BURMISTRZ GOŁDAPI Tomasz Luto 19.12.2017r.

SPRAWOZDANIE

Temat: SYSTEM ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI/DANYCH TELEINFORMATYCZNYCH I KONTROLI ZARZĄDCZEJ W SZKOLE PODSTAWOWEJ W GRABOWIE 2016-DO DNIA AUDYTU

Audytor wewnętrzny: Ewa Kraśniewska

I. INFORMACJA PODSTAWOWE:

1. Temat zadania audytowego: ***System zarządzania bezpieczeństwem informacji/danych teleinformatycznych i kontroli zarządczej w Szkole Podstawowej w Grabowie 2016-do dnia audytu.***
2. Data sporządzenia wstępnych wyników z audytu: 28 listopada 2017r.
3. Data sporządzenia sprawozdania: 1 grudnia 2017r.
3. Nazwa jednostki, w której przeprowadzany był audyt wewnętrzny:

Szkoła Podstawowa im. M. Kajki w Grabowie

4. Termin przeprowadzenia zadania audytowego: 15 listopada – 28 listopada 2017r.
5. Cel przeprowadzenia zadania audytowego:

Cel ogólny: *ocena prawidłowości funkcjonowania systemu zarządzania bezpieczeństwem informacji/danych teleinformatycznych i kontroli zarządczej w Szkole Podstawowej w Grabowie w aspekcie wewnętrznych uregulowań.*

Cele szczegółowe:

1) Stwierdzenie istnienia procedur wewnętrznych dotyczących kontroli zarządczej i bezpieczeństwa teleinformatycznego zapewniających funkcjonowanie jednostki zgodne z przepisami prawa.
2) Analiza procedur i praktyk dotyczących kontroli zarządczej i bezpieczeństwa teleinformatycznego. Weryfikacja stanu faktycznego (na próbie) w zakresie określania ryzyk, przeprowadzania samooceny, ochrony danych osobowych itp.

6. Zakres zadania audytowego:

Szkoła Podstawowa im. M. Kajki w Grabowie

Przeprowadzono wywiady z:

- wybranymi pracownikami szkoły.

Przedmiotowy:

W celu sprawdzenia poprawności przebiegu badanego procesu oraz zbadania jego zgodności z przepisami obowiązującymi w tym obszarze, zakresem przedmiotowym zadania audytowego objęte zostały:

- regulacje wewnętrzne z zakresu kontroli zarządczej;
- regulacje wewnętrzne z zakresu bezpieczeństwa informacji;
- dokumentacja przeprowadzonej samooceny kz;
- dokumentacja dotycząca analizy ryzyka;
- dokumentacja przeprowadzania wewnętrznych kontroli;
- dokumentacja prowadzona zgodnie z regulacjami;
- rejestracja zbiorów danych osobowych,
- zakresy czynności wybranych osób biorących udział w badanych procesach, upoważnienia do przetwarzania danych osobowych,

II. ANALIZA RYZYKA

Czynności audytowe zgodnie z zakresem przedmiotowym zadania, zostały skierowane na organizację systemu w zakresie następujących ryzyk:

1. braku procedur dotyczących kontroli zarządczej;
2. niestosowanie się do wewnętrznych procedur i zewnętrznych uregulowań np. Ustawy o finansach publicznych;
3. brak określenia ryzyk, celów i zadań oraz mierników;
4. niedocenianie ryzyk, które są najbardziej znaczące w obszarze bezpieczeństwa informacji,
5. brak delegowania odpowiedzialności z zakresu zarządzania ryzykiem bezpieczeństwa informacji na wszystkie poziomy organizacji,

7. brak monitorowania działań w zakresie zarządzania ryzykiem w celu zapewnienia zgodności z przyjętymi procedurami/politykami,
8. brak wdrożenia praktyk w zakresie zarządzania bieżącym ryzykiem związanym z bezpieczeństwem informacji w organizacji.

III. PRZEPISY PRAWNE (KRYTERIA), USTALENIA ORAZ REGULACJE WEWNĘTRZNE DOTYCZĄCE BADANEGO OBSZARU

Przepisy prawne:

1. Rozporządzenie Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych z dnia 12 kwietnia 2012 r. (Dz.U. z 2016 r. poz. 113))
2. Ustawa o ochronie danych osobowych z dnia 29 sierpnia 1997r. (Dz.U. z 2016 r. poz. 922)
3. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych z dnia 29 kwietnia 2004r. (Dz. U. z 2004r., nr 100, poz. 1024)
4. Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewniania przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji (Dz.U. rok 2015 poz. 745)
5. Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbiorów danych (Dz.U. rok 2015 poz. 719)
6. Ustawa o finansach publicznych z dnia 27 sierpnia 2009r. (Dz.U. z 2016 r. poz. 1870)
7. Komunikat nr 23 Ministra Finansów w sprawie standardów kontroli zarządczej dla sektora finansów publicznych z dnia 16 grudnia 2009 r. (Dz. Urz. MF rok 2009 nr 15 poz. 84)
8. Komunikat Nr 3 Ministra Finansów w sprawie szczegółowych wytycznych w zakresie samooceny kontroli zarządczej dla jednostek sektora finansów publicznych (Dz. Urz. MF rok 2011 Nr 2, poz. 11)

Regulacje wewnętrzne:

- procedury dotyczące bezpieczeństwa informacji,
- procedury dotyczące funkcjonowania kontroli zarządczej
- upoważnienia do przetwarzania danych osobowych.

Kryteria oceny

a) zgodność działalności z przepisami prawa oraz procedurami wewnętrznymi,
b) dokumentowanie systemu kontroli zarządczej,
c) ochrona zasobów,
d) prowadzenie nadzoru nad wykonaniem zadań,
e) zarządzanie ryzykiem,
f) celowość wydatkowanych środków,
g) efektywność, oszczędność ponoszonych nakładów i zasobów na zrealizowanie celu,
h) poufność,
i) dostępność,
j) istnienie mechanizmów kontrolnych dotyczących operacji finansowych i gospodarczych,
k) istnienie mechanizmów kontroli dotyczących systemów informatycznych,
l) monitorowanie i ocena systemu kontroli zarządczej,

Kryteria uzgodniono **15 listopada 2017r.**

IV. SZCZEGÓŁOWE USTALENIA DOKONANE NA PODSTAWIE CZYNNOŚCI AUDYTOWYCH W OBSZARACH WYTYPOWANYCH DO BADANIA WRAZ ZE SKLASYFIKOWANYMI WYNIKAMI ICH OCENY WG KRYTERIÓW

Cel kontroli 1

Stwierdzenie istnienia procedur wewnętrznych dotyczących kontroli zarządczej i bezpieczeństwa teleinformatycznego zapewniających zgodne z przepisami prawa funkcjonowanie jednostki

Metodyka (sposób weryfikacji)

Audytor dokonał analizy procedur wewnętrznych zapewniających bezpieczeństwo informacji i prawidłowe funkcjonowanie kontroli zarządczej w Szkole Podstawowej w Grabowie

