Starostwo Powiatowe
ul. Krótka 1
19-500 Gołdap

Rzeszów, dn. 25 maja 2024 r.

AW 1720. 1 .2024

Egz. nr 1

Sprawozdanie
z zadania audytowego przeprowadzonego na rzecz Powiatu gołdapskiego

Temat: Audyt bezpieczeństwa informacji i ochrony danych osobowych

w Poradni Psychologiczno-Pedagogicznej w Gołdapi

Audytor wewnętrzny:

Łukasz Skowroński

Zadanie audytowe przeprowadzono zgodnie ze standardami audytu wewnętrznego

STAROSTWO POWIATOWE
W GOŁDAPI
19-500 Gołdap, ul. Krótka 1
tel. 87 615-44-44, fax 87 615-44-45

Za zgodność z oryginałem
stwierdzam na str. 1 do str. 24
Gołdap dn. 25.05.2024

Z up. STAROSTY
mgr Anna Makowska
SEKRETARZ POWIATU

I. Wstęp

Zadanie audytowe zostało przeprowadzone zgodnie z planem audytu wewnętrznego na rok 2024 w Powiecie gołdapskim.

Zadanie audytowe przeprowadził audytor wewnętrzny realizujący zlecenie na rzecz Powiatu gołdapskiego:

- Łukasz Skowroński - audytor wewnętrzny, na podstawie upoważnienia do przeprowadzenia zadania audytowego;

II. Temat i cel zadania zapewniającego:

Temat zadania zapewniającego:

Audyt bezpieczeństwa informacji i ochrony danych osobowych w Poradni Psychologiczno-Pedagogicznej w Gołdapi.

Cel zadania zapewniającego:

- Racjonalne zapewnienie kierownika jednostki, że obowiązujące w jednostce mechanizmy kontrolne i schematy działania dotyczące bezpieczeństwa informacji są zgodne z przepisami powszechnie obowiązującego prawa.
- Racjonalne zapewnienie kierownika jednostki, że funkcjonujący w jednostce system bezpieczeństwa informacji zapewnia optymalną ochronę informacji przed nieautoryzowanym dostępem.
- Racjonalne zapewnienie kierownika jednostki, że zastosowane w systemie mechanizmy zarządzania informacją, jak również mechanizmy kontroli zarządczej są adekwatne do znaczenia audytowanych procesów w ramach funkcjonowania całej jednostki.

W wyniku przeglądu wstępnego audytorzy postanowili objąć zadaniem audytowym następujące obszary ryzyka:

- Adekwatność i aktualność regulacji wewnętrznych w zakresie dotyczącym ochrony danych osobowych.

- Przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy.
- Podział kompetencji pomiędzy osoby zaangażowane w zarządzanie bezpieczeństwem informacji.
- Ochrona przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami.
- Zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie.
- Ustalenia zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych.
- Zapewnienia odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych.

III. Zakres podmiotowy i przedmiotowy zadania zapewniającego:

Zakresem przedmiotowym zadania audytowego objęto analizę systemu bezpieczeństwa informacji, kwestię podziału obowiązków osób zaangażowanych w zarządzanie bezpieczeństwem informacji, oraz kwestię ochrony danych osobowych.

IV. Podjęte działania i zastosowane techniki przeprowadzania zadania audytowego:

W trakcie zadania audytowego przeprowadzone zostały rozmowy z pracownikami jednostki bezpośrednio zaangażowanymi w przebieg procesu zarządzania bezpieczeństwem informacji. Sporządzono listę pytań kontrolnych, przeprowadzono testy zgodności i testy kroczące, poddano analizie całość dokumentacji powstałej w procesie zarządzania bezpieczeństwem informacji.

Data rozpoczęcia zadania: 24 kwietnia 2024 r.

Ustalenia i ocena: według kryteriów przyjętych w programie o którym mowa w § 16 ust. 1 Rozporządzenia Ministra Finansów z dnia 4 września 2015 r. w sprawie audytu wewnętrznego oraz informacji o pracy i wynikach tego audytu (Dz. U. 2018 r., poz. 506)

Podstawa prawna:

1. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. 2018 poz. 1000 ze zm.);
2. 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.2012.526), zwane dale „Rozporządzeniem".
3. 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).
4. Zarządzenie nr 39/2021 Dyrektora Poradni Psychologiczno-Pedagogicznej w Gołdapi w sprawie wprowadzenia Polityki Bezpieczeństwa przetwarzania danych osobowych w Poradni Psychologiczno-Pedagogicznej w Gołdapi, Instrukcji Zarządzania systemem informatycznym w Poradni Psychologiczno-Pedagogicznej w Gołdapi oraz Polityki Bezpieczeństwa informacji w Poradni Psychologiczno-Pedagogicznej w Gołdapi.

