PROGRAM ZADANIA ZAPEWNIAJĄCEGO:

I. Temat zadania: Ocena zapewnienia bezpieczeństwa informacji.

II. Cel zadania:

Celem głównym zadania było potwierdzenie, że Urząd Gminy Zaniemyśl podejmuje skuteczne działania w zakresie zapewnienia poufności, dostępności i integralności informacji.

III. Zakres zadania zapewniającego :

Podmiotowy: Zadanie zostało przeprowadzone w komórkach organizacyjnych Urzędu Gminy Zaniemyśl.

Przedmiotowy: W zakresie przedmiotowym ocenie poddano obszar działań podejmowanych przez komórki organizacyjne pod względem ich zgodności z obowiązującymi przepisami prawa, w tym rozporządzeniem RODO - Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119) oraz uwzględnia zapisy rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012r. w sprawie w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. z 2017r., poz. 2247).
Niniejszy audyt nie dotyczy zapewnienia bezpieczeństwa informacji, o których mowa w ustawie z dnia 5 sierpnia 2010r. o ochronie informacji niejawnych (Dz.U. z 2019r., poz. 742).

IV. Analiza ryzyka:

Wskazane obiekty audytu wyłoniono na podstawie wyodrębnionych przez audytora obszarów ryzyka, zgodnie z zakresem przedmiotowym realizowanego zadania audytowego. Przyjmując taki zakres ryzyk audytor zwrócił szczególną uwagę na ryzyka związane z:

1. niewystarczającym dla należytego zabezpieczenia danych systemem zapewnienia bezpieczeństwa danych,
2. brakiem należytej wiedzy pracowników,
3. nieefektywnym i nieterminowym podejmowaniem czynności związanych z zapewnieniem ochrony danych, czego efektem może być naruszenie ochrony danych osobowych czy nałożenie kar przez organ nadzoru.

W wyniku przeprowadzonej analizy audytor stwierdził, że wyłonione obiekty audytu zagrożone są podobnym ryzykiem, nieco większa materializacja ryzyka dotyczy nieefektywnego i nieterminowego podejmowania czynności, a w konsekwencji może prowadzić do naruszenia bezpieczeństwa danych osobowych czy wywołać skutki finansowe dla budżetu Gminy.

Metodyka:
1. Analiza dokumentacji – polega na zgromadzeniu i gruntownym zbadaniu materiałów dostępnych u audytowanego. W szczególności technika ta przydatna będzie w odniesieniu do wyników poprzednio przeprowadzonych badań i analiz (ewaluacje, audyty, oceny okresowe, pomiary i testy, sprawozdania z kontroli) oraz do zapoznania się z modelowymi zachowaniami (regulaminy, podręczniki wdrażania, schematy organizacyjne itp.).
2. Rozmowa, Wywiad – uzyskiwanie informacji ustnych od pracowników komórek, w których przeprowadzany jest audyt oraz informacji uzupełniających od innych pracowników Jednostki.
3. Procedury analityczne – wykorzystywane do oceny informacji zgromadzonych w trakcie badania. Ocena wynika z porównania zebranych informacji z oczekiwaniami audytora. Mogą obejmować w zależności od potrzeb:
- porównanie informacji dotyczących bieżącego okresu z analogicznymi informacjami dotyczącymi okresów poprzednich,
- porównanie informacji dotyczących bieżącego okresu z budżetem lub prognozami.
- badanie powiązań pomiędzy informacjami finansowymi a odpowiednimi informacjami pozafinansowymi.
4. Testy przeglądowe – testy, które pozwalają zrozumieć działalność audytowanej jednostki i zidentyfikować elementy kontroli wewnętrznej.
5. Testy zgodności – zbadanie sposobu przetwarzania wybranych operacji przez kontrolowany system w celu stwierdzenia, czy system działał w sposób ciągły (tj. w całym okresie objętym audytem), spójny (tj. wszystkie operacje podlegające działaniu systemu traktowane były w sposób jednakowy) i skuteczny (tj. osiągał cele związane z jego ustanowieniem).
6. Testy wiarygodności – bezpośrednie badanie operacji objętych audytem w celu uzyskania dowodów audytu.
7. Testy poprawności – badanie operacji, w tym ocena zgodności z przepisami prawa, ocena systemów kontroli wewnętrznej, badanie działań pod względem legalności i rzetelności w obrębie przedmiotu audytu.
8. Rekonstrukcja obliczeń – pozwala na powtórzeniu operacji matematycznych zastosowanych przez audytowanego.
9. Konfrontacja wewnętrzna polega na ustaleniu, czy treść badanych dokumentów odpowiada stanowi faktycznemu. Konfrontacja wewnętrzna polega na porównaniu faktów ustalonych na podstawie dowodów w komórce objętej badaniem z odpowiadającymi im faktami czy dowodami znajdującymi się w tej samej komórce.
10. Konfrontacja zewnętrzna polega na porównaniu faktów ustalonych na podstawie dowodów w komórce objętej badaniem z odpowiadającymi im faktami czy dowodami znajdującymi się w komórkach z nią współdziałającymi.