Kryteria (stan oczekiwany)

a) dokumentowanie systemu kontroli zarządczej,
b) monitorowanie i ocena systemu kontroli zarządczej,

Ustalenia stanu faktycznego

1. **Wdrożenie procedur zapewniających przestrzeganie standardów kontroli zarządczej.**

Ustawa o finansach publicznych w art. 68. ustaliła pojęcie i cele kontroli zarządczej:
1. Kontrolę zarządczą w jednostkach sektora finansów publicznych stanowi ogół działań podejmowanych dla zapewnienia realizacji celów i zadań w sposób zgodny z prawem, efektywny, oszczędny i terminowy.
2. Celem kontroli zarządczej jest zapewnienie w szczególności:
1) zgodności działalności z przepisami prawa oraz procedurami wewnętrznymi;
2) skuteczności i efektywności działania;
3) wiarygodności sprawozdań;
4) ochrony zasobów;
5) przestrzegania i promowania zasad etycznego postępowania;
6) efektywności i skuteczności przepływu informacji;
7) zarządzania ryzykiem.

Artykuł ten uszczegóławiają Standardy kontroli zarządczej dla sektora finansów publicznych, które określają podstawowe wymagania odnoszące się do kontroli zarządczej w sektorze finansów publicznych. Standardy definiują elementy kontroli zarządczej - pięć najważniejszych płaszczyzn czyli obszarów zarządzania. Stan każdego z nich ma wpływ na realizację wszystkich celów i zadań w sposób zgodny prawem, oszczędny i terminowy. Każdy z nich występuje we wszystkich komórkach organizacyjnych w jednostce. Każdy z nich można ocenić pod względem kryteriów adekwatności, efektywności i skuteczności.

A. ŚRODOWISKO WEWNĘTRZNE
Standard A.1: Przestrzeganie wartości etycznych
Standard A.2: Kompetencje zawodowe
Standard A.3: Struktura organizacyjna
Standard A.4: Delegowanie uprawnień
B. CELE I ZARZĄDZANIE RYZYKIEM
Standard B.5: Misja
Standard B.6: Określanie celów i zadań, monitorowanie i ocena ich realizacji
Standard B.7: Identyfikacja ryzyka
Standard B.8: Analiza ryzyka
Standard B.9: Reakcja na ryzyko
C. MECHANIZMY KONTROLI
Standard C.10: Dokumentowanie systemu kontroli zarządczej
Standard C.11: Nadzór

Standard C.12: Ciągłość działalności
Standard C.13: Ochrona zasobów
Standard C.14: Szczegółowe mechanizmy kontroli dotyczące operacji finansowych i gospodarczych
Standard C.15: Mechanizmy kontroli dotyczące systemów informatycznych
D. INFORMACJA I KOMUNIKACJA
Standard D.16: Bieżąca informacja
Standard D.17: Komunikacja wewnętrzna
Standard D.18: Komunikacja zewnętrzna
E. MONITOROWANIE I OCENA
Standard E.19: Monitorowanie systemu kontroli zarządczej
Standard E.20: Samoocena
Standard E.21: Audyt wewnętrzny
Standard E.22: Uzyskanie zapewnienia o stanie kontroli zarządczej

W jednostce funkcjonują następujące regulacje wewnętrzne:

1. Projekt Statutu Szkoły Podstawowej im. M. Kajki w Grabowie przekazany do UM 10 listopada 2017r.
2. Regulamin dokonywania oceny nauczycieli wprowadzony 7 października 2005r.
3. Regulamin dofinansowania form doskonalenia zawodowego nauczycieli w Szkole Podstawowej w Grabowie z 20.10.2017r.
4. Instrukcja przechowywania i wydawania kluczy z 16 grudnia 2015r.
5. Zasady prowadzenia kontroli zarządczej z 7 września 2011r.
6. Regulamin udzielania zamówień publicznych o wartości nieprzekraczającej kwoty wskazanej w art. 4 pkt.8 Ustawy Prawo Zamówień Publicznych z 17.11.2015
7. Regulamin naboru na wolne stanowiska urzędnicze w tym kierownicze stanowiska urzędnicze z 20.11.2015r
8. Kodeks Etyki z 11 kwietnia 2016r.
9. Regulamin Zakładowego Funduszu Świadczeń Socjalnych z 13 października 2017r.
10. Regulamin kontroli wewnętrznej z 20 grudnia 2016r.
11. Regulamin przeprowadzenia okresowej oceny kwalifikacyjnej z 18 października 2017r.
12. Regulamin wynagradzania pracowników samorządowych z 20.10.2016r
13. Regulamin pracy z 04 czerwca 2013r.
14. Instrukcja kasowa z 12 listopada 2011r.
15. Zasady (polityka) rachunkowości z 10 października 2017r.

2. Wdrożenie procedur wewnętrznych zapewniających bezpieczeństwo informacji

Rozporządzenie MSWiA w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych określa sposób prowadzenia i zakres dokumentacji opisującej sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną.

Na dokumentację, składa się polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym.

Polityka bezpieczeństwa, zawiera w szczególności:

1) wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe;

2) wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych;

3) opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi;

4) sposób przepływu danych pomiędzy poszczególnymi systemami;

5) określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.
Instrukcja, o której mowa w § 3 ust. 1, zawiera w szczególności:
1) procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności;
2) stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem;
3) procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu;
4) procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania;
5) sposób, miejsce i okres przechowywania:
a) elektronicznych nośników informacji zawierających dane osobowe,
b) kopii zapasowych, o których mowa w pkt 4,
6) sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, o którym mowa w pkt III ppkt 1 załącznika do rozporządzenia;
7) sposób realizacji wymogów, o których mowa w § 7 ust. 1 pkt 4;
8) procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.

Audytor otrzymał do analizy następujące procedury:

1. Politykę bezpieczeństwa wraz z załącznikami – wprowadzoną 29 maja 2014r.
2. Instrukcję zarządzania systemem informatycznym – wprowadzoną 29 maja 2014r.
3. Procedurę alarmową – wprowadzoną 30 grudnia 2016r.

Ewidencja osób upoważnionych do przetwarzania danych zawiera elementy wskazane w art. 39 Ustawy o ochronie danych osobowych.
W pozostałej dokumentacji nieprawidłowości nie stwierdzono. Jest ona zgodna z obowiązującymi przepisami prawa.

Klasyfikacja wyników wg kryteriów
Ocena adekwatna - zastane mechanizmy oraz procedury w pełni odpowiadają potrzebom oraz wymogom prawa.
Wskazanie słabości kontroli zarządczej i ich skutki
Nie wskazano
Zalecenia
Nie wydano

Cel kontroli 2
Analiza procedur i praktyk dotyczących bezpieczeństwa informacji
Metodyka (sposób weryfikacji)
Audytor sprawdził poprawności przebiegu badanego procesu (na próbie) oraz zbadał jego zgodności z przepisami obowiązującymi w tym obszarze poprzez zapoznanie się z dokumentami i przepisami prawa, uzyskiwanie wyjaśnień i informacji od pracowników jednostki oraz analizę mechanizmów kontrolnych.
Kryteria (stan oczekiwany)
a) zgodność działalności z przepisami prawa oraz procedurami wewnętrznymi, b) ochrona zasobów, c) prowadzenie nadzoru nad wykonaniem zadań, d) zarządzanie ryzykiem, e) poufność, f) dostępność, g) istnienie mechanizmów kontroli dotyczących systemów informatycznych.