Kryterium audytu była w szczególności treść § 20. 2 Rozporządzenia 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.2012.526), według treści którego zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie następujących działań:

1. zapewnienia aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia;
2. przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy;

3. podejmowania działań zapewniających, 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 mających na celu zapewnienie bezpieczeństwa informacji;

4. bezzwłocznej zmiany uprawnień, w przypadku zmiany zadań osób, o których mowa w pkt 4;

5. zapewnienia szkolenia osób zaangażowanych w proces przetwarzania informacji ze szczególnym uwzględnieniem takich zagadnień, jak:

   a) zagrożenia bezpieczeństwa informacji,

   b) skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna,

   c) stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich;

6. zapewnienia ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, przez:

   a) monitorowanie dostępu do informacji;

   b) czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji;

   c) zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji;

7. ustanowienia podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość;

8. zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie;

9. zawierania w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji;

10. ustalenia zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych;

11. zapewnienia odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na:

a) dbałości o aktualizację oprogramowania,
b) minimalizowaniu ryzyka utraty informacji w wyniku awarii,
c) ochronie przed błędami, utratą, nieuprawnioną modyfikacją,
d) stosowaniu mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa,
e) zapewnieniu bezpieczeństwa plików systemowych,
f) redukcji ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych,
g) niezwłocznym podejmowaniu działań po dostrzeżeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa,
h) kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa;

12. bezzwłocznego zgłaszania incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących.

Opis stanu faktycznego:

Obszar nr 1: Zapewnienie aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia (§ 20 ust. 2, pkt. 1)

Sposób przeprowadzenia czynności audytowych:

- Analiza aktów wewnętrznych dot. bezpieczeństwa informacji.
- Uzyskiwanie wyjaśnień i informacji od osób odpowiedzialnych za prawidłowe funkcjonowanie systemu bezpieczeństwa informacji oraz od innych pracowników jednostki.
- Zapoznawanie się z innymi dokumentami służbowymi, na podstawie których można będzie dokonać ustalenia stanu faktycznego w badanym zakresie.

TREŚĆ PYTANIA	ODPOWIEDZI		DOWÓD W PRZYPADKU ZAZNACZENIA "TAK"
	TAK	NIE	

1.	Czy w regulacjach wewnętrznych są zapisy dotyczące przeprowadzania przeglądu dokumentacji bezpieczeństwa jednostce?	x		Arkusze aktualizacyjne
2.	Czy w regularnych odstępach czasowych i przez kogo wykonywany jest przegląd dokumentacji bezpieczeństwa celem zapewnienia, że pozostaje ona przydatna, adekwatna i skuteczna?	x		IOD
3.	Czy obowiązki w zakresie opracowania, przeglądu i oceny dokumentacji bezpieczeństwa przypisane są określonym osobom? W jakich dokumentach?	x		IOD; Powołanie IOD do pełnienia tej funkcji w jednostkach powiatowych nastąpiło na mocy Zarządzenia Starosty
4.	Czy w latach 2018-2022 aktualizowano dokumentację bezpieczeństwa? (podać datę ostatniej aktualizacji)	x		7.02.2024
5.	Czy zmiany w dokumentacji bezpieczeństwa informacji zostały zatwierdzone przez kierownictwo jednostki?	x		Akceptacja arkusza aktualizacyjnego; Dokumentacja została wprowadzona w życie zarządzeniem dyrektora jednostki
6.	Czy określono, że poza harmonogramem aktualizacja powinna następować w przypadku: - zmian struktury? - zmiany regulacji zewnętrznych i wewnętrznych mających wpływ na bezpieczeństwo informacji? - informacji o trendach związanych z zagrożeniami i podatnościami systemów informatycznych? – informacji o incydentach dotyczących bezpieczeństwa informacji?	X		

Rekomendacje: brak

Obszar nr 2: Utrzymywanie aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację (§ 20 ust. 2, pkt. 2)

Sposób przeprowadzenia czynności audytowych:

- Analiza aktów wewnętrznych dot. inwentaryzacji oraz zarządzania majątkiem.
- Uzyskiwanie wyjaśnień i informacji od osób odpowiedzialnych za prawidłowe funkcjonowanie systemu bezpieczeństwa informacji oraz od innych pracowników jednostki.
- Zapoznawanie się z dokumentami służbowymi, na podstawie których można będzie dokonać ustalenia stanu faktycznego w badanym zakresie.