Sposób przeprowadzenia badania i techniki zastosowane w trakcie audytu:
Analiza dokumentacji, wywiady personalne, w tym formularzowe i indywidualne, oględziny infrastruktury technicznej, kwestionariusze, check listy, badanie zainstalowanego oprogramowania, badanie plików konfiguracyjnych, testy techniczne (zakres i sposób przeprowadzenia uzgodniony z audytowanym). Zabezpieczenia

Kryteria oceny ustaleń dokonanych w badanych obszarach

1. Legalność: rozumiana jako ocena kontrolowanej działalności z punktu widzenia jej zgodności z prawem materialnym, proceduralnym oraz ustrojowym, określającym zadania i kompetencje audytowanych podmiotów. Legalność realizacji zadań oceniana jest na podstawie przepisów prawa powszechnie obowiązującego oraz procedur wewnętrznych.
2. Efektywność podejmowanych działań oceniana w kontekście skutecznego podejmowania działań przez komórki objęte badaniem;

Sposób klasyfikowania wyników dla danego kryterium:

V.	**Kryteria oceny ustaleń stanu faktycznego i sposób ich klasyfikowania.**		
Określenie kryterium oceny ustaleń:		Klasyfikacja wyników dla danego kryterium:	Opis sposobu klasyfikacji wyników ustaleń dla danego kryterium
1	**Zgodność (prawidłowość)**	**Zgodny**– nie stwierdzono żadnych ryzyk, zidentyfikowane zyska mają znaczenie małe lub znikome **Zgodny z zastrzeżeniami** – zidentyfikowano ryzyka o średnim znaczeniu dla obszaru audytowanego, większość ryzyk ma znaczenie średnie, nie stwierdzono ryzyk krytycznych **Niezgodny**- większość zidentyfikowanych ryzyk ma znaczenie duże, lub stwierdzono ryzyka krytyczne dla obszaru audytowanego	Prawidłowe to zgodne z prawem i rzetelne Rzetelność oceniana jest w kontekście poprawności rachunkowej oraz kompletności dokumentacji i jej zgodności ze stanem faktycznym. Nieprawidłowości będą oceniane w pięciostopniowej skali ryzyk z nimi związanych: ➢ krytyczne - poważne konsekwencje ➢ duże – ryzyka o znaczącym znaczeniu, ale nie krytycznym ➢ średnie- skutki mogą mieć znaczenie , ale nie wpłyną znacząco na działalność ➢ małe - małe konsekwencje ➢ znikome – znikome znaczenie dla działalności
	Efektywność	**Optymalny** – przewaga korzyści nad kosztami lub znikome ryzyka nieefektywności **Efektywny –** większość zidentyfikowanych ryzyk przewagi kosztów nad korzyściami mają małe i znikome znaczenie **Efektywny z zastrzeżeniami** - zidentyfikowane ryzyka przewagi kosztów nad korzyściami o znaczeniu średnim i dużym, ale nie decydujące o ocenie nieefektywnej **Nieefektywny** - zidentyfikowano krytyczne ryzyka nieefektywności lub większość ryzyk ma znaczenie duże	Obejmuje badanie uzyskania najlepszych efektów w ramach stosowanych środków oraz proporcjonalności efektów działań do zastosowanych środków ich osiągnięcia. Gospodarność dotyczy oszczędnego i wydajnego wykorzystania środków, uzyskania właściwej relacji nakładów do efektów (czy wynik działalności można byłoby osiągnięć mniejszym nakładem środków lub zastosowanymi środkami można było osiągną lepszy wynik). Nieefektywność wydatków dla realizacji zadań będzie oceniana w pięciostopniowej skali ryzyk odzwierciedlających stopień w jaki nie zapewnia efektywność (przewagę korzyści nad kosztami wybranych form działania) • krytyczne- brak istotnych korzyści, istotne koszty, brak wydajności, • duże – przewaga kosztów nad korzyściami (bardzo niska wydajność), • średnie – koszty równe korzyściom, • małe – przewaga korzyści nad kosztami wysokie korzyści, wydajne wykorzystanie zasobów, • znikome ryzyka nieefektywności przewagi

