AW.1721.2.2024

SPRAWOZDANIE Z WYKONANIA PLANU AUDYTU WEWNĘTRZNEGO NA ROK 2023

1. Jednostki organizacyjne objęte audytem wewnętrznym

Lp.	Rodzaj jednostki	*Nazwa jednostki*
1.	Jednostka zatrudniająca audytora wewnętrznego	Starostwo Powiatowe w Wodzisławiu Śląskim
2.	Jednostki objęte audytem wewnętrznym w roku sprawozdawczym	1. Starostwo Powiatowe w Wodzisławiu Śląskim. 2. Powiatowe Centrum Pomocy Rodzinie w Wodzisławiu Śląskim. *3.* Zespół Szkół Ekonomicznych w Wodzisławiu Śląskim.

2. Podstawowe informacje o komórce audytu wewnętrznego

Lp.	Imię i nazwisko	Nazwa stanowiska	Wymiar czasu pracy [etaty/osobodni]	*Kwalifikacje zawodowe*
1.	Mariusz Hałacz	Audytor wewnętrzny	Zatrudnienie: 0,5 etatu / 125 osobodni	Uprawnienia audytora wewnętrznego jednostek sektora finansów publicznych na podstawie art. 286 ust. 1 pkt 5 lit. d ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych: • Studia podyplomowe „Audyt wewnętrzny w jednostkach sektora finansów publicznych” (Akademia Ekonomiczna w Katowicach) • Dwuletnia praktyka w zakresie audytu wewnętrznego (zaświadczenie Starosty Wodzisławskiego o odbyciu praktyki – BKR.224.34.2020 z dnia 16.09.2020 r.)

3. Przeprowadzone zadania audytowe w roku sprawozdawczym

Lp.	Nazwa zadania audytowego – rodzaj zadania	Nazwa obszaru ryzyka	Planowany czas realizacji zadania [osobodni]	Faktyczny czas realizacji zadania [osobodni]	Uwagi
1.	**Prowadzenie spraw związanych z udzielaniem dotacji podmiotowi leczniczemu niebędącemu przedsiębiorcą**	Promocja i ochrona zdrowia / Wydział Zdrowia i Polityki Społecznej	20	20	
2.	**Gromadzenie, prowadzenie i udostępnianie powiatowego zasobu geodezyjnego i kartograficznego oraz kontrola opracowań przyjmowanych do zasobu**	Geodezja, kartografia i kataster / Wydział Geodezji	25	20	W trakcie realizacji - kontynuacja zadania w 2024 roku
3.	**Audyt polityki bezpieczeństwa informacji w Powiatowym Centrum Pomocy Rodzinie w Wodzisławiu Śląskim**	Polityka bezpieczeństwa informacji, przetwarzanie danych osobowych, ochrona danych / Powiatowe Centrum Pomocy Rodzinie w Wodzisławiu Śląskim	10	14	
4.	**Audyt polityki bezpieczeństwa informacji w Zespole Szkół Ekonomicznych w Wodzisławiu Śląskim**	Polityka bezpieczeństwa informacji, przetwarzanie danych osobowych, ochrona danych / Zespół Szkół Ekonomicznych w Wodzisławiu Śląskim	10	11	

4. Wyniki realizacji zadań audytowych

Lp.	Nazwa zadania audytowego – rodzaj zadania	Zidentyfikowane istotne ryzyka i słabości kontroli zarządczej	*Podstawowe zalecenia, opinie i wnioski poaudytowe*
1.	Prowadzenie spraw związanych z udzielaniem dotacji podmiotowi leczniczemu	1. Zapisy w umowie dotacji dające możliwości odmiennej ich interpretacji. 2. Nieobjęcie w umowach wszystkich praw i	1. Wdrożyć skuteczne mechanizmy weryfikacji złożonych wniosków o dotacje, służące wyeliminowaniu braków merytorycznych w tych dokumentach. 2. Przeprowadzić pogłębioną analizę prawną treści zawartych umów