TREŚĆ PYTANIA		ODPOWIEDZI		DOWÓD W PRZYPADKU ZAZNACZENIA "TAK"
		TAK	NIE	
1.	Czy określono zasady przeprowadzania inwentaryzacji	x		Zgodnie z przepisami prawa; Zarządzenie Dyrektora PPP w sprawie ustalenia przyjętych zasad polityki rachunkowości, instrukcji gospodarki majątkiem trwałym, inwentaryzacji majątki i zasad odpowiedzialności za powierzone mienie
2.	Czy i jakie grupy aktywów zostały zidentyfikowane?	x		Środki trwałe, pozostałe środki trwałe, wartości niematerialne i prawne,
3.	Czy i w jaki sposób dokumentowane są wyniki inwentaryzacji aktywów?	x		Spisy z natury, protokoły, sprawozdanie z inwentaryzacji, uzgodnienie sald, aktywów i pasywów, wycena aktywów i pasywów; spisy inwentaryzacyjne sporządzane przez zespoły inwentaryzacyjne i dokumentowanie bieżących działań dokonywanych przez informatyków
4.	Jakie informacje zawiera spis aktywów?	x		Stacje robocze, urządzenia brzegowe, licencje - wszelkie potrzebne informacje do odtworzenia po potencjalnej katastrofie
5.	Czy ewidencja odzwierciedla stan faktyczny? Czy zapewnia się aktualność spisu inwentaryzacyjnego w przypadku likwidacji sprzętu?	x		W przypadku likwidacji sprzętu, sporządzany jest protokół zniszczenia ze wskazaniem nr inwentarzowego, wartości zakupu i nazwy likwidowanego składnika; wszystkie aktywa są jasno zidentyfikowane oraz powinien być sporządzony i utrzymywany spis wszystkich ważnych aktywów

6.	Czy poszczególne grupy aktywów posiadają swoich właścicieli?	x		W jednostce zastosowano mechanizm personalizacji odpowiedzialności poprzez powierzenie mienia; aktywa mają właściciela - są przypisane do konkretnych osób
7.	Czy obowiązki związane z bezpieczeństwem informacji przypisano właścicielom aktywów	x		Obowiązki te mogą wynikać np. z zakresów czynności lub mogą być określone w innych dokumentach.
8.	Czy zapewnia się i w jaki sposób, że właściciele aktywów realizują swoje obowiązki związane z zapewnieniem bezpieczeństwa?	x		Formalne przyjęcie powierzonego mienia (umowy o przyjęciu odpowiedzialności za powierzone mienie)
9.	Czy właściciele aktywów mają do dyspozycji zasoby, które służą zapewnieniu bezpieczeństwa?	x		zabezpieczenia fizyczne, ograniczenia systemowe

Rekomendacje: brak

Obszar nr 3: Przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy (§ 20 ust. 2, pkt. 3)

Sposób przeprowadzenia czynności audytowych:

- Analiza aktów wewnętrznych dot. zarządzania ryzykiem.
- Uzyskiwanie wyjaśnień i informacji od osób odpowiedzialnych za prawidłowe funkcjonowanie systemu bezpieczeństwa informacji oraz od innych pracowników jednostki.
- Zapoznawanie się z dokumentami służbowymi, na podstawie których można będzie dokonać ustalenia stanu faktycznego w badanym zakresie.

	ODPOWIEDZI	DOWÓD W

	TREŚĆ PYTANIA	TAK	NIE	PRZYPADKU ZAZNACZENIA „TAK”
1.	Czy zarządzanie ryzykiem w jednostce obejmuje zarządzanie ryzykiem w obszarze bezpieczeństwa informacji?	x		Analiza ryzyka
2.	Czy zarządzanie ryzykiem w obszarze bezpieczeństwa informacji jest integralną częścią zarządzania bezpieczeństwem informacji zarówno na etapie wdrożenia jak i podczas eksploatacji?	x		
3.	Czy w ramach szacowania ryzyka dokonano kategoryzacji skutków ryzyka ze względu na utratę integralności, dostępności oraz poufności informacji?	x		
4.	Czy przeprowadzono analizę i ocenę ryzyka?	x		
5.	Czy w ramach postępowania z ryzykiem określono kryteria (poziom) ryzyka akceptowalnego?	x		
6.	Jaki wariant sposobu postępowania z ryzykiem wdrożono w jednostce: a) wprowadzenie zabezpieczeń zmniejszających ryzyko? b) zaakceptowanie ryzyka pod warunkiem spełnienia kryteriów ryzyka akceptowalnego? c) niedopuszczenie działań, które mogą zwiększyć ryzyko? (unikanie ryzyka) d) przeniesienia ryzyka na inne podmioty?	x		
7.	Czy określono działania minimalizujące ryzyko utraty integralności, dostępności lub poufności informacji?	x		

Rekomendacje: brak

Obszar nr 4: Podejmowanie działań zapewniających, 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 mających na celu zapewnienie bezpieczeństwa informacji (§ 20 ust. 2, pkt. 4).