			kosztów nad korzyściami (niewydajności).
Ponadto audytor w trakcie audytu ocenia kontrolę zarządczą w obszarze audytowanym stosując kryteria:			
1	Skuteczność kontroli zarządczej w obszarze audytowanym	Skuteczny/ Nieskuteczny	Skuteczny system kontroli zarządczej zapewnia realizację przyjętych celów w zgodzie z zamierzeniami, przepisami prawa i efektywnie
2	Adekwatność kontroli zarządczej w obszarze audytowanym	Adekwatny/ Nieadekwatny	Adekwatna (prawidłowa) kontrola zarządcza została tak zaprojektowana aby zapewnić realizację celów zgodzie z zamierzeniami, przepisami prawa i efektywnie
3	Efektywność kontroli zarządczej w obszarze audytowanym	Efektywny/ Nieefektywny	Efektywny system kontroli zarządczej pozwala zachować odpowiednią proporcję kosztów i korzyści.

Kryteria oceny wyników audytu

Przyjęto, że ocena wyników audytu obszaru audytowanego będzie klasyfikowana w sposób następujący:

Ocena najwyższa =Nie stwierdzono żadnych ryzyk, zidentyfikowane ryzyka mają znaczenie małe lub znikome, stwierdzono ryzyka średnie ale większość ryzyk ma charakter mały i znikomy; Optymalna lub efektywna**,** skuteczna realizacja zadań, omyłki rachunkowe, przypadki niekompletności, do 10% w próbie

Ocena średnia = Zidentyfikowano ryzyka o średnim znaczeniu dla obszaru audytowanego, większość ryzyk ma znaczenie średnie, nie stwierdzono ryzyk krytycznych. omyłki rachunkowe, przypadki niekompletności, do 11%-25% w próbie Efektywna i skuteczna, z zastrzeżeniami realizacja zadań.

Ocena najniższa = Większość zidentyfikowanych ryzyk ma znaczenie duże, lub stwierdzono ryzyka krytyczne dla obszaru audytowanego, omyłki rachunkowe, przypadki niekompletności, od 26% w próbie i więcej. Nieefektywne nieskuteczne realizowanie zadań ze środków gminnych

SPRAWOZDANIE Z ZADANIA ZAPEWNIAJĄCEGO

I. Temat i cel zadania: Ocena zapewnienia bezpieczeństwa informacji**.**

Celem głównym zadania było potwierdzenie, że Urząd Gminy Zaniemyśl podejmuje skuteczne działania w zakresie zapewnienia poufności, dostępności i integralności informacji.

II. Audytor: Agnieszka Krupa - Sokołowska

III. Zakres zadania zapewniającego :

Podmiotowy: Zadanie zostało przeprowadzone w komórkach organizacyjnych Urzędu Gminy Zaniemyśl.

Przedmiotowy: W zakresie przedmiotowym ocenie poddano obszar działań podejmowanych przez komórki organizacyjne pod względem ich zgodności z obowiązującymi przepisami prawa, w tym rozporządzeniem RODO - Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119) oraz uwzględnia zapisy rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012r. w sprawie w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. z 2017r., poz. 2247).
Niniejszy audyt nie dotyczy zapewnienia bezpieczeństwa informacji, o których mowa w ustawie z dnia 5 sierpnia 2010r. o ochronie informacji niejawnych (Dz.U. z 2019r., poz. 742).