Ustalenia stanu faktycznego

Zgodność procedur z Krajowymi Ramami Interoperacyjności

Zgodnie z §20 *Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych:*

[Zarządzanie bezpieczeństwem informacji] 1. 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.

2. 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;

W szkole regulacje wewnętrzne są na bieżąco aktualizowane.

2) utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację;

W jednostce zinwentaryzowano posiadane aktywa informacyjne, nie ustalono natomiast schematu klasyfikacji danych w oparciu o kryteria ważności i wrażliwości danych. W jednostce nie występują sytuacje nieautoryzowanych zmian sprzętu lub oprogramowania.

W jednostce nie dokonano klasyfikacja zasobów informacyjnych, pod względem ich istotności w odniesieniu do funkcji organizacji. Nie dokonano również analizy zagrożeń poszczególnych grup zasobów informacyjnych.

W jednostce dokonano inwentaryzacji środków trwałych, licencji, oprogramowania zgodnie Ustawą o rachunkowości, nie dokonywano dodatkowej inwentaryzacji na potrzeby bezpieczeństwa informacji. Własność aktywów określono poprzez przekazanie pracownikom sprzętu czy oprogramowanie.

3) przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy;

Szacowanie ryzyka w Szkole Podstawowej w Grabowie dokonywane jest raz w roku przy okazji dokonywania rocznej identyfikacji celów i zadań oraz identyfikacji i analizy ryzyka.

W rejestrze ryzyk na rok 2017 dla kryterium Administrowanie siecią IT przyporządkowano ryzyko – awaria systemu informatycznego, utrata danych, niestosowanie zaleceń polityki bezpieczeństwa, niewystarczające środki finansowe; dla kryterium Ochrona informacji niejawnych i danych osobowych - nieprzestrzeganie przepisów o poufności, przystępności i wyłączności danych w zależności od ich ważności i przeznaczenia. Czynniki ryzyka zostały ocenione na poziomie niskim.

4) 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;

Użytkownicy upoważnieni w zakresie przetwarzania danych osobowych potwierdzają pisemnie w składanym oświadczeniu, że znają zasady przetwarzania danych osobowych.

Administrator Danych Osobowych zobowiązany jest do wydawania, ewidencjonowania i przechowywania imiennych upoważnień do przetwarzania danych osobowych oraz cofniętych upoważnień.

W jednostce jest prowadzona Ewidencja osób upoważnionych do przetwarzania danych osobowych. Zgodnie z Art. 39. Ustawy o ochronie danych osobowych Administrator danych prowadzi ewidencję osób upoważnionych do ich przetwarzania, która powinna zawierać:

1) imię i nazwisko osoby upoważnionej;

2) datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych;

3) identyfikator, jeżeli dane są przetwarzane w systemie informatycznym.
Administrator bezpieczeństwa informacji dokonuje corocznych sprawdzeń i dokumentuje je za pomocą protokołów.
W jednostce przestrzegany jest zakaz nie wydawania innym użytkownikom wykorzystanych wcześniej identyfikatorów używanych w systemie informatycznym.
5) bezzwłocznej zmiany uprawnień, w przypadku zmiany zadań osób, o których mowa w pkt 4;
W okresie obowiązywania polityki nie było sytuacji w której należało obniżyć uprawnienia użytkownika.
6) zapewnienia szkolenia osób zaangażowanych w proces przetwarzania informacji ze szczególnym uwzględnieniem takich zagadnień, jak:
a) zagrożenia bezpieczeństwa informacji,
Wszyscy pracownicy uczestniczyli w szkoleniu na w/w temat.
b) skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna,
Wszyscy pracownicy uczestniczyli w szkoleniu na w/w temat.
c) stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich;
Wszyscy pracownicy uczestniczyli w szkoleniu na w/w temat.
7) zapewnienia ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, przez:
a) monitorowanie dostępu do informacji,
W Szkole Podstawowej w Grabowie monitorowanie dostępu do informacji odbywa się pod nadzorem upoważnionych osób. W jednostce określono zakres obowiązków:
- **Administratora Danych Osobowych** - rozumie się przez to organ, jednostkę organizacyjną, podmiot lub osobę, decydującą o celach i środkach przetwarzania danych osobowych. W szkole funkcję tę pełni: **Dyrektor szkoły.**
- **Administratora Bezpieczeństwa Informacji** - osoba funkcyjna wyznaczona przez ADO odpowiedzialna za przestrzeganie zasad ochrony danych osobowych oraz zapewnienie środków technicznych i organizacyjnych zapewniających ochronę danych osobowych w szkole funkcję tę pełni: **Wicedyrektor.**

W jednostce wprowadzono system haseł przypisanych do użytkowników – umożliwiający tylko osobom upoważnionym dostęp do danych osobowych.
b) czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji,
Komórką organizacyjną/stanowiskiem odpowiedzialnym za kontakty z użytkownikami jest administrator danych osobowych i administrator bezpieczeństwa informacji. Do zgłaszania problemów i incydentów ustalony został adres e-mail i telefon kontaktowy.
Zgłaszanie problemów i incydentów nie zostało sformalizowane, nie prowadzono rejestru zdarzeń.
Przeglądy i testy systemów informatycznych w zakresie ich bezpieczeństwa przeprowadza systematycznie nauczyciel - Informatyk. Nie są dokumentowane.
c) zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji;
W szkole wprowadzono środki zapobiegawcze, wykrywające i naprawcze w zakresie ochrony przed wirusami, robakami, oprogramowaniem szpiegującym, spamem (program antywirusowy).
W systemie wprowadzane są aktualne patche ("łatki bezpieczeństwa" - poprawka lub uaktualnienie do programu).
8) ustanowienia podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość;
W jednostce nie jest wykonywana praca na odległość.
9) zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnieniu, modyfikacji, usunięciu lub zniszczeniu;
System tworzenia i zmiany haseł w szkole zapewnia wymagany poziom bezpieczeństwa.

Hasła składają się z 8 znaków - małe i duże litery oraz cyfry, znaki specjalne.
Zmiana haseł wymuszana jest automatycznie przez systemy co 30 dni, dlatego w jednostce nie prowadzi się harmonogramu zmiany haseł.
Kopie zapasowe są przechowywane w szafie pancernej i w zamykanej kasetce w księgowości. Ustalono osoby mające dostęp do miejsca, w którym przechowywane są kopie zapasowe. Klucze do pomieszczeń przechowywane są w sposób bezpieczny.