Sposób przeprowadzenia czynności audytowych:

- Analiza aktów wewnętrznych dot. naboru kandydatów do pracy oraz nadawania i odbierania uprawnień.
- Uzyskiwanie wyjaśnień i informacji od osób odpowiedzialnych za nadawanie i odbieranie uprawnień oraz od innych pracowników jednostki.
- Zapoznawanie się z dokumentami służbowymi, na podstawie których można będzie dokonać ustalenia stanu faktycznego w badanym zakresie (np. przegląd dokumentacji kontrolnej, ewidencji upoważnień, procedur) .
- Weryfikacja uprawnień w systemach informatycznych.

	TREŚĆ PYTANIA	ODPOWIEDZI		DOWÓD W PRZYPADKU ZAZNACZENIA "TAK"
		TAK	NIE	
1.	Czy przed przyznaniem dostępu do informacji wrażliwych i systemów krytycznych pracownik formalnie przyjął obowiązki i czy złożył zobowiązanie do zachowania tajemnicy? Czy przeszedł wymagane szkolenia?	x		Nowo zatrudniony pracownik jest każdorazowo przeszkalany; przedstawiono rejestr kart szkolenia wstępnego z zakresu ochrony danych osobowych w jednostkach organizacyjnych powiatu gołdapskiego; klauzula poufności stosowana w jednostce obowiązuje zarówno w trakcie jak i po ustaniu stosunku pracy

2.	Czy nowo zatrudnieni pracownicy pisemnie potwierdzają odpowiedzialność w zakresie zachowania poufności i nieujawniania informacji, w przypadku dostępu do danych prawnie chronionych?	x		Stosowne oświadczenie stanowi część upoważnienia do przetwarzania danych
3.	Czy opracowana została procedura zarządzania uprawnieniami (określono zasady nadawania, odbierania i weryfikacji uprawnień)?	x		W PBI; w jednostce prowadzony jest rejestr osób upoważnionych
4.	Czy i kto dokonuje okresowej weryfikacji nadanych uprawnień pracownikom?	x		PBI
5.	Czy opracowana została procedura postępowania w sytuacji naruszenia bezpieczeństwa informacji?	x		Instrukcja postępowania w sytuacjach naruszenia ochrony danych stanowi załącznik do PBI

Rekomendacje: brak

Obszar nr 5: Procedura bezzwłocznej zmiany uprawnień, w przypadku zmiany zadań osób uprawnionych do przetwarzania danych osobowych (§ 20 ust. 2, pkt. 5).

Sposób przeprowadzenia czynności audytowych:

- Analiza aktów wewnętrznych dot. nadawania, zmiany i odbierania uprawnień.
- Uzyskiwanie wyjaśnień i informacji od osób odpowiedzialnych za nadawanie i odbieranie uprawnień oraz od innych pracowników jednostki.
- Zapoznawanie się z dokumentami służbowymi, na podstawie których można będzie dokonać ustalenia stanu faktycznego w badanym zakresie.
- Dokonanie analizy porównawczej - czy zmiany w zakresie uprawnień odpowiadają złożonym wnioskom.
- Sprawdzenie odebranych uprawnień w systemach informatycznych.

	ODPOWIEDZI	DOWÓD W

	TREŚĆ PYTANIA	TAK	NIE	PRZYPADKU ZAZNACZENIA "TAK"
1.	Czy opracowano procedury definiujące proces nadawania, odbierania lub modyfikacji praw dostępu logicznego i fizycznego do aktywów organizacji w przypadku zmiany komórki organizacyjnej, zmiany zakresu obowiązków, długotrwałej nieobecności w pracy, zakończenia stosunku pracy, umowy? Czy określono w procedurach zasady dokonywania zmiany uprawnień: - kto jest odpowiedzialny, - kto i komu zgłasza zmianę zakresu zadań/uprawnień i w jakim terminie (przepływ informacji pomiędzy komórkami), - w którym momencie następuje odebranie/modyfikacja praw dostępu?		x	PBDO zawiera wskazówki dotyczące zasad postępowania przy nadawaniu/anulowaniu uprawnień, natomiast nie zawierają opisu mechanizmu działania na wypadek zmiany komórki organizacyjnej, zmiany zakresu obowiązków, długotrwałej nieobecności w pracy, zakończenia stosunku pracy, umowy
2.	Czy gromadzone są wnioski dotyczące nadawania lub odbierania praw dostępu?		nd	Program FK jest obsługiwany przez jedną osobę (czyli przysługuje jej dostęp w pełnym zakresie). Wielkość i specyfika jednostki uzasadniają brak konieczności wprowadzenia systemu zarządzania uprawnieniami.
3.	Czy jednostka zapewnia, że obowiązki wynikające z wymagań bezpieczeństwa są dopełnione po ustaniu stosunku pracy z pracownikami oraz wygaśnięciu umów z wykonawcami oraz użytkownikami stron trzecich?	x		Oświadczenie zawierające klauzulę poufności rozciągającą się zarówno w czasie trwania jak i po ustaniu stosunku pracy

