieczeństwa informacji w Procedurze zarządzania incydentami związanymi z bezpieczeństwem informacji i cyberbezpieczeństwem w Urzędzie Gminy w Przeworsku.
Rejestr incydentów i działań korygujących w Urzędzie Gminy Przeworsk nie został przedstawiony.

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 był wykonany w 2025 roku. Warto zwrócić uwagę, że celem audytów jest ewentualne ujawnienie słabości systemów, a także słabości zabezpieczeń lub ich stosowania. Uregulowania wewnętrzne nie zawierały zapisów dotyczących konieczności audytowania i sprawdzeń w zakresie bezpieczeństwa informacji.

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

W 2024 roku nie był wykonany audyt dotyczący bezpieczeństwa informacji, ani sprawdzenie przez Inspektora Ochrony Danych w zakresie ochrony danych osobowych.

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 Przeworsk obowiązywały wymagania określone w Polityce Bezpieczeństwa Systemów Teleinformatycznych (§ 49 Procedury tworzenia kopii bezpieczeństwa i kopii zapasowych).
Kopie folderów, maszyn wirtualnych były wykonywane według harmonogramu ustalonego przez ASI oraz przechowywane na serwerze NAS. Kopie wykonywano przy pomocy narzędzia Ferro Backup System Pro.
Wykonywanie odtworzenia systemów z kopii zapasowych było testowane oraz odbywało się w razie potrzeby.
Przechowywanie kopii zapasowej poza siedzibą Urzędu nie zostało uregulowane i opisane.

2.11. Projektowanie, wdrażanie i eksploatacja systemów teleinformatycznych

W Urzędzie Gminy Przeworsk proces administrowania technicznego i monitorowania określonych obszarów systemów, aplikacji, danych, infrastruktury sieciowej i stacji roboczych był wykonywany przez pracownika zatrudnionego, jako informatyk, 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.

W przypadku tych systemów należy pamiętać, aby w umowach serwisowych z firmami trzecimi zawrzeć odpowiednie zapisy dotyczące kanałów komunikacji i czasów reakcji.

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.
Część zabezpieczeń techniczno-organizacyjnych dostępu do informacji opisano w Regulaminie Użytkownika Systemów Teleinformatycznych, Polityce Bezpieczeństwa Systemów Teleinformatycznych oraz Polityce Bezpieczeństwa Informacji i Ochrony Danych Osobowych).
Ochrona przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami realizowana była przez:

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;
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 Gminy Przeworsk posiadał pomieszczenia biurowe zlokalizowane w jednym budynku.
Obiekt był objęty systemem alarmowym ochrony fizycznej oraz był objęty systemem monitoringu na zewnątrz i wewnątrz budynku. Do otwierania głównych drzwi budynku oraz rozbrajania systemu alarmowego byli upoważnieni wyznaczeni pracownicy.
Klucze do pomieszczeń biurowych pracownicy pobierali z sekretariatu.
W budynku oprócz systemu alarmowego były również czujki przeciwpożarowe.
Urząd Gminy dysponował jedną główną serwerownią. Serwerownia znajdowała się w pomieszczeniu wyodrębnionym na ten cel.
Drzwi do serwerowni nie były wzmocnione i nie posiadały atestu. Serwerownia posiadała system kontroli dostępu na kartę oraz na kod.
Występowało monitorowanie parametrów środowiskowych w serwerowni (temperatury i wilgotności). Pomieszczenie było klimatyzowane. W pomieszczeniu nie były przechowywane materiały łatwopalne.
Dostęp do serwerowni był ograniczony i możliwy jedynie dla upoważnionych pracowników Urzędu. Ważnym elementem ochrony było asystowanie osobom wchodzącym i wykonującym prace serwisowe.
Dodatkowo Urząd dysponował drugim pomieszczeniem, na innej kondygnacji, mogącym pełnić funkcję serwerowni zapasowej. Przechowywane tu były kopie zapasowe. Kopie zapasowe nie były przechowywane poza Urzędem.
Podstawowe urządzenie infrastruktury informatycznej: serwer, urządzenia sieciowe były zakupione w ramach Projektu.
W serwerowni znajdowały się UPSy, który podtrzymywały pracę serwera i urządzeń sieciowych. Zapewniono redundancję łączy internetowych od niezależnych dostawców.
Monitorowanie ruchu wchodzącego i wychodzącego realizowane było przez maszynę sprzętową firewall: UTM Fortigate. Nie zapewniono redundancji firewall – zgodnie z całościowym prawidłowym podejściem do infrastruktury.

Nie wszystkie systemy dziedzinowe były zainstalowane na serwerze znajdującym się w serwerowni.

Wszystkie komputery oraz urządzenie sieciowe posiadały oprogramowanie systemowe zaktualizowane do wersji posiadających wsparcie producenta.

