SPRAWOZDANIE Z AUDYTU WEWNĘTRZNEGO

TEMAT ZADANIA	Audyt bezpieczeństwa informacji, zgodnie z wymogiem § 20 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.2017.2247)
IMIĘ I NAZWISKO AUDYTORA PRZEPROWADZAJĄCEGO AUDYT	Arkadiusz Pliszka, Justyna Koszel – audytorzy bezpieczeństwa informacji w Zespole Szkolno-Przedszkolnym nr 9 w Rzeszowie
NR UPOWAŻNIENIA	ZSP9.012.15A.2021 r
CEL AUDYTU	Zadanie to ma charakter zadania zapewniającego, którego celem jest dostarczenie niezależnej i obiektywnej oceny działania badanego obszaru oraz wykazanie, że kontrola zarządcza w badanym obszarze funkcjonuje prawidłowo lub wymaga wzmocnienia.
PODMIOTOWY I PRZEDMIOTOWY ZAKRES AUDYTU	Audytowi poddano działanie Zespołu Szkolno-Przedszkolnego nr 9 w Rzeszowie w zakresie bezpieczeństwa informacji przetwarzanej w systemie teleinformatycznym. Przedmiotem audytu było sprawdzenie realizacji obowiązków wynikających z § 20 ust. 1 i 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.2017 .2247).
PODJĘTE CZYNNOSCI I ZASTOSOWANE TECHNIKI	Stosowane podczas audytu narzędzia i techniki to testy przeglądowe, zgodności, kontroli i rzeczywiste oraz przegląd dokumentacji, a także wywiady z pracownikami jednostki audytowanej.
OPIS DZIAŁAŃ JEDNOSTKI W BADANYM OBSZARZE	ZSP nr 9 posiada system teleinformatyczny w rozumieniu ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j. - Dz.U. z 2020 r., poz. 346 ze zm.), czyli zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniający przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieć szkolną za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego w rozumieniu przepisów ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz.U.2020.374 ze zm). Jednostka gromadzi i przetwarza w systemie teleinformatycznym informacje będące informacją publiczną w rozumieniu ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej. Część informacji jest publikowana w serwisie Biuletyn Informacji Publicznej oraz na stronie internetowej http://www.sp19.rzeszow.pl/. Szczególnym zasadom ochrony podlegają informacje zawierające dane osobowe - zgodnie z wymogami ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U.2019.1781)
TERMIN AUDYTU	17 -18.11.2021 r
DATA SPORZĄDZENIA SPRAWOZDANIA	19.11.2021 r

1. STRESZCZENIE

W trakcie audytu stwierdzono, że jednostka jako podmiot realizujący zadania publiczne ustanowiła system zarządzania bezpieczeństwem informacji i zapewnia poufność, dostępność i integralność informacji przetwarzanych w systemie teleinformatycznym z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność – zgodnie z wymogami § 20 ust. 1 i 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.2017.2247).

W trakcie audytu nie stwierdzono uchybień w zakresie 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 oraz utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację.

2. USTALENIA STANU FAKTYCZNEGO ZE SKLASYFIKOWANYMI WYNIKAMI OCENY WEDLUG KRYTERIÓW OCENY STANU FAKTYCZNEGO.

Zgodnie z § 20 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.2017.2247) 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) utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację;
3) przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy;
4) podejmowania działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestnicą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji;
5) bezzwłocznej zmiany uprawnień, w przypadku zmiany zadań osób, o których mowa w pkt 4);
6) zapewnienia szkolenia osobom zaangażowanym 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;
7) 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;
8) ustanowienia podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość;
9) zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie;
10) zawierania w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji;
11) ustalenia zasad postępowania z informacjami, zapewniających minimalizacji wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych;
12) zapewnienia odpowiedniego poziomu bezpieczeństwa, w systemach teleinformatycznych, polegającego w szczególności na:
   a) dbałości o aktualizacje oprogramowania,

b) minimalizowaniu ryzyka utraty informacji w wyniku awarii,
c) zapewnieniu bezpieczeństwa plików systemowych,
d) redukcji ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych,
e) niezwłocznym podejmowaniu działań po dostrzeżeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa,
f) kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa;
13) bezzwłocznego zgłaszania incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących;
14) zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok.