Lp.	Nazwa zadania audytowego – rodzaj zadania	Zidentyfikowane istotne ryzyka i słabości kontroli zarządczej	*Podstawowe zalecenia, opinie i wnioski poaudytowe*
	niebędącemu przedsiębiorcą	obowiązków stron umowy.	dotacyjnych oraz na podstawie jej wyników doprecyzować / zmodyfikować zapisy w „nowych” umowach dotacyjnych. 3. Zwiększyć intensywność przeprowadzanych kontroli w podmiotach leczniczych w zakresie wykorzystania dotacji celowych. 4. Wzmocnić mechanizmy, które pozwolą na jednorodny sposób postępowania przy udzielaniu dotacji w reżimie art. 114 ust. 1 pkt 4 ustawy o działalności leczniczej. 5. Przestrzegać zapisy umowne oraz realizować prawa i obowiązki wynikające z treści podpisanych umów.
2.	Audyt polityki bezpieczeństwa informacji w Powiatowym Centrum Pomocy Rodzinie w Wodzisławiu Śląskim	1. Nieuwzględnienie w dokumentacji polityki bezpieczeństwa ochrony danych i obowiązujących instrukcjach wszystkich istotnych elementów przyczyniających się do zapewnienia poufności, dostępności i integralności danych. 2. Niepełny sposób informowania kierownictwa o zagrożeniach związanych z przetwarzaniem informacji. 3. Brak utrzymania aktualności inwentaryzacji sprzętu i oprogramowania do przetwarzania informacji. 4. Wskazanie w upoważnieniach do przetwarzania danych osobowych wydanych przed 25 maja 2018 r. jako podstawy prawnej wydania takiego upoważnienia, ustawy, która nie obowiązuje. 5. Nieaktualne zakresy czynności, upoważnienia do przetwarzania danych osobowych w kontekście ewidencji nadanych uprawnień do systemów informatycznych. 6. Niewystarczająca wiedza użytkowników w zakresie	1. Przeprowadzić aktualizację Polityki bezpieczeństwa ochrony danych osobowych w kontekście spełnienia norm, o których mowa w § 20 rozporządzenia KRI. 2. Przeprowadzić całościowy przegląd regulacji wewnętrznych dotyczących systemu bezpieczeństwa danych osobowych pod kątem identyfikacji formalnego zakresu stosowania poszczególnych zabezpieczeń (dane osobowe vs. wszystkie informacje wymagające zachowania poufności, dostępności i integralności). 3. Uwzględnić w regulacjach wewnętrznych dotyczących systemu bezpieczeństwa danych osobowych ścieżki postępowania dotyczącej zgłaszania incydentów bezpieczeństwa do wyznaczonej osoby w Starostwie Powiatowym w Wodzisławiu Śląskim w zakresie związanym z wymogami KSC. 4. Uszczegółowić obowiązujące regulacje wewnętrzne dotyczące systemu bezpieczeństwa danych osobowych o zasady dokumentowania, szczegółowe terminy, okresy tworzenia, przechowywania oraz testowania kopii zapasowych danych i systemów podmiotu. 5. Analizę ryzyka przeprowadzać, co najmniej raz w roku z uwzględnieniem wszystkich przetwarzanych danych a nie tylko danych osobowych.