10) zawierania w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji;

W szkole w niewielkim stopniu korzysta się z usług firm zewnętrznych w zakresie serwisu. W związku z tym nie jest prowadzony rejestr usług zewnętrznych IT. W jednostce monitoruje się sposób realizacji usług zewnętrznych IT w celu zapewnienia, że spełniane są wymagania i zapisy umowne.

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

Dane osobowe przetwarzane w szkole przechowywane są w sposób zapewniający ich bezpieczeństwo w zamykanych na klucz pomieszczeniach, w szafkach zamykanych na zamek.

12) zapewnienia odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na:

a) dbałości o aktualizację oprogramowania,

W jednostce na bieżąco aktualizuje się oprogramowanie.

b) minimalizowaniu ryzyka utraty informacji w wyniku awarii,

W jednostce ustalono system tworzenia i przechowywania kopii zapasowych.

c) ochronie przed błędami, utratą, nieuprawnioną modyfikacją,

W jednostce wprowadzono system haseł przypisanych do użytkowników, zmienianych co 30 dni.
W szkole pracownicy upoważnieni są do przetwarzania danych osobowych.

d) stosowaniu mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa,

Zgodnie z Ustawą z dnia 15 kwietnia 2011 r. o systemie informacji oświatowej określającej organizację i zasady działania systemu informacji oświatowej (dalej: SIO), przetwarzane są dane dotyczące publicznych placówek oświatowych. W SIO gromadzi się dane osobowe pracowników pedagogicznych i dzieci objętych: pomocą psychologiczno-pedagogiczną, wczesnym wspomaganiem rozwoju w szkołach i placówkach oświatowych oraz wychowaniem przedszkolnym.
Program sam szyfruje i pakuje dane tworząc plik exp.

e) zapewnieniu bezpieczeństwa plików systemowych,

Bezpieczeństwo plików systemowych jest zapewniane poprzez nadawanie odpowiednich uprawnień do modyfikacji danych użytkownikom.

f) redukcji ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych,

Aby redukować ryzyko wynikające z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych w jednostce na bieżąco programy są aktualizowane, są ściągane do nich dostępne poprawki, które mają ograniczać w/w ryzyka.

g) niezwłocznym podejmowaniu działań po dostrzeżeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa,

W szkole nie odnotowano nieujawnionych podatność systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa.

h) kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa;

W jednostce kontroluje się zgodność systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa – bieżący nadzór Administratora Bezpieczeństwa Informacji.

13) bezzwłocznego zgłaszania incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących;

Zgodnie z obowiązującymi procedurami w jednostce osoby upoważnione do przetwarzania danych osobowych w szkole zobowiązane są do: natychmiastowego zgłoszenia Administratorowi Systemu

Informatycznego podejrzenia lub stwierdzenia faktu naruszenia bezpieczeństwa danych osobowych przetwarzanych w jednostce.

14) zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok.

W jednostce zapewniono okresowy audyt wewnętrzny w zakresie bezpieczeństwa informacji w roku 2017.

Rozdział 6 Ustawy o ochronie danych osobowych zobowiązuje administratora danych do zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi, z wyjątkiem przypadków, o których mowa w art. 43 ust. 1.

Dyrektor szkoły zgłosił zbiory danych osobowych przetwarzane w jednostce Generalnemu Inspektorowi Ochrony Danych Osobowych:

- zamówienia publiczne,
- rejestr korespondencji,
- zbiory archiwum.

Klasyfikacja wyników wg kryteriów
Ocena adekwatna - zastane mechanizmy oraz procedury w pełni odpowiadają potrzebom oraz wymogom prawa.
Wskazanie słabości kontroli zarządczej i ich skutki
Nie wskazano
Zalecenia
Nie wydano

Cel kontroli 3
Analiza procedur i praktyk dotyczących kontroli zarządczej
Metodyka (sposób weryfikacji)
Audytor sprawdził poprawności przebiegu badanego procesu (na próbie) oraz zbadał jego zgodności z przepisami obowiązującymi w tym obszarze poprzez zapoznanie się z dokumentami i przepisami prawa, uzyskiwanie wyjaśnień i informacji od pracowników jednostki oraz analizę mechanizmów kontrolnych.
Kryteria (stan oczekiwany)
a) zgodność działalności z przepisami prawa oraz procedurami wewnętrznymi, b) dokumentowanie systemu kontroli zarządczej, c) ochrona zasobów, d) prowadzenie nadzoru nad wykonaniem zadań, e) zarządzanie ryzykiem, f) celowość wydatkowanych środków, g) efektywność, oszczędność ponoszonych nakładów i zasobów na zrealizowanie celu, h) istnienie mechanizmów kontrolnych dotyczących operacji finansowych i gospodarczych, i) monitorowanie i ocena systemu kontroli zarządczej,

Ustalenia stanu faktycznego

A. ŚRODOWISKO WEWNĘTRZNE

Standard A.1: Przestrzeganie wartości etycznych
Standard A.2: Kompetencje zawodowe
Standard A.3: Struktura organizacyjna
Standard A.4: Delegowanie uprawnień
W jednostce funkcjonują regulacje wewnętrzne wskazane na str. 4.

Ponadto wszyscy pracownicy administracji i obsługi mają sporządzone na piśmie zakresy czynności. Delegowanie uprawnień odbywa się również w formie pisemnej.

B. CELE I ZARZĄDZANIE RYZYKIEM

Standard B.5: Misja
Standard B.6: Określanie celów i zadań, monitorowanie i ocena ich realizacji
Standard B.7: Identyfikacja ryzyka
Standard B.8: Analiza ryzyka
Standard B.9: Reakcja na ryzyko
W roku 2016 i w 2017 w Szkole Podstawowej w Grabowie przeprowadzono analizę ryzyka w stosunku do zadań realizowanych przez jednostkę, określono właścicieli ryzyka i reakcję na ryzyko.

C. MECHANIZMY KONTROLI

Standard C.10: Dokumentowanie systemu kontroli zarządczej
Standard C.11: Nadzór
Standard C.12: Ciągłość działalności
Standard C.13: Ochrona zasobów
Standard C.14: Szczegółowe mechanizmy kontroli dotyczące operacji finansowych i gospodarczych
Standard C.15: Mechanizmy kontroli dotyczące systemów informatycznych

W zakresie tej grupy standardów audytor dokonał sprawdzenia:

1. Funkcjonowanie Zakładowego Funduszu Świadczeń Socjalnych.

Ustawa o zakładowym funduszu wskazuje na jakie cele można przeznaczyć środki z zakładowego funduszu świadczeń socjalnych. Działalnością socjalną według ustawy jest:

- **wypoczynek pracowników** zorganizowany w formie wczasów, wczasów profilaktycznych, pobytu w sanatorium na leczeniu lub rekonwalescencji itp.
- **wypoczynek dzieci i młodzieży** organizowany w formie -kolonii wypoczynkowych i zdrowotnych, obozów i zimowisk, wczasów wypoczynkowych, wyjazdów klimatycznych i zielonych szkół,
- **wypoczynek organizowany przez pracowników we własnym zakresie** (tzw. wczasy turystyczne, wczasy pod gruszą, agroturystyka)
- **sport i rekreacja** - bilety wstępu na imprezy sportowe, pływalnie, korty tenisowe i inne usługi zakupione u wyspecjalizowanych organizatorów, jeśli pracodawca nie posiada własnej bazy sportowo-rekreacyjnej
- **zakup biletów** do kina, teatru, na wystawy i inne imprezy o charakterze kulturalno-oświatowym
- **pomoc materialno - rzeczowa** przyznawana osobom znajdującym się w trudnej sytuacji życiowej i materialnej oraz zapomogi pieniężne udzielane w wypadkach życiowych i losowych
- **zwrotna lub bezzwrotna pomoc na cele mieszkaniowe** udzielona na warunkach określonych w umowie między pracodawcą a pracownikiem

Wszelkie zapisy odnośnie zasad i warunków korzystania z usług i świadczeń finansowanych z funduszu oraz zasad przeznaczania środków funduszu na poszczególne cele i rodzaje działalności

socjalnej powinny znaleźć swe miejsce w regulaminie, który pracodawca uzgadnia z zakładową organizacją związkową. W sytuacji, gdy na terenie firmy nie działa taka organizacja, pracodawca powinien uzgodnić regulamin w porozumieniu z pracownikiem wybranym przez załogę do reprezentowania jej interesów (art. 8 ust. 2 ustawy).

W jednostce funkcjonuje Regulamin Zakładowego Funduszu Świadczeń Socjalnych wprowadzony Zarządzeniem nr 06/2017 przez Dyrektora placówki w dniu 13 października 2017r.
Wcześniej obowiązywał Regulamin Zakładowego Funduszu Świadczeń Socjalnych z 24 września 2012r.

Zarządzenie już w dniu wprowadzenia posiadało nieaktualną podstawę prawną:
- Ustawa o zakładowym funduszu świadczeń socjalnych (Dz.U. z 1996r. nr 70, poz. 335 z późn. zm.) – 13 października 2017r. obowiązywał już tekst jednolity ustawy ogłoszony w Dz.U. z 2016r. poz. 800.
- Ustawa o związkach zawodowych (Dz.U. nr 79, poz. 854 z późn. zm.) – 13 października 2017r. obowiązywał już tekst jednolity ustawy ogłoszony w Dz. U. z 2015r. poz. 1881.
- Rozporządzenie Ministra Pracy i Polityki Socjalnej z dnia 14 marca 1994r. w sprawie sposobu ustalania przeciętnej liczby zatrudnionych w celu naliczenia odpisu na zakładowy fundusz świadczeń socjalnych (Dz.U. nr 43, poz. 168 z późn. zm.) – obowiązujące jest Rozporządzenie Ministra Pracy i Polityki Społecznej z dnia 9 marca 2009 r. w sprawie sposobu ustalania przeciętnej liczby zatrudnionych w celu naliczania odpisu na zakładowy fundusz świadczeń socjalnych (Dz. U. rok 2009 nr 43 poz. 349)

Podobne sam regulamin w Rozdziale I §3 jako podstawę opracowania podaje:
- Ustawę z 13 marca 2003r. o szczególnych zasadach rozwiązywania z pracownikami stosunków pracy z przyczyn niedotyczących pracowników (Dz. U. z 2003r. nr 90, poz. 844 z późn. zm.) – aktualny jest tekst jednolity ogłoszony w Dzienniku Ustaw w roku 2016 poz. 1474.

Wykonanie ZFŚS
2016r.
Wpływy – 191 102,25 zł
Wydatki:
- pożyczki mieszkaniowe – 55 000,00 zł,
- Wielkanoc (zapomogi świąteczne) – 16 100,00 zł,
- świadczenia urlopowe n-li – 29 171,46 zł,
- emeryci – dofinansowanie wypoczynku – 7 180,00 zł,
- administracja i obsługa – dofinansowanie wypoczynku – 6 310,00 zł,
- wypoczynek letni dzieci – 700,00 zł,
- zapomoga socjalna – 700,00 zł,
- wyjazd do filharmonii – 972,00 zł,
- Boże Narodzenie – zapomogi (zapomogi świąteczne) – 59 760,00 zł

Razem: 175 893,46 zł.
2017r.
Wpływy – 169 786,96 zł
Wydatki:
- pożyczki mieszkaniowe – 50 000,00 zł,
- Wielkanoc (zapomogi świąteczne) – 20 650,00 zł,
- świadczenia urlopowe n-li – 30 547,22 zł,
- emeryci – dofinansowanie wypoczynku – 7 610,00 zł,
- administracja i obsługa – dofinansowanie wypoczynku – 7 010,00 zł,
- zapomoga socjalna – 970,00 zł,
- zapomoga losowa – 1 000,00 zł,

- spektakl – 975,00 zł,
Razem: 118 762,22 zł.
Obydwa regulaminy wskazują, że środki funduszu powinny być przeznaczone na:
- zapomogi losowe i socjalne,
- dofinansowanie wypoczynku,
- pomoc na cele mieszkaniowe,
- działalność kulturalno-oświatową i sportowo-rekreacyjną, wydatków na korzystanie z obiektów i urządzeń sportowych.

Wypoczynek
W dniu 27.06.2016r. przyznano dofinansowanie do wypoczynku letniego pracowników.
Progi:
- dochód na osobę 1500 zł brutto – dofinansowanie 320 zł
- dochód na osobę 1501-3000 zł brutto – dofinansowanie 300 zł
- dochód na osobę powyżej 3001 brutto – dofinansowanie 280 zł
W dniu 29.07.2016r. przyznano świadczenie socjalne do wypoczynku pracowników administracji i obsługi.
Progi:
- dochód na osobę 1500 zł brutto – świadczenie 710 zł
- dochód na osobę 1501-3000 zł brutto – świadczenie 700 zł
- dochód na osobę powyżej 3001 brutto – świadczenie 690 zł.

Zapomogi
W dniu 1 grudnia 2016r. Decyzją Dyrektora przyznano dofinansowanie do zakupów świątecznych, które pracownicy zorganizują we własnym zakresie.
Progi:
- dochód na osobę do 1500 zł brutto – dofinansowanie 1040 zł
- dochód na osobę 1501-3000 zł brutto – dofinansowanie 1030 zł
- dochód na osobę powyżej 3001 brutto – dofinansowanie 1020 zł
W dniu 3 marca 2016r. przyznano dofinansowania pracownikom szkoły i emerytom z okazji zbliżających się Świąt Wielkanocnych. W regulaminie nie ma takiej formy.