Powyższe działania mają na celu zapewnienie, ze podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląd oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność.

Wymagania te uznaje się również za spełnione, jeżeli system zarządzania bezpieczeństwem informacji został opracowany na podstawie Polskiej Normy PN-ISO/IEC 27001, a ustanawianie zabezpieczeń, zarządzanie ryzykiem oraz audytowanie odbywa się na podstawie Polskich N o r m .
Niezależnie od zapewnienia działań, o których mowa powyżej, w przypadkach uzasadnionych analiz ryzyka w systemach teleinformatycznych podmiotów realizujących zadania publiczne należy ustanowić dodatkowe zabezpieczenia.

Podczas audytu dokonano kategoryzacji informacji pozostającej w zasobach Zespołu Szkolno-Przedszkolnego nr 9 w Rzeszowie, przetwarzanych w systemie teleinformatycznym. Wymogi przepisów prawa w zakresie różnych kategorii informacji i gromadzonych i przetwarzanych w systemie teleinformatycznym nakładając na różne obowiązki związane z funkcjonowaniem i zabezpieczeniami takiego systemu. I tak zidentyfikowano:

1) informacje stanowiące informację publiczną, do której dostęp należy zapewnić poprzez publikację informacji na stronie internetowej szkoły http://www.sp19.rzeszow.pl oraz na stronie Biuletynu Informacji Publicznej.
2) informacje podlegające ochronie czyli dane osobowe, system teleinformatyczny powinien spełniać wymogi określone w ustawie o ochronie danych osobowych i rozporządzeniu wykonawczym do tej ustawy.

2.1. Zapewnienie aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia.

Podczas audytu zidentyfikowano następujące regulacje wewnętrzne zawierające unormowania w zakresie zapewnienia bezpieczeństwa informacji w systemie teleinformatycznym jednostki:

1) Zarządzenie nr 1/05/2018 Dyrektora Zespołu Szkolno-Przedszkolnego nr 9 z dnia 25 maja 2018 r. w sprawie wprowadzenia polityki bezpieczeństwa w zakresie zarządzania systemem informatycznym służącym do przetwarzania danych osobowych i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych. Według zarządzenia na system ten składa się przestrzeganie regulacji jednostki zawierających dane osobowe, szkolenia, zapewnienie fizycznego bezpieczeństwa, współpraca pracowników z administratorem bezpieczeństwa informacji oraz coroczna weryfikacja systemu.

W trakcie audytu sprawdzono na losowo wybranej próbie 5 komputerów aktualność ww. metryk. Stwierdzono, że:

1. Sala nr 16, będąca pod opieką Pani Beaty Kochańskiej, posiada na stanie komputer typu desktop: System operacyjny Windows 10, oprogramowanie antywirusowe Gdata, konto nauczyciela zabezpieczone hasłem, dostęp do platformy edu.erzeszow.pl oraz portal.resman.pl zabezpieczone niezapamiętanym hasłem; aktywna kontrola Internetu oprogramowaniem Beniamin, oraz łącze internetowe OSE posiadające zaawansowane zabezpieczenia użytkowników w lokalnej sieci szkolnej. Aplikacja Teams bez zapisanych haseł użytkowników. Pakiet Office 365 w ramach licencji z Urzędem Miasta w Rzeszowie, oraz oprogramowanie tablicy multimedialnej firmy Avtek.

2. Sala nr 21 nr będąca pod opieką Pani Karoliny Krzanowskiej-Wienc posiada na stanie laptop Lenovo: System operacyjny Windows 10, oprogramowanie antywirusowe Gdata, konto nauczyciela zabezpieczone hasłem, dostęp do platformy edu.erzeszow.pl oraz portal.resman.pl zabezpieczone niezapamiętanym hasłem; aktywna kontrola Internetu oprogramowaniem Beniamin, oraz łącze internetowe OSE posiadające

zaawansowane zabezpieczenia użytkowników w lokalnej sieci szkolnej. Aplikacja Teams bez zapisanych haseł użytkowników. Pakiet Office 365 w ramach licencji z Urzędem Miasta w Rzeszowie, oraz oprogramowanie tablicy multimedialnej firmy Avtek.