Lp.	Nazwa zadania audytowego – rodzaj zadania	Zidentyfikowane istotne ryzyka i słabości kontroli zarządczej	*Podstawowe zalecenia, opinie i wnioski poaudytowe*
		zapewnienia poufności, dostępności i integralności informacji. 7. Możliwość utraty poufności informacji urzędu podczas korzystania z mobilnych urządzeń do przetwarzania danych. 8. Brak możliwości egzekwowania przez Zamawiającego naruszenia przez Wykonawcę zapisów dot. poufności informacji. 9. Nieskuteczny proces zgłaszania incydentów bezpieczeństwa informacji w kontekście realizacji ustawy o krajowym systemie cyberbezpieczeństwa. 10. Niska efektywność i ograniczona skuteczność zidentyfikowania słabości funkcjonowania systemu bezpieczeństwa informatycznego w jednostce. 11. Ograniczona wiedza organizacji w zakresie poprawności konfiguracji kopii zapasowych oraz posiadanej sprawności w odtwarzaniu danych z kopii zapasowych. 12. Nieuwzględnienie w dokumentacji polityki bezpieczeństwa ochrony danych i obowiązujących instrukcji procesu projektowania, wdrażania i eksploatacji systemów teleinformatycznych. 13. Niepełne respektowanie zapisów obowiązujących regulacji wewnętrznych w zakresie bezpieczeństwa danych przez pracowników PCPR. 14. Niska efektywność monitorowania wykorzystywania sprzętu. 15. Niski poziom zautomatyzowania dostępnych narzędzi do monitorowania w	6. Utworzyć rejestr, który w sposób wyczerpujący i szczegółowy określi wszystkie najistotniejsze parametry stanowiska komputerowego. 7. Przeprowadzić analizę i na podstawie jej wyników przy uwzględnieniu zapisów w zakresach czynności dostosować treść wydanych przed 25 maja 2018 r. upoważnień do przetwarzania danych osobowych do obowiązującego rozporządzenia 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. 8. Zweryfikować pod względem zgodności z ewidencją nadanych uprawnień do systemów informatycznych i obowiązujących zakresów czynności, wydane upoważnienia do przetwarzania danych osobowych. 9. Przeanalizować możliwość zastosowanie rozwiązania polegającego na szyfrowaniu dysków twardych komputerów przenośnych. 10. Przeprowadzić analizę prawną zagadnienia związanego z zachowaniem przez Wykonawcę tajemnicy co do uzyskanych informacji i usuwaniem niezbędnych pozyskanych danych na etapie realizacji umowy oraz w oparciu o wyniki tej analizy wprowadzić ewentualną modyfikację dotychczasowych praktyk. 11. Przeprowadzać audyty bezpieczeństwa w zakresie bezpieczeństwa informacji nie rzadziej niż raz w roku. 12. W regulacjach wewnętrznych dotyczących systemu bezpieczeństwa danych osobowych ustanowić proces wdrażania systemów informatycznych, który określałby sposób dostarczania i instalacji systemu teleinformatycznego oraz wymagania sprzętowe. 13. Wyłączyć opcję autouzupełniania formularzy na wszystkich komputerach i usunąć zapamiętane hasła. 14. Zainstalować na komputerach systemy operacyjne, spełniające

Lp.	Nazwa zadania audytowego – rodzaj zadania	Zidentyfikowane istotne ryzyka i słabości kontroli zarządczej	*Podstawowe zalecenia, opinie i wnioski poaudytowe*
		stosunku do występujących i narastających zagrożeń. 16. Okresowe przeglądanie logów systemowych.	minimalne wymagania systemowe oraz takie, które gwarantują aktualność oraz bezpieczeństwo przetwarzania informacji. 15. Wprowadzić nadzór i monitoring nad korzystaniem z portów USB, czytników kart pamięci, bluetooth oraz dysków CD/DVD oraz uwzględnić przyjęte rozwiązania w dokumentacji polityki bezpieczeństwa danych osobowych w PCPR. 16. Rozważyć opracowanie „świadomej" polityki logów, w celu umożliwienia zarówno bieżącego nadzorowania systemów jak również objęcia skuteczną analizą wszystkich kluczowych zdarzeń związanych z uzyskiwaniem przez użytkowników dostępu do systemów informatycznych i przetwarzanych w nich danych. 17. Wdrożyć rozwiązania zapewniające odpowiednie zabezpieczenie urządzenia sieciowego typu NAS (Synology DS. 918+).
3.	Audyt polityki bezpieczeństwa informacji w Zespole Szkół Ekonomicznych w Wodzisławiu Śląskim	1. Nieuwzględnienie w dokumentacji polityki bezpieczeństwa ochrony danych i obowiązujących instrukcjach wszystkich istotnych elementów przyczyniających się do zapewnienia poufności, dostępności i integralności danych. 2. Niepełny sposób informowania kierownictwa o zagrożeniach związanych z przetwarzaniem informacji. 3. Brak utrzymania aktualności inwentaryzacji sprzętu i oprogramowania do przetwarzania informacji. 4. Nieregularny proces aktualizacji uprawnień osób zaangażowanych w proces przetwarzania danych. 5. Niewystarczająca wiedza użytkowników w zakresie zapewnienia poufności, dostępności i integralności informacji.	1. Przeprowadzić całościowy przegląd regulacji wewnętrznych dotyczących systemu bezpieczeństwa danych osobowych w zakresie zgodnym z przeprowadzonym audytem wewnętrznym i w wyniku przeprowadzonej analizy dokonać stosownych zmian, aktualizacji, uzupełnień, w tym spełnienia wymogów KRI. 2. Wdrożyć rozwiązania umożliwiające elastyczne zarządzanie uprawnieniami i szybką zmianę dostępu w przypadku zmiany zadań. 3. Opracować program szkoleniowy, który będzie obejmował wszystkie istotne zagadnienia związane z bezpieczeństwem informacji. 4. Dokonać aktualizacji zarządzenia nr 28/2022 Dyrektora Zespołu Szkół Ekonomicznych w Wodzisławiu Śląskim o wyróżnienie modeli wykorzystania komputerów służbowych i prywatnych w edukacji zdalnej. 5. Przeprowadzić analizę prawną stosowanych zapisów w umowach serwisowanych w zakresie wskazanym w audycie oraz w oparciu o wyniki tej analizy wprowadzić