Rekomendacja: brak

Obszar nr 6: Zapewnienie szkolenia osób zaangażowanych w proces przetwarzania informacji (§ 20 ust. 2, pkt. 6)

Kryterium: zapewnienia szkolenia osób zaangażowanych w proces przetwarzania informacji ze szczególnym uwzględnieniem takich zagadnień jak:

a) zagrożenia bezpieczeństwa informacji;
b) skutki naruszenia zasad bezpieczeństwa informacji w tym odpowiedzialność prawna;
c) stosowanie środków zapewniających bezpieczeństwo informacji w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich;

Sposób przeprowadzenia czynności audytowych:

- Uzyskiwanie wyjaśnień i informacji od osób odpowiedzialnych za planowanie i realizację szkoleń w zakresie bezpieczeństwa informacji oraz od innych pracowników jednostki.
- Zapoznawanie się z dokumentami służbowymi, na podstawie których można będzie dokonać ustalenia stanu faktycznego w badanym zakresie.
- W celu ustalenia czy wszyscy pracownicy zaangażowani w procesie przetwarzania informacji są szkoleni można dokonać analizy porównawczej listy pracowników zaangażowanych z listą pracowników przeszkolonych.

TREŚĆ PYTANIA	ODPOWIEDZI		DOWÓD W PRZYPADKU ZAZNACZENIA "TAK"
	TAK	NIE	

1.	Czy w jednostce opracowano plan szkoleń w zakresie bezpieczeństwa informacji i czy jest realizowany? (protokoły ze szkoleń, lista uczestników). Czy procedury wewnętrzne określają częstotliwość szkolenia pracowników?	x		Planu szkoleń jako taki nie funkcjonuje, natomiast okresowo, regularnie organizowane są szkolenia, których tematyka dotyczy bezpieczeństwa informacji; Starostwo Powiatowe opracowało plan szkoleń obejmujący starostwo oraz jednostki powiatowe.
2.	Czy obszary/zagadnienia dotyczące bezpieczeństwa są uwzględniane w programach szkoleń i czy programy są dostosowane do różnych grup odbiorców?	x		
3.	Czy pracownicy są szkoleni w zakresie: a) zagrożeń bezpieczeństwa informacji? b)skutków naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialności prawnej? c) stosowania środków zapewniających bezpieczeństwo informacji, w tym urządzeń i oprogramowania minimalizującego ryzyko błędów ludzkich?	x		

Rekomendacje: brak

Obszar nr 7: Zapewnienie ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami (§ 20 ust. 2, pkt. 7)

Kryterium: zapewnienia ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, przez;

a) monitorowanie dostępu do informacji;

b) czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji;

c) zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji.

Sposób przeprowadzenia czynności audytowych:

- Zapoznanie się z dokumentacją w zakresie bezpieczeństwa informacji.
- Sprawdzenie czy opisane w procedurach zabezpieczenia fizyczne i logiczne są stosowane.
- Wywiad z pracownikami na potwierdzenie świadomości oraz znajomości zasad obowiązujących w zakresie przetwarzania informacji oraz zgłaszania incydentów.
- Potwierdzenie formalnego zobowiązania pracowników do ochrony informacji (czy odbywa się to poprzez zapis w zakresie obowiązków czy również w formie zobowiązania składanego przy przyjęciu do pracy).
- Sprawdzenie czy administrator dokonuje przeglądu logów systemowych i czy jest to dokumentowane? (dla każdego systemu prowadzony jest oddzielny dziennik systemowy - wszystkie dzienniki mogą być w jednym dokumencie. W dzienniku systemowym powinien być zapis, że administrator przeglądał logi systemowe. W dzienniku będą również inne zapisy np. o dokonaniu zmiany hasła, o przerwach w zasilaniu, o wykonywaniu kopii).
- Uzyskanie potwierdzenia istnienia rejestru incydentów. Dokonanie przeglądu zarejestrowanych incydentów i sprawdzenie czy podjęto działania w odpowiedzi na zagrożenia wynikające z incydentów.
- Dokonanie analizy porównawczej nadanych uprawnień z wnioskami o ich nadanie.
- Ustalenie jakie są stosowane środki uniemożliwiające nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji? (np. czy przy logowaniu się do systemu trzeba podać login i hasło, czy hasło wygasa po 30 dniach, jaka jest złożoność hasła (8 znaków itp.), z poziomu administratora można uzyskać informację o zmianie hasła – będą zapisy o tym w dziennikach systemowych)