3. Sala nr 32 nr będąca pod opieką Pani Renaty Kamyckiej posiada na stanie laptop Toshiba: System operacyjny Windows 10, oprogramowanie antywirusowe Gdata, konto nauczyciela zabezpieczone hasłem, dostęp do platformy edu.erzeszow.pl oraz portal.resman.pl zabezpieczone niezapamiętanym hasłem; aktywna kontrola Internetu oprogramowaniem Beniamin oraz łącze internetowe OSE posiadające zaawansowane zabezpieczenia użytkowników w lokalnej sieci szkolnej. Aplikacja Teams bez zapisanych haseł użytkowników. Pakiet Office 365 w ramach licencji z Urzędem Miasta w Rzeszowie, oprogramowanie tablicy multimedialnej firmy espritDT.

4. Sala nr 13 nr będąca pod opieką Arkadiusza Pliszki posiada na stanie komputer stacjonarny: System operacyjny Windows 10, oprogramowanie antywirusowe Gdata, konto nauczyciela zabezpieczone hasłem, dostęp do platformy edu.erzeszow.pl oraz portal.resman.pl zabezpieczone niezapamiętanym hasłem; aktywna kontrola Internetu oprogramowaniem Beniamin, pakiet Office 365 w ramach licencji z Urzędem Miasta w Rzeszowie. W pracowni jest 26 komputerów uczniowskich posiadających konta o nazwie „Uczeń" i „Uczeń 1-3" oraz konta nauczycielskie zabezpieczone niezapamiętanym hasłem. Na komputerach zainstalowana jest aplikacja Teams, w której nie ma zapisanych haseł użytkowników. Oprogramowanie zainstalowane na w/w komputerach to: pakiet Office 365, aktywna kontrola Internetu oprogramowaniem Beniamin, oraz łącze internetowe OSE posiadające zaawansowane zabezpieczenia użytkowników w lokalnej sieci szkolnej.

5. Sala nr 3 nr będąca pod opieką Pani Elżbiety Dymek posiada na stanie laptop Asus: System operacyjny Windows 10, oprogramowanie antywirusowe Gdata, konto nauczyciela zabezpieczone hasłem, dostęp do platformy edu.erzeszow.pl oraz portal.resman.pl zabezpieczone niezapamiętanym hasłem; aktywna kontrola Internetu oprogramowaniem Beniamin, pakiet Office 365 oraz łącze internetowe OSE posiadające zaawansowane zabezpieczenia użytkowników w lokalnej sieci szkolnej. Aplikacja Teams bez zapisanych haseł użytkowników. Pakiet Office 365 w ramach licencji z Urzędem Miasta w Rzeszowie.

2.2. Przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy.

Polityka reguluje odpowiedzialność za zarządzanie ryzykiem procedurami corocznej identyfikacji ryzyka; bieżące zarządzanie ryzykiem oraz dokumentowanie procesu zarządzania ryzykiem. Polityka określa coroczną identyfikację i analizę ryzyka, z której wynikają jednostki organizacyjne zobowiązane do przeprowadzenia udokumentowanej identyfikacji i analizy ryzyka w drugim półroczu każdego roku kalendarzowego, według zasad określonych w tej polityce. Jednostki wypełniają rejestr ryzyk według wzoru stanowiącego załącznik nr l do polityki.
Na rok 2022 w Zespole Szkolno-Przedszkolnym nr 9 w Rzeszowie, w celu wdrożenia i funkcjonowania mechanizmów kontrolnych zaplanowano następujące działania:
a) szkolenia pracowników z zakresu ochrony danych osobowych. W przypadku zaistnienia potrzeby (np. zmian przepisów) zlecane jest szkolenie dla pracowników;
b) chroniony dostęp do komputerów i serwerowni (zabezpieczenia fizyczne), wykonywanie kopii zapasowych, firewall, program antywirusowy, system bezpieczeństwa informatycznego OSE, bieżący nadzór informatyka, utrzymanie dokumentacji w formie papierowej. Odpowiedzialny za to jest informatyk (Arkadiusz Pliszka).

Podczas audytu stwierdzono podjęcie wszystkich zaplanowanych działań. W obu przypadkach poziom ryzyka rezydualnego po zastosowaniu zaplanowanych mechanizmów kontrolnych określono jako ,,wzorowy".

2.3. 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. Zmiana uprawnień.

Administratorem bezpieczeństwa informacji w zakresie ochrony danych osobowych jest Pan Arkadiusz Pliszka.