Zgodnie z obowiązującymi interpretacjami prawnymi dotyczącymi zapomogi:
Zapomoga to bezzwrotna pomoc finansowa udzielona osobie fizycznej zwykle w związku ze zdarzeniem losowym. Jest to jednorazowy akt wsparcia kogoś, kto z różnych przyczyn znalazł się w trudnej sytuacji (interpretacja indywidualna dyrektora IS w Bydgoszczy z 5.6.2014 r., ITPB2/415-240/14/IL, Legalis). Cechuje ją doraźność udzielania; nie kwalifikujemy tu świadczeń powtarzalnych, okresowych (decyzja oddziału ZUS w Lublinie z 7.1.2013 r., WPI/200000/451/1399/2012). Aby można było do niej zastosować wskazane zwolnienia, uprawniony musi dostać zapomogę pieniężną w związku z:
1) zdarzeniem losowym – wszelkie nagłe, niespodziewane, pojedyncze zdarzenia wywołane przyczynami zewnętrznymi, których nie można przewidzieć, a które są niezależne od człowieka nawet przy zachowaniu należytej staranności, np. kradzieże, włamania, zniszczenie domu lub mieszkania spowodowane zalaniem wodą lub pożarem, nieszczęśliwe wypadki powodujące uszczerbek na zdrowiu (np. interpretacja indywidualna dyrektora IS w Katowicach z 2.5.2012 r., IBPBII/1/415-110/12/BJ, Legalis);
2) długotrwałą chorobą – schorzenie wymagające długotrwałego leczenia w sposób stały lub przez długi okres, mające długotrwały przebieg. „Nie sposób odwołać się do konkretnych ram czasowych przesądzających o tym, jak długo ma ona trwać, by możliwe było objęcie zapomogi wypłaconej w związku z tą chorobą zwolnieniem z opodatkowania. Z medycznego punktu widzenia długotrwałe choroby to choroby przewlekłe, nieuleczalne, wrodzone. Do chorób długotrwałych zaliczyć należy zatem nie tylko choroby przewlekłe, ale również takie, które mają długotrwały przebieg (trwające

miesiące lub latami) i wymagające leczenia w sposób stały lub przez długi okres" (interpretacja indywidualna dyrektora IS w Poznaniu z 2.12.2011 r., ILPB1/415-1086/11-5/AMN, Legalis);
3) klęską żywiołową – katastrofa naturalna lub awaria techniczna, których skutki zagrażają życiu lub zdrowiu dużej liczby osób, mieniu w wielkich rozmiarach albo środowisku na znacznych obszarach, a pomoc i ochrona mogą być skutecznie podjęte tylko przy zastosowaniu nadzwyczajnych środków, we współdziałaniu różnych organów i instytucji oraz specjalistycznych służb i formacji działających pod jednolitym kierownictwem;
4) śmiercią – w przypadku zwolnienia podatkowego.

Przyznane świadczenia „świąteczne" są zdaniem audytującego wskazaną w ustawie szeroko rozumianą formą pomocy udzielania pomocy materialnej - rzeczowej lub finansowej pracownikom. W regulaminie należałoby wyróżnić taką formę świadczeń finansowych dla pracowników, jak również wskazać kryteria ich przyznawania.

W grudniu 2016r. przyznano pracownikom posiadającym dzieci do 15 roku życia dofinansowanie w wysokości 70 zł na jedno dziecko.

Przyznawanie świadczeń socjalnych (niezależnie od rodzaju dofinansowania) wszystkim w jednakowej kwocie jest niezgodne z ustawą i może rodzić problemy ze strony ZUS i izby skarbowej, ponieważ działanie takie może doprowadzić do potraktowania przez organy kontrolujące dofinansowań, jako dodatków do wynagrodzeń, od których należy pobrać składki i których nie dotyczą zwolnienia podatkowe jak przy wypłacie środków socjalnych. Stanowisko to popiera Ministerstwo Finansów w piśmie z dnia 27 kwietnia 1999 r., nr PB 3-942/722-136/Wk/99.

2. Gospodarka kasowa w jednostce.

W szkole na dzień audytu funkcjonowała procedura wewnętrzna pn. Instrukcja kasowa z 12 listopada 2011r.
W raportach kasowych głównie odnotowywano zbiorczo opłaty za obiady na podstawie dowodów księgowych wewnętrznych.

3. Stosowanie Instrukcji kancelaryjnej.

W § 6 Ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (Dz.U.2015.1446) określono, iż:
1. Organy państwowe oraz państwowe jednostki organizacyjne, organy jednostek samorządu terytorialnego oraz samorządowe jednostki organizacyjne obowiązane są zapewnić odpowiednią ewidencję, przechowywanie oraz ochronę przed uszkodzeniem, zniszczeniem bądź utratą:
1) powstającej w nich dokumentacji, w sposób odzwierciedlający przebieg załatwiania i rozstrzygania spraw;
2) nadsyłanej i składanej do nich dokumentacji, w sposób, o którym mowa w pkt 1.
2. Organy i kierownicy jednostek organizacyjnych, o których mowa w ust. 1, w porozumieniu z Naczelnym Dyrektorem Archiwów Państwowych, określają:
1) instrukcję kancelaryjną określającą szczegółowe zasady i tryb wykonywania czynności kancelaryjnych;
2) sposób klasyfikowania i kwalifikowania dokumentacji w formie jednolitego rzeczowego wykazu akt, który określa klasy, według których w organie lub jednostce organizacyjnej, o których mowa w ust. 1, grupuje się jednolicie, w systemie dziesiętnym, dokumentację powstającą i gromadzoną w tych organach i jednostkach oraz ustala dla dokumentacji kwalifikację archiwalną; jednolity rzeczowy wykaz akt stanowi podstawę oznaczania, rejestracji i grupowania dokumentacji w organie lub jednostce organizacyjnej w chwili wszczynania spraw oraz może być uzupełniony przez kwalifikator dokumentacji, który określa kwalifikację archiwalną jednorodnego rodzaju lub typu dokumentacji;

Instrukcja kancelaryjna obowiązująca w Szkole Podstawowej w Grabowie nie została zatwierdzona

przez Naczelnego Dyrektora Archiwów Państwowych.

Segregatory z dokumentami na dzień audytu nie posiadały nadanych numerów, kategorii archiwalnej, wewnątrz nie było spisów spraw, dokumenty nie były numerowane.

Wyjaśnienie Pani Dyrektor: Pracownik odbył szkolenie z zakresu instrukcji kancelaryjnej. I zabieramy się do pracy.

4. Polityka kadrowa w jednostce – przyznawanie dodatków motywacyjnych i specjalnych.

Zgodnie z art. 36 ust. 5 ustawy o pracownikach samorządowych pracownikowi samorządowemu może zostać przyznany dodatek specjalny z tytułu okresowego zwiększenia obowiązków służbowych lub powierzenia dodatkowych zadań.

W latach 2016 - 2017 dyrektor szkoły nie przyznał żadnemu pracownikowi dodatku specjalnego.

W roku 2016 i 2017 dyrektor przyznał nauczycielom dodatki motywacyjne i wyróżniającym się pracownikom nagrody roczne.
W miesiącach wrzesień-grudzień 2016r. pracownikom administracji i obsługi dyrektor przyznał premie w wysokościach zgodnych z Regulaminem wynagradzania obowiązującym w jednostce.