Lp.	Nazwa zadania audytowego – rodzaj zadania	Zidentyfikowane istotne ryzyka i słabości kontroli zarządczej	*Podstawowe zalecenia, opinie i wnioski poaudytowe*
		6. Możliwość utraty poufności informacji szkoły podczas prowadzenia edukacji zdalnej. 7. Brak możliwości egzekwowania przez Zamawiającego naruszenia przez Wykonawcę zapisów dot. poufności informacji. 8. Nieskuteczny proces zgłaszania incydentów bezpieczeństwa informacji w kontekście realizacji ustawy o krajowym systemie cyberbezpieczeństwa. 9. Niska efektywność i ograniczona skuteczność zidentyfikowania słabości funkcjonowania systemu bezpieczeństwa informatycznego w jednostce. 10. Ograniczona wiedza organizacji w zakresie poprawności konfiguracji kopii zapasowych oraz posiadanej sprawności w odtwarzaniu danych z kopii zapasowych. 11. Nieuwzględnienie w dokumentacji polityki bezpieczeństwa ochrony danych i obowiązujących instrukcji procesu projektowania, wdrażania i eksploatacji systemów teleinformatycznych. 12. Utrata informacji w wyniku awarii. 13. Ograniczone możliwości analizy ruchu sieciowego. 14. Niska efektywność monitorowania wykorzystywania sprzętu. 15. Niski poziom zautomatyzowania dostępnych narzędzi do monitorowania w stosunku do występujących i narastających zagrożeń. 16. Okresowe przeglądanie logów systemowych	ewentualną modyfikację dotychczasowych praktyk. 6. Uzupełnić system podtrzymywania zasilania sprzętu komputerowego w elementy niezbędne dla zminimalizowania ryzyka utraty informacji oraz zapewnienia ciągłości działalności jednostki. 7. Zautomatyzować proces zarządzania sprzętem i oprogramowaniem wykorzystywanym w systemie informatycznym szkoły. 8. Wdrożyć system analizy ruchu sieciowego. 9. Usunąć nieużytkowany sprzęt komputerowy z inwentaryzacji szkoły. 10. Wprowadzić nadzór i monitoring nad korzystaniem z portów USB, czytników kart pamięci, bluetooth oraz dysków CD/DVD oraz uwzględnić przyjęte rozwiązania w dokumentacji polityki bezpieczeństwa danych osobowych w ZSE. 11. Rozważyć opracowanie „świadomej” polityki logów, w celu umożliwienia zarówno bieżącego nadzorowania systemów jak również objęcia skuteczną analizą wszystkich kluczowych zdarzeń związanych z uzyskiwaniem przez użytkowników dostępu do systemów informatycznych i przetwarzanych w nich danych.