2.13. Zabezpieczenia techniczno-organizacyjne systemów informatycznych

Stosowanie zabezpieczeń techniczno-organizacyjnych również powinno wynikać z analizy ryzyka i powstałego w jej wyniku planu postępowania z ryzykiem i deklaracji stosowania zabezpieczeń.
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 wymagało przyznania dostępu do danych dla uprawnionych użytkowników. Wszelkie działania związane z przetwarzaniem informacji, a także działania administratorów muszą podlegać dokumentowaniu w postaci zapisów w dziennikach systemów (logi), co zapewnia rozliczalność operacji. Informacje zawarte w logach (tj. kto, kiedy i co wykonał w systemie teleinformatycznym) powinny być regularnie przeglądane w celu wykrycia działań niepożądanych i muszą być przechowywane w bezpieczny sposób, co najmniej dwa lata. Świadomość użytkowników, że żadne działanie nie zostanie anonimowe podnosi poziom bezpieczeństwa informacji.

W Polityce Bezpieczeństwa Systemów Teleinformatycznych zostały częściowo ustanowione zasady zarządzania logami takie jak: rejestrowanie faktu rozpoczęcia pracy przez użytkowników, odnotowywania prób nieautoryzowanego dostępu w systemie oraz przechowywania logów przez dwa lata.
Sprawdzane systemy informatyczne użytkowe miały udokumentowaną rozliczalność.
Warto, w celu zapewnienia rozliczalności każdemu użytkownikowi przypisać indywidualne konto, w szczególności dla administratorów, (w tym z firm zewnętrznych) oraz zdeponować hasła administratorów do najważniejszych systemów i urządzeń w bezpiecznym miejscu w powiązaniu z procedurą ciągłości działania.

3. Zapewnienie dostępności informacji zawartych na stronie BIP oraz internetowej urzędu 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.

Systemy informatyczne wspomagające realizację zadań Urzędu nie były objęte wymogami WCAG 2.0 w zakresie dostępności ze względu na brak interakcji z klientami za pośrednictwem sieci publicznej.

Analizując poprawność kodu strony BIP oraz www poprzez walidator dostępny pod adresem: https://validator.utilitia.pl/ badane strony uzyskały wynik 7,7 pkt na 10 możliwych.

Ww. ustalenia, w tym ocena kontrolowanej działalności, zostały udokumentowane w aktach kontroli, na które składają się kopie dokumentów.

Przy czym do ww. ustaleń kontrolnych (przekazanych do wiadomości w dniu 5 grudnia 2025 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. Należy dokonać przeglądu wszystkich umów serwisowych zawartych z podmiotami zewnętrznymi i w razie potrzeby, uzupełnić je o zapisy gwarantujące odpowiedni poziom bezpieczeństwa informacji, w szczególności poprzez określenie parametrów SLA (Service Level Agreement) obejmujących: gwarantowany poziom świadczenia usług, ciągłość działania, zasady oraz czas dostępu zdalnego, a także czas i sposób reakcji na zgłaszane problemy, oraz zapewnić bieżący nadzór nad wykonawcami w zakresie zgodności realizowanych usług z regulacjami wewnętrznymi i zapisami umownymi.
2. Zaleca się, aby kopie zapasowe przechowywać również w odrębnej lokalizacji niż siedziba Urzędu Gminy, w celu ograniczenia ryzyka ich utraty w przypadku zdarzeń losowych dotyczących budynku urzędu.
3. Należy monitorować, przeglądać i doskonalić pełny system zarządzania bezpieczeństwem informacji, obejmując analizą ryzyka utratę integralności, dostępności i poufności wszystkich przetwarzanych informacji (nie tylko danych osobowych), uwzględniając konieczność zachowania ciągłości działania oraz bezpieczeństwa systemów i Urzędu, a także zapewniając pełną rozliczalność działań użytkowników i administratorów.
4. Dokonać szyfrowania urządzeń przenośnych w celu zminimalizowania ryzyka nieuprawnionego dostępu do informacji w przypadku ich utraty lub kradzieży.
5. Należy dążyć do umieszczenia wszystkich istotnych systemów dziedzinowych na serwerach zlokalizowanych w serwerowni Urzędu.
6. Wskazane jest wzmocnienie zabezpieczeń fizycznych pomieszczenia serwerowni, w szczególności poprzez zastosowanie wzmocnionych, atestowanych drzwi, adekwatnych do znaczenia przetwarzanych tam zasobów.
7. Zaleca się dążenie do zapewnienia redundancji urządzenia typu firewall (UTM), aby zwiększyć niezawodność ochrony perymetrycznej sieci oraz ograniczyć ryzyko przestoju w przypadku awarii pojedynczego urządzenia.

O sposobie wykonania powyższych wniosków pokontrolnych, bądź działaniach podjętych w celu ich realizacji, oczekuję od Pana odpowiedzi na piśmie wraz ze skanami dokumentów lub innych potwierdzeń dotyczących sposobu wdrożenia zaleceń, w terminie 21 dni od dnia otrzymania niniejszego wystąpienia.

WOJEWODA PODKARPACKI

(-)

Teresa Kubas-Hul

(Podpisane bezpiecznym podpisem elektronicznym)