TREŚĆ PYTANIA	ODPOWIEDZI		DOWÓD W PRZYPADKU ZAZNACZENIA "TAK"
	TAK	NIE	

1.	Czy jest monitorowany dostęp do informacji? W jaki sposób?	x		Nadawanie uprawnień określone zostało w PBDI; potwierdzeniem stosowania ww. procedury jest m.in. rejestr upoważnień.
2.	Czy są podejmowane czynności w celu wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji? Jakie są to czynności?	x		2 stopniowe logowanie; monitoring wizyjny obejmujący teren jednostki; określone zostały zasady gospodarowania kluczami
3.	Czy zapewnia się środki w celu uniemożliwienia nieautoryzowanego dostępu na poziomie systemów operacyjnych, usług sieciowych i aplikacji? Jakie są to środki?	x		Logowanie; wzmocnione zabezpieczenia (klucze elektroniczne)
4.	Czy opracowano i udokumentowano politykę kontroli dostępu uwzględniającą potrzeby urzędu i wymogi dotyczące bezpieczeństwa? Jakie zagadnienia obejmuje polityka?	x		IZSI
5.	Czy stosowane są fizyczne zabezpieczenia w celu zapewnienia ochrony przetwarzanych informacji, np. ochrona fizyczna, kraty, przepustki, identyfikatory, zabezpieczenia pomieszczeń, monitoring wizyjny?	x		Zasady gospodarowania kluczami; kraty i rolety antywłamaniowe
7.	Czy uregulowano i jakie są stosowane rozwiązania w urzędzie w celu ochrony obszarów, w których zlokalizowane są krytyczne zasoby informacyjne i środki przetwarzania informacji? (np. ochrona fizyczna, karty dla pracowników, system wydawania kluczy, monitoring wizyjny)	x		Szafy zamykane na klucz; procedury dotyczące ograniczenia dostępu do pomieszczenia kasy.
8.	Czy i jakie rozwiązania stosuje jednostka w celu zagwarantowania, że tylko autoryzowane osoby mają fizyczny dostęp do obszarów bezpiecznych? np. identyfikacja pracowników	x		Gospodarka kluczami,
9.	Czy i jakie są stosowane narzędzia techniczne, które wspierają zabezpieczenie wejścia? np. odpowiednia klasa drzwi i zamków	x		odpowiednia klasa drzwi i zamków

10.	Czy stosuje się i jakie są środki bezpieczeństwa i nadzoru nad publicznie dostępnymi punktami, aby ograniczyć ryzyko nieautoryzowanego dostępu? (np. dozór pracownika ochrony, właściwie ustawione monitory)	x		Polityka ustawienia monitora, polityka nadzoru nad klientem przebywającym w pomieszczeniu, w którym przetwarzane są dane osobowe. W jednostce nie stosuje się blokady portów USB.
11.	Czy osoby nieupoważnione przebywające w obszarach przetwarzania danych osobowych zawsze są pod nadzorem osób upoważnionych?	x		
12.	Czy i jakie są stosowane zabezpieczenia logiczne w celu zapewnienia ochrony przetwarzanych informacji, np. autoryzacja operacji wykonywanych w systemach, system nadawania uprawnień, zabezpieczenia w ramach aplikacji?	x		autoryzacja operacji wykonywanych w systemach, system nadawania uprawnień, zabezpieczenia w ramach aplikacji.
13.	Czy w jednostce opracowano procedury dotyczące rejestrowania incydentów – próby dostępu do systemu przez nieuprawnione osoby?	x		PBDO
14.	Czy incydenty są rejestrowane i analizowane?	x		Jednostka posiada odpowiednie mechanizmy pozwalające na rejestrowanie i analizowanie incydentów (procedura zgłoszenia incydentu, rejestr incydentów); do dnia przeprowadzenia audytu nie odnotowano incydentów.

Rekomendacje: brak

Obszar nr 8: Zabezpieczenie informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie (§ 20 ust. 2, pkt. 9)

Sposób przeprowadzenia czynności audytowych:

- Zapoznanie się z procedurami wewnętrznymi w zakresie zabezpieczenia informacji przed nieuprawnionym jej ujawnieniem, modyfikacją, usunięciem lub zniszczeniem.
- Zapoznanie się z dokumentami służbowymi, na podstawie których można będzie dokonać ustalenia stanu faktycznego w badanym zakresie.
- Na podstawie dokumentów źródłowych (np. protokołów) sprawdzić jak w praktyce przebiega proces usuwania informacji przed zbyciem sprzętu lub przekazaniem go do ponownego użycia.
- Na podstawie dokumentów źródłowych (np. protokołów z likwidacji / przekazania sprzętu, notatek itp.) sprawdzić jak przebiega proces przekazywania sprzętu do zbycia lub do ponownego użycia. Sprawdzenia dokonać pod kątem uprzedniego usunięcia wrażliwych danych i licencjonowanego oprogramowania.
- Na podstawie dokumentów źródłowych, na wybranej próbie sprzętu lokalnego, sprawdzić kiedy była przeprowadzana ostatnia konserwacja oraz czy były wykonane aktualizacje oprogramowania wymagane przez producenta?
- Na podstawie dokumentów źródłowych i rozmów z pracownikami ustalić czy i kiedy była sprawdzana instalacja zasilająca. Dodatkowo na wybranej próbie pomieszczeń sprawdzić czy do sieci zasilającej dla sprzętu komputerowego nie są podpięte inne urządzenia (np. czajniki).
- Na wybranej próbie komputerów dokonać sprawdzenia czy jest zainstalowany program antywirusowy i czy jest aktualny. Sprawdzeniem można również objąć aktualizację oprogramowania antywirusowego.
- Ustalić gdzie są składowane nośniki oczekujące na zniszczenie, dokonać wizji lokalnej, ustalić kto ma do nich dostęp.