5. Przeprowadzone czynności sprawdzające w roku sprawozdawczym

Lp.	Nazwa zadania zapewniającego, którego dotyczą czynności sprawdzające	Ustalenia czynności sprawdzających	Planowany czas realizacji zadania [osobodni]	Faktyczny czas realizacji zadania [osobodni]	Uwagi
1.	Kopie bezpieczeństwa w systemach informatycznych	Szczegółowe informacje z przeprowadzonych czynności sprawdzających znajdują się w notatce informacyjnej o sygnaturze AW.1720.3.2022 z dnia 21.03.2023 r. Zalecenie 1) – zrealizowano Zalecenie 2) – zrealizowano Zalecenie 3) – zrealizowano Zalecenie 4) – nie zrealizowano Zalecenie 5) - zrealizowano	5	5	
2.	System zarządzania bezpieczeństwem informacji	Szczegółowe informacje z przeprowadzonych czynności sprawdzających znajdują się w notatce informacyjnej o sygnaturze AW.1720.2.2022 z dnia 21.02.2023 r. Zalecenie 1) – zrealizowano Zalecenie 2) – częściowo zrealizowano Zalecenie 3) – zrealizowano Zalecenie 4) – zrealizowano Zalecenie 5) – brak uwag Zalecenie 6) – częściowo zrealizowano	5	5	
3.	Realizacja dochodów z nieruchomości powiatu	Szczegółowe informacje z przeprowadzonych czynności sprawdzających znajdują się w notatce informacyjnej o sygnaturze AW.1720.1.2023 z dnia 20.02.2023 r. Zalecenie 1) – zrealizowano Zalecenie 2) – nie zrealizowano Zalecenie 3) – zrealizowano Zalecenie 4) – zrealizowano Zalecenie 5) – zrealizowano Zalecenie 6) – zrealizowano	5	5	
4.	Realizacja zadań starosty w sprawach zarządzania kryzysowego		5	2	W trakcie realizacji - kontynuacja zadania w 2024 roku

6. Przeprowadzone czynności doradcze w roku sprawozdawczym

Lp.	Nazwa zadania audytowego – rodzaj zadania	Planowany czas realizacji zadania [osobodni]	Faktyczny czas realizacji zadania [osobodni]	*Wybrane czynności audytora*
1.	Analiza spełnienia na poziomie Starostwa Powiatowego w Wodzisławiu Śląskim oraz jednostek organizacyjnych Powiatu Wodzisławskiego wymogów w zakresie Systemu Zarządzania Bezpieczeństwem Informacji	1	11	1. Przygotowanie struktury arkusza kalkulacyjnego umożliwiającego przeprowadzenie sprawnej ankietyzacji. 2. Analiza spełnienia na poziomie Starostwa Powiatowego w Wodzisławiu Śląskim oraz jednostek organizacyjnych Powiatu Wodzisławskiego wymogów w zakresie systemu zarządzania bezpieczeństwem informacji. *3.* Opracowanie zbiorczej informacji w zakresie spełnienia na poziomie Starostwa Powiatowego w Wodzisławiu Śląskim oraz jednostek organizacyjnych Powiatu.

7. Znaczące odstępstwa od realizacji planu audytu

Nie dotyczy

8. Inne istotne informacje dotyczące prowadzenia audytu wewnętrznego w roku sprawozdawczym

a) Zaangażowanie audytora wewnętrznego w realizację zadań niezwiązanych z audytem wewnętrznym wynika z konieczności wykonywania przez niego również zadań przypisanych do realizacji przez Wydział Funduszy Zewnętrznych i Zamówień Publicznych w zakresie pozyskiwania środków pozabudżetowych.

15.01.2024 /-/ Mariusz Hałacz

data *podpis i pieczątka audytora*