Pracownicy posiadający dostęp do danych osobowych mają wystawione stosowne upoważnienia i podpisali oświadczenia zgodne z przyjętymi w jednostce procedurami.

W jednostce istnieją procedury unieważniania nadawanych upoważnień (np. przekreślenie i opis:

anulowano, lub w inny widoczny sposób; na upoważnieniach nieaktualnych stwierdzono ślady potwierdzające, że zostały one anulowane oraz wskazania daty ich anulowania).
W rejestrze (Konta Resman) widnieją daty nadania i odebrania uprawnień wynikających z aktualnego stanowiska pracy i są skrupulatnie aktualizowane w systemie.

2.4. Zapewnienie ochrony przetwarzanych informacji przed nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami. Zabezpieczenia fizyczne.

Jednostka posiada również zabezpieczenia systemu teleinformatycznego mające na celu:

1) monitorowanie dostępu do informacji,
2) czynności zmierzające do wykrycia działań związanych z przetwarzaniem informacji,
3) zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji.

2.5. Zawieranie w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji.

Jednostka nie posiada podpisanej umowy serwisowej, która sprawdza pod kątem stosowania odpowiednich zapisów dotyczących ochrony informacji.
Osoba, która jest zatrudniona w Zespole Szkolno-Przedszkolnym nr 9 w Rzeszowie jako Operator Sprzętu Komputerowego jest odpowiedzialna za poziom bezpieczeństwa informacji oraz za prawidłowe działanie infrastruktury teleinformatycznej jednostki.

2.6. Ustalenie zasad postępowania z informacjami, zapewniających minimalizacji wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym - urządzeń mobilnych. Zapewnienia odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych.

Wymogi zapewnienia odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych regulują następujące akty prawne:

- 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 .2017.2247);

Zgodnie z powyższym rozporządzeniem zapewnienie odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych odbywa się m.in. poprzez:

a) dbałość o aktualizacje oprogramowania,
b) minimalizowanie ryzyka utraty informacji w wyniku awarii,
c) ochrony przed błędami, utracie, nieuprawnionej modyfikacji,
d) stosowanie mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa,
e) zapewnienie 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,

Nie stwierdzono uchybień w powyższym zakresie.

2.7 Zgłaszanie incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących.

Do zgłaszania incydentów został zobligowany każdy pracownik, który stwierdzi naruszenie danych osobowych. Zobowiązano pracowników do natychmiastowego zgłoszenia o tym fakcie bezpośredniego u przełożonego, a w przypadku danych utrwalonych w zbiorach informatycznych – administratora bezpieczeństwa informacji. Regulacje te ustalają sposób postępowania z incydentami naruszenia ochrony danych osobowych.

2.8 Słabości kontroli zarządczej w odniesieniu do ustalonych kryteriów oceny stanu faktycznego, analiza przyczyn tych słabości oraz skutków i ryzyk wynikających ze wskazanych słabości.

Głównym kryterium oceny stanu faktycznego były przepisy:

1) 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.2017.2247);
2) rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 18 stycznia 2007 r. w sprawie Biuletynu Informacji Publicznej (Dz. U. 2007 nr 10, poz. 68).

Nie stwierdzono niezgodności w zakresie stosowania § 20 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagali dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych w obrębie:

- 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.
- utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację.

2.9.Zalecenia.

3) Dołożyć należytej staranności przy podejmowaniu 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) Utrzymywać aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację.

3. Opinia audytora w sprawie adekwatności, skuteczności i efektywności kontroli zarządczej w obszarze objętym audytem.

Audyt dostarcza zapewnienia, że w audytowanym obszarze ustanowiono adekwatne, skuteczne, efektywne mechanizmy kontroli zarządczej. ZSP nr 9 w Rzeszowie posiada wyczerpujące regulacje dotyczące ochrony informacji przetwarzanych w systemie teleinformatycznym.

W Zespole Szkolno-Przedszkolnym nr 9 w Rzeszowie eksploatuje się, monitoruje i dokonuje przeglądów oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji, z uwzględnieniem rodzajów przetwarzanych informacji i wymogów, przepisów prawa w tym zakresie. Nie twierdzono uchybień, które mogłyby być wyeliminowane poprzez wdrożenie zaleceń pozaaudytowych.