	TREŚĆ PYTANIA	ODPOWIEDZI		DOWÓD W PRZYPADKU ZAZNACZENIA "TAK"
		TAK	NIE	
1.	Czy opracowano procedury określające uprawnienia dostępu do informacji?	x		
2.	Czy dokonano podziału ról i odpowiedzialności w zakresie nadawania uprawnień?	x		

3.	Czy opracowano i wdrożono procedury postępowania z informacjami oraz ich przechowywania w celu ograniczenia ryzyka ujawnienia bądź właściwego użycia? (np. uregulowanie w aktach wewnętrznych sposobu przekazywania informacji, udostępniania informacji publicznej, udzielania odpowiedzi na zapytania)		x	
4.	Czy stosowana jest opcja wygaszania ekranu?	x		Około 10 minut
5.	Czy jest określona i stosowana zasada blokowania komputera przed opuszczeniem stanowiska pracy?	x		
6.	Czy procedury wewnętrzne regulują zasady konserwacji sprzętu. W jaki sposób konserwuje się sprzęt w celu zapewnienia jego dostępności i integralności? Kto przeprowadza i kto nadzoruje proces konserwacji sprzętu?	x		IZSI
7.	Czy opracowano i udokumentowano procedury dotyczące zarządzania nośnikami wymiennymi? (wymienne nośniki to np. pendrive, taśmy, dyski, pamięci typu flash, wyjmowane dyski twarde, płyty CD i DVD oraz wydruki)	x		W jednostce nie likwidowano dotychczas wycofanych z użytkowania nośników danych;
8.	Czy opracowano formalne procedury bezpiecznego niszczenia nośników? a) jakie metody niszczenia się stosuje i czy są one dostosowane do poziomu krytyczności i wrażliwości informacji? b) jak zabezpiecza się nośniki oczekujące na zniszczenie?	x		IZSI
9.	Czy nośniki danych przed ich likwidacją, naprawą bądź przekazaniem osobom nieuprawnionym są pozbawione zapisów?	x		
10.	Czy i jak zapewnia się ochronę przed kodem złośliwym znajdującym się na wymiennych nośnikach?	x		Oprogramowanie antywirusowe.

11.	Czy uregulowano proces rejestracji i obsługi błędów zgłaszanych przez systemy bądź użytkowników, a dotyczących przetwarzania informacji lub systemów komunikacyjnych?	x		Usługi ASI świadczy usługodawca, po jego stronie leży zorganizowanie systemu rejestracji zgłoszeń
12.	Czy i jak sposób nadzoruje się rozwiązywanie błędów?	x		ASI w ramach realizowanej umowy (cywilnoprawnej)
13.	Czy są wykonywane kopie zapasowe oraz czy mają zapewnioną fizyczną ochronę nie gorszą niż dane źródłowe?	x		Kopie zapasowe robione są raz w tygodniu i wysyłane do dysku sieciowego Qnap; Dysk Qnap umieszczony jest w metalowej skrzynce zamkniętej na klucz.
14.	Czy i w jaki sposób zapewnia się, że dostęp do kopii zapasowych jest ograniczony i ściśle kontrolowany?	x		Kopie zapasowe są w formie fizycznej w odpowiednio zabezpieczonych pojemnikach
15.	Czy testowany jest system awaryjnego zasilania UPS?	x		UPS są przy określonych stacjach roboczych

Rekomendacje: brak

Obszar nr 9: zawieranie w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji (§ 20 ust. 2, pkt. 10)

Sposób przeprowadzenia czynności audytowych:

- Ustalenie czy i kto weryfikuje / akceptuje projekt umowy pod kątem wymagań bezpieczeństwa.
- Analiza wybranych umów pod kątem zapisów dot. wymagań bezpieczeństwa.