IV. Data rozpoczęcia zadania zapewniającego;
Zadanie zostało rozpoczęte w lutym 2024r.

V. Kryteria szczegółowe

1.1. Przepisy prawa:

a) rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. *w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia Dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)*, nazywane też rozporządzeniem w sprawie RODO (Dz.Urz.UE L Nr 119, str. 1, Dz.Urz.UE L 2018 Nr 127, poz. 2 oraz Dz.Urz.UE L 2021 Nr 74, poz. 35),
b) rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. *w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych* (Dz.U. z 2017 r., poz. 2247),
c) ustawa z dnia 17 lutego 2005 r. *o informatyzacji działalności podmiotów realizujących zadania publiczne* (Dz.U. z 2021 r., poz. 2070 z późn. zm.),
d) ustawa z dnia 10 maja 2018 r. *o ochronie danych osobowych* (Dz.U. z 2019 r. poz. 1781),
e) Konstytucja RP z dnia 02 kwietnia 1997 r. (Dz.U. z 1997 r. Nr 78, poz. 483 z późn. zm.) w części art. 47 i 51 - dotyczących ochrony danych,
f) ustawa z dnia 27 sierpnia 2009 r. *o finansach publicznych* (Dz.U. z 2021 r., poz. 305 z późn. zm.), szczególnie artykuły dotyczące funkcjonowania kontroli zarządczej,
g) *Standardy kontroli zarządczej dla sektora finansów publicznych* – Komunikat Nr 23 Ministra Finansów z dnia 16 grudnia 2009 r. (Dz. Urz. MF z 2009 r. Nr 15, poz. 84),
h) *Standardy audytu wewnętrznego dla jednostek sektora finansów publicznych* – Komunikat Ministra Rozwoju i Finansów z dnia 12 grudnia 2016 r. (Dz. Urz. MRiF z 2016 r., poz. 28).

Podstawę prawną do realizowania zadania gminy objętego badaniem stanowią przepisy zawarte w rozporządzeniu Rady Ministrów z dnia 12 kwietnia 2012r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. z 2017r., poz. 2247).
Przepis § 20 ust 2 pkt 14 niniejszego rozporządzenia wśród czynności związanych ze stworzeniem i prowadzeniem efektywnego systemu zarządzania bezpieczeństwem informacji nakłada na podmioty realizujące zadania publiczne obowiązek zapewnienia okresowego audytu wewnętrznego bezpieczeństwa informacji, nie rzadziej niż raz na rok.

Krótki opis audytowanego obszaru

Szybki postęp techniczny i globalizacja spowodowały gwałtowny wzrost skali zbierania i wymiany danych osobowych. W związku z tym, że występowały różnice w stopniu ochrony danych wynikające z różnic we wdrożeniu i stosowaniu dyrektywy 95/46/WE (poprzedniego rozporządzenia w sprawie ochrony danych) oraz w celu zapewnienia wysokiego i spójnego stopnia ochrony osób fizycznych oraz usunięcia przeszkód w przepływie danych osobowych w Unii Europejskiej, a także mając na względzie zapewnienie równorzędnego we wszystkich państwach członkowskich stopnia ochrony praw i wolności osób fizycznych, w związku z przetwarzaniem ich danych – opracowano i wdrożono spójne i jednolite przepisy obowiązujące w całej Unii, czyli rozporządzenie w sprawie RODO. Zawarto w nim też wskazanie, że państwa członkowskie powinny wprowadzić krajowe przepisy doprecyzowujące stosowanie ww. rozporządzenia.
Aktem prawnym obowiązującym w Polsce, który stanowi uzupełnienie zapisów zawartych w rozporządzeniu unijnym w sprawie RODO, jest ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych, która weszła w życie dnia 25 maja 2018 r.