Audytor dokonał sprawdzenia wynagrodzenia na próbie.
W próbie stwierdzono: wysokość dodatku funkcyjnego dla stanowiska główny księgowych w załączniku nr 1 Regulaminu wynagradzania to 4 czyli zgodnie z załącznikiem nr 3 to 80% najniższego wynagrodzenia zasadniczego w I kategorii zaszeregowania.
W regulaminie wynagradzania przyjęto, że dla I kategoria zaszeregowania minimalne wynagrodzenie zasadnicze wynosi 1700 zł, czyli dodatek powinien wynosić 1496 zł, a w 2016r. wypłacono dodatek funkcyjny w wysokości 450 zł.
Ponadto minimalny poziom wynagrodzenia dla poszczególnych kategorii różni się w tabeli 1 i 2.

Pozostałe składniki wynagrodzenia zgodne były z angażami a wysokość dodatku mieszkaniowego, terenowego, funkcyjnego i za wychowawstwo przyznano zgodnie z Kartą Nauczyciela oraz Uchwałą nr XXXIII/204/09 Rady Miejskiej w Gołdapi z 26 marca 2009r. w sprawie regulaminu wynagradzania i przyznawania dodatków nauczycielom zatrudnionym w szkołach prowadzonych przez Gminę Gołdap.

5. Dofinansowywanie kształcenia nauczycieli

W 2016 r. wydatkowano na dokształcanie i doskonalenia nauczycieli kwotę **12400,00** zł z tego :
4503,73 -indywidualne doskonalenie nauczycieli **max 6450 czyli do 50% kwoty przyznanej**
7789,27 - szkolenie rady pedagogicznej, **max 3225 czyli do 25% kwoty przyznanej**
107,00 -zwrot przejazdów nauczycieli koszty delegacji nauczycieli. **max 3225 czyli do 25% kwoty przyznanej**

Zarządzenie Burmistrza Nr 526/III/2016 z dnia 8 marca 2016 roku w/s planu dofinansowania form doskonalenia zawodowego nauczycieli szkół i przedszkoli prowadzonych przez Gminę Gołdap w § 2 określa przeznaczoną dla szkoły kwotę **12900,00** zł.
W § 3, oznaczono, że środki mogą być wydatkowane następująco: do 50% kwoty na indywidualne formy doskonalenia i dokształcania, do 25% kwoty na organizację szkoleń rad pedagogicznych, seminariów, konferencji, warsztatów metodycznych, do 25% kwoty na zwrot przejazdów nauczycieli, którzy na podstawie delegowania przez dyrektora uczestniczą w różnych formach doskonalenia zawodowego. W związku z reformą oświaty były organizowane dodatkowe szkolenia MEN przygotowujące do przeprowadzenia reformy oświaty, między innymi podstawy programowe i dlatego wydatkowano więcej na szkolenia Rady Pedagogicznej.

6. Dochody własne

W jednostce nie wynajmowano pomieszczeń w latach 2016-2017.
Główne źródło dochodów jednostki to opłaty za wydawane posiłki:

Miesiąc	Wydatki na artykuły żywnościowe	Średnia wartość obiadu	Ilość wydanych obiadów	Wartość wydanych obiadów
2016				
styczeń	9059,79	3,01	3245	9764,42
luty	14907,94	3,21	4744	15231,03
marzec	15539,91	2,56	5591	14338,73
kwiecień	16866,52	3,09	5840	18047,01
maj	17788,83	3,26	5377	17505,50
czerwiec	14328,97	3,37	4732	15969,53
wrzesień	16282,83	2,34	5947	13934,88
październik	16726,00	2,91	5832	16958,59
listopad	17537,62	2,85	5895	16818,64
grudzień	41201,52	7,29	4764	34741,85
2017				
styczeń	5137,05	3,20	3853	12331,47
luty	16000,76	3,27	4870	15930,19
marzec	22525,08	3,40	6577	22361,62
kwiecień	13448,98	3,32	4345	14421,63
maj	21388,02	3,74	5211	19495,09
czerwiec	10838,45	3,58	3910	14002,54
wrzesień	16237,16	2,63	5209	13700,16
październik	15944,44	3,11	5607	17403,71

W jednostce obowiązuje Regulamin stołówki szkolnej.
W roku szkolnym 2016/2017 opłata za obiad wynosiła 4 zł.
Rodzice wychowanków ponoszą odpłatność za posiłki obejmujące koszty zużytych do przygotowania produktów tzw. wsad do kotła.
Opłata za dożywianie dzieci w szkołach na mocy porozumienia z OPS – za obiad 4,00 zł.

7. Inwentaryzacja
Ostatni spis z natury w jednostce przeprowadzono w 2015r.

W roku 2016 w ramach inwentaryzacji rocznej sporządzono:
- protokół z inwentaryzacji kasy,
- protokół weryfikacji sald kont analitycznych,
- protokół inwentaryzacji magazynu żywnościowego,
- potwierdzono salda należności,
- potwierdzono salda rachunków bankowych.

D. INFORMACJA I KOMUNIKACJA
Standard D.16: Bieżąca informacja
Standard D.17: Komunikacja wewnętrzna
Standard D.18: Komunikacja zewnętrzna
W jednostce zwoływane są spotkania pracowników – Rady pedagogiczne. Dyrektor spotyka się

również indywidualnie z poszczególnymi pracownikami szkoły.

E. MONITOROWANIE I OCENA
Standard E.19: Monitorowanie systemu kontroli zarządczej
Standard E.20: Samoocena
Standard E.21: Audyt wewnętrzny
Standard E.22: Uzyskanie zapewnienia o stanie kontroli zarządczej
W jednostce dyrektor podpisał oświadczenie o właściwym funkcjonowaniu kontroli zarządczej.
Audyt wewnętrzny przeprowadzony został w 2016 i w 2017r.

W szkole przeprowadza się samoocenę kontroli zarządczej poprzez analizę wniosków z kontroli zewnętrznych (przeprowadzanych przez kuratorium oświaty, organ prowadzący szkołę, sanepid, straż pożarną itp.) i wewnętrznych działań (hospitacje zajęć, sprawdzanie dokumentacji, inwentaryzacje, itp.) oraz zbierając opinię od pracowników szkoły w anonimowej ankiecie na zakończenie roku szkolnego. Informacje uzyskane w ten sposób wykorzystywane są do organizacji dalszej pracy szkoły i sporządzenia rejestru ryzyka.

Klasyfikacja wyników wg kryteriów

Ocena wystarczająca - audytor zidentyfikował luki czy słabości, jednakże nie mają one istotnego wpływu na poprawności procesu.