	ODPOWIEDZI	DOWÓD W

	TREŚĆ PYTANIA	TAK	NIE	PRZYPADKU ZAZNACZENIA "TAK"
1.	Czy umowy podpisywane z wykonawcami i użytkownikami stron trzecich zawierają zasady, warunki i obowiązki w zakresie bezpieczeństwa informacji? Jakie zapisy obejmują umowy? (np. zapis o tym, że pracownik serwisu posiada upoważnienie firmy do wykonania usługi, zobowiązanie do zachowania tajemnicy, przebywanie w określonych pomieszczeniach urzędu tylko w obecności pracownika urzędu itp.)	x		
2.	Czy umowy zawierają klauzule odpowiedzialności odszkodowawczej od strony trzeciej?	x		

Rekomendacje: brak

Obszar nr 10: Ustalenie zasad postępowania z informacjami, zapewniającymi minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych (§ 20 ust. 2, pkt. 11)

Sposób przeprowadzenia czynności audytowych:

- Analiza procedur wewnętrznych w zakresie bezpieczeństwa informacji.
- Zapoznanie się z przeprowadzoną analizą ryzyka w zakresie bezpieczeństwa informacji.

	TREŚĆ PYTANIA	ODPOWIEDZI		DOWÓD W PRZYPADKU ZAZNACZENIA "TAK"
		TAK	NIE	
1.	Czy w jednostce określone zostały zasady postępowania z informacjami, ograniczające ryzyko kradzieży informacji i środków przetwarzania informacji? Kto ustala te zasady?	x		

2.	Czy w ramach zarządzania ryzykiem oceniono ryzyko kradzieży informacji i środków przetwarzania informacji oraz czy ustanowiono i wprowadzono działania ograniczające to ryzyko.	x		

Rekomendacje: brak

V. ZALECENIA: brak

VI. ODNIESIENIE DO ZASTRZEŻEŃ, O KTÓRYCH MOWA W § 17 UST 3 ROZPORZĄDZENIA MINISTRA FINANSÓW Z DNIA 4 WRZEŚNIA 2015 R. W SPRAWIE AUDYTU WEWNĘTRZNEGO ORAZ INFORMACJI O PRACY I WYNIKACH TEGO AUDYTU (DZ. U. 2018 R., POZ. 506): Brak

VII. OGÓLNA OCENA ADEKWATNOŚCI, SKUTECZNOŚCI I EFEKTYWNOŚCI KONTROLI ZARZĄDCZEJ W OBSZARZE DZIAŁALNOŚCI JEDNOSTKI OBJĘTYM ZADANIEM:

System kontroli zarządczej w obszarze audytowanym zapewnia realizację celów i zadań zgodnie z obowiązującym prawem, w sposób adekwatny, skuteczny i terminowy, uzyskując tym samym ocenę pozytywną.

VIII. DATA SPORZĄDZENIA SPRAWOZDANIA: 31 października 2023 r.

Dokumenty robocze znajdują się w dokumentacji bieżącej zadania audytowego.

Pouczenie dotyczące wstępnych wyników audytu:

Na mocy § 17 ust. 3 Rozporządzenia Ministra Finansów z dnia 4 września 2015 roku (Dz. U. 2018 poz. 506) w sprawie audytu wewnętrznego oraz informacji o pracy i wynikach tego

audytu audytowany może zgłosić pisemne zastrzeżenia w terminie 7 dni od dnia poinformowania audytowanego o wstępnych wynikach.

Pouczenie dotyczące sprawozdania z zadania zapewniającego:

Na mocy § 19 Rozporządzenia Ministra Finansów z dnia 4 września 2015 roku (Dz. U. 2018 poz. 506) w sprawie audytu wewnętrznego oraz informacji o pracy i wynikach tego audytu kierownik komórki audytu wewnętrznego przekazuje sprawozdanie audytowanemu i kierownikowi jednostki. Audytowany, w terminie 14 dni kalendarzowych od dnia otrzymania sprawozdania, ustala sposób i termin realizacji zaleceń oraz wyznacza osoby odpowiedzialne za realizację zaleceń, powiadamiając o tym na piśmie kierownika komórki audytu wewnętrznego i kierownika jednostki.

W przypadku odmowy realizacji zaleceń audytowany przedstawia, w terminie 7 dni kalendarzowych od dnia otrzymania sprawozdania, pisemne stanowisko kierownikowi jednostki i audytorowi wewnętrznemu. W takim przypadku kierownik jednostki podejmuje decyzję dotyczącą realizacji zaleceń, informując o tym audytowanego i kierownika komórki audytu wewnętrznego.

Audytor wewnętrzny monitoruje realizację zaleceń.

Audytor wewnętrzny po upływie terminów realizacji zaleceń przeprowadza czynności sprawdzające.

Wynik czynności sprawdzających audytor wewnętrzny przedstawia w notatce informacyjnej kierownikowi jednostki i audytowanemu.

Niniejsze sprawozdanie sporządzono w trzech jednobrzmiących egzemplarzach na 24 stronach, które otrzymują:

Rozdzielnik:

1. Starosta Gołdapski
2. Dyrektor Poradni Psychologiczno-Pedagogicznej w Gołdapi
3. a/a

Łukasz Skowroński
AUDYTOR WEWNETRZNY
ZAŚWIADCZENIE MF 329/2004

.....

Podpis audytora wewnętrznego