Rozporządzenie Rady Ministrów z 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności określa minimalne wymagania dla rejestrów publicznych i przepisy dot. wymiany informacji w postaci elektronicznej. Rozporządzenie to nakłada na podmioty publiczne liczne obowiązki w trzech podstawowych obszarach: polityka bezpieczeństwa, minimalne wymagania dla systemów informatycznych, wytyczne z zakresu bezpieczeństwa sieci informatycznych. Do ważniejszych wymogów KRI należy ochrona przetwarzanych informacji przed kradzieżą, zakłóceniami czy nieuprawnionym dostępem.

Opinia audytora w sprawie adekwatności, skuteczności i efektywności kontroli zarządczej w obszarze ryzyka objętym zadaniem:

Kontrola zarządcza w jednostkach sektora finansów publicznych obejmuje 5 grup zagadnień, tj. środowisko wewnętrzne, cele i zarządzanie ryzykiem, mechanizmy kontroli,

informację i komunikację, monitorowanie i ocenę. Ogólne cele kontroli zarządczej, określone w ustawie obejmują zapewnienie w szczególności:
- zgodności działalności z przepisami prawa oraz procedurami wewnętrznymi, czyli legalności działania;
- skuteczności i efektywności działania;
- wiarygodności sprawozdań,
- ochrony zasobów,
- przestrzegania i promowania zasad etycznego postępowania (środowisko wewnętrzne).
- efektywności i skuteczności przepływu informacji (informacja i komunikacja).
- zarządzania ryzykiem (cele i zarządzanie ryzykiem), które ma na celu zwiększenie prawdopodobieństwa i realizacji zadań.

W zakresie oceny kontroli zarządczej w obszarze bezpieczeństwa informacji audytujący wskazuje na następujące zapisy w Standardach Kontroli Zarządczej dla Sektora Finansów Publicznych opublikowanych Komunikatem Nr 23 Ministra Finansów z dnia 16 grudnia 2009 r. w sprawie standardów kontroli zarządczej dla sektora finansów publicznych:
C. Mechanizmy kontroli:
12. Ciągłość działalności
Należy zapewnić istnienie mechanizmów służących utrzymaniu ciągłości działalności jednostki sektora finansów publicznych wykorzystując, między innymi, wyniki analizy ryzyka.
13. Ochrona zasobów
Należy zadbać, aby dostęp do zasobów jednostki miały wyłącznie upoważnione osoby. Osobom zarządzającym i pracownikom należy powierzyć odpowiedzialność za zapewnienie ochrony i właściwe wykorzystanie zasobów jednostki.
15. Mechanizmy kontroli dotyczące systemów informatycznych
Należy określić mechanizmy służące zapewnieniu bezpieczeństwa danych i systemów informatycznych.

Jednocześnie Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych w § 20 wskazuje na minimalne wymagania w zakresie systemu zapewnienia bezpieczeństwa informacji oraz określa, iż mogą one być spełnione poprzez spełnienie wymagań standardu PN-ISO-IEC-27001 do budowy systemu bezpieczeństwa informacji.

Przeprowadzona ocena funkcjonowania systemu zapewnienia ubezpieczenia informacji w jednostce audytowanej pozwala na ocenę pozytywną kontroli zarządczej w badanym obszarze zastrzeżeniami **z zastrzeżeniami** tzn., iż **w ograniczonym stopniu funkcjonowała adekwatna, skuteczna i efektywna kontrola zarządcza** w zakresie bezpieczeństwa informacji.

Realizując nałożone przepisami ustawy o finansach publicznych obowiązki w zakresie wdrożenia standardów kontroli zarządczej, kierownik jednostki powinien uwzględnić

powyższe wytyczne w funkcjonujących procedurach regulujących obszar systemów informatycznych.

Stwierdzić należy, że system kontroli zarządczej w badanym obszarze funkcjonuje w stopniu zapewniającym realizację nałożonych zadań zgodnie z przepisami prawa, terminowo i efektywnie. Stosowane procedury zapewniają pożądany poziom kontroli zarządczej w zakresie ochrony zasobów oraz ustanowionych mechanizmów kontroli.

Biorąc pod uwagę zawarte w niniejszym sprawozdaniu ustalenia stanu faktycznego, oceniając funkcjonujący w badanym obszarze system kontroli zarządczej nie stwierdzono słabości kontroli zarządczej.