Wskazanie słabości kontroli zarządczej i ich skutki

Słabości:

1) Regulamin Zakładowego Funduszu Świadczeń Socjalnych wprowadzony Zarządzeniem nr 06/2017 przez Dyrektora placówki w dniu 13 października 2017r. już w dniu wprowadzenia posiadał nieaktualne podstawy prawne.
2) Nie stosowanie zapisów Regulaminu Zakładowego Funduszu Świadczeń Socjalnych w zakresie dofinansowywania świadczeń nie wskazanych regulaminem np. dofinansowanie do zakupów świątecznych.

Związki zawodowe mają prawo żądania zwrotu środków w przypadku nieprawidłowego, w odniesieniu do ustawy o ZFŚS, dysponowania zasobami pieniężnymi. Związki zawodowe maja prawo złożenia w sądzie pracy roszczenia dotyczącego zwrotu nieprawidłowo wykorzystanych środków.

W przypadku nieprawidłowości pracodawca musi liczyć się także z możliwością kary grzywny przyznanej przez organ kontrolujący fundusz, jakim jest Państwowa Inspekcja Pracy. Wynika to z tego, że kto będąc odpowiedzialnym za właściwe stosowanie przepisów prawa, nie realizuje ich lub stosuje je w sposób niezgodny, podlega karze grzywny. Przepisy te maja w szczególności zastosowanie w przypadku dopuszczania się dyskryminacji ze względu na rodzaj umowy, staż pracy, wymiar czasu pracy, ocena pracy i inne niebędące w myśl ustawy o zakładowym funduszu świadczeń socjalnych kryterium socjalnym.

Dotyczy to również braku konsultacji ze związkami zawodowymi, czy braku wewnętrznego regulaminu funduszu świadczeń socjalnych, stanowiącego o zasadach udzielania pomocy ze środków funduszu socjalnego.

3) Przyznawanie świadczeń z ZFŚS w jednakowej kwocie – pracownikom posiadającym dzieci przyznano świadczenie w kwocie 70 zł na jedno dziecko..

Przyznawanie świadczeń socjalnych (niezależnie od rodzaju dofinansowania) wszystkim w jednakowej kwocie jest niezgodne z ustawą i może rodzić problemy ze strony ZUS i izby skarbowej, ponieważ działanie takie może doprowadzić do potraktowania przez organy kontrolujące dofinansowań, jako dodatków do wynagrodzeń, od których należy pobrać składki i których nie dotyczą zwolnienia podatkowe jak przy wypłacie środków socjalnych. Stanowisko to popiera

Ministerstwo Finansów w piśmie z dnia 27 kwietnia 1999 r., nr PB 3-942/722-136/Wk/99.

4) Instrukcja kancelaryjna obowiązująca w Szkole Podstawowej w Grabowie nie została zatwierdzona przez Naczelnego Dyrektora Archiwów Państwowych. Segregatory z dokumentami na dzień audytu nie posiadały nadanych numerów, kategorii archiwalnej, wewnątrz nie było spisów spraw, dokumenty nie były numerowane.
5) W regulaminie wynagradzania przyjęto, że dla I kategoria zaszeregowania minimalne wynagrodzenie zasadnicze wynosi 1700 zł, czyli dodatek powinien wynosić 1496 zł, a w 2016r. wypłacono dodatek funkcyjny w wysokości 450 zł. Ponadto minimalny poziom wynagrodzenia dla poszczególnych kategorii różni się w tabeli 1 i 2 regulaminu.

Zalecenia

Ad. 1) Aktualizacja Regulaminu ZFŚS pod kątem podstaw prawnych.
Ad. 2) Stosowanie się do zapisów Regulaminu Zakładowego Funduszu Świadczeń Socjalnych zatwierdzonego przez dyrektora i zakładowe związki zawodowe.
Ad. 3) Wydatkowanie środków ZFŚS zgodnie z ustawą i wewnętrznymi regulacjami.
Ad. 4) Wysłanie instrukcji kancelaryjnej obowiązującej w Szkole Podstawowej w Grabowie do zatwierdzenia przez Naczelnego Dyrektora Archiwów Państwowych i stosowanie jej od nowego roku – 2018.
Ad. 5) Uporządkowanie informacji w załącznikach do regulaminu wynagradzania. Przyznawanie dodatków funkcyjnych zgodnie z obowiązującym regulaminem.

V. OPINIA W SPRAWIE ADEKWATNOŚCI, SKUTECZNOŚCI I EFEKTYWNOŚCI BADANYCH ELEMENTÓW SYSTEMU KONTROLI ZARZĄDCZEJ

Badanie audytowe wykazało słabości kontroli zarządczej w obszarach ryzyka objętych zadaniem zapewniającym:
- niestosowanie się do wewnętrznych procedur i zewnętrznych uregulowań w zakresie przyznawania świadczeń z ZFŚS i stosowania instrukcji kancelaryjnej.
Celem zapewnienia adekwatnej, skutecznej i efektywnej kontroli zarządczej w badanych elementach systemu jest wprowadzenie stosownych zmian w zakresie wskazanym w sformułowanych zaleceniach.

Pouczenie

Zgodnie z § 19 Rozporządzenia Ministra Finansów z dnia 4 września 2015r. w sprawie audytu wewnętrznego oraz informacji o pracy i wynikach tego audytu (Dz.U. poz.1480)
§ 17. 1. Audytor wewnętrzny po przeprowadzeniu czynności audytowych uzgadnia pisemnie z audytowanym wstępne wyniki audytu wewnętrznego, w tym w szczególności ustalenia i propozycje zaleceń.
2. W celu uzgodnienia wstępnych wyników audytu wewnętrznego, o których mowa w ust. 1, audytor *wewnętrzny* może przeprowadzić naradę zamykającą.
3. W przypadku nieuzgodnienia wstępnych wyników audytu wewnętrznego, o których mowa w ust. 1, audytowany może zgłosić pisemne zastrzeżenia, w terminie określonym przez audytora wewnętrznego, nie krótszym niż 7 dni kalendarzowych od dnia poinformowania audytowanego o wstępnych wynikach.
§ 19. 1. Kierownik komórki audytu wewnętrznego przekazuje sprawozdanie audytowanemu i kierownikowi jednostki.
2. 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.
3. W przypadku odmowy realizacji zaleceń audytowany przedstawia, w terminie 7 dni kalendarzowych od dnia otrzymania sprawozdania, pisemne stanowisko kierownikowi jednostki i audytorowi wewnętrznemu.
4. W przypadku, o którym mowa w ust. 3, kierownik jednostki podejmuje decyzję dotyczącą realizacji zaleceń, informując o tym audytowanego i kierownika komórki audytu wewnętrznego.
§ 20. Audytor wewnętrzny monitoruje realizację zaleceń.
§ 21. 1. Audytor wewnętrzny po upływie terminów realizacji zaleceń przeprowadza czynności sprawdzające.

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

Sprawozdanie otrzymują:

1) Egz. nr 1 – Burmistrz Gołdapi – wersja papierowa i elektroniczna
2) Egz. nr 2 – Dyrektor Szkoły Podstawowej w Grabowie – wersja elektroniczna

Audytor Wewnętrzny
CGAP S.N.3700
Ewa Krasniewska