AW.1720.4.74.2022

Miejska Biblioteka Publiczna w Koluszkach

Sprawozdanie z audytu wewnętrznego

Temat: Bezpieczeństwo informacji.

Zadanie przeprowadził:

Przemysław Wójcik

Niniejsze zadanie audytowe zostało przeprowadzone zgodnie z planem audytu jako zadanie zapewniające.

Koluszki, grudzień 2022 r.

I. INFORMACJE PODSTAWOWE

1. **Temat zadania audytowego:**

   Bezpieczeństwo informacji.

2. **Nazwa i adres jednostki, w której przeprowadzono audyt wewnętrzny:**

   Miejska Biblioteka Publiczna w Koluszkach

   ul. 11 Listopada 33

   95-040 Koluszki

3. **Data rozpoczęcia zadania zapewniającego:** 05.10.2022 r.

4. **Data sporządzenia sprawozdania z audytu wewnętrznego:** 27.12.2022 r.

5. **Audytor Wewnętrzny:** Przemysław Wójcik

6. **Cel przeprowadzonego zadania audytowego:** dostarczenie Burmistrzowi Koluszek obiektywnej i niezależnej oceny adekwatności, skuteczności i efektywności kontroli zarządczej w zakresie bezpieczeństwa informacji.

7. **Zakres zadania audytowego:**

Podmiotowy: Miejska Biblioteka Publiczna w Koluszkach.

Przedmiotowy: w zakresie przedmiotowym zadanie audytowe obejmowało ocenę:

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 uczestniczą 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 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;

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 minimalizację 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 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;

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

II. USTALENIA I OCENA WEDŁUG KRYTERIÓW PRZYJĘTYCH W PROGRAMIE ZADANIA ZAPEWNIAJĄCEGO

Kryteria przyjęte w programie zadania zapewniającego

Legalność - zgodność z wymogami 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 (t.j. Dz. U. z 2017 r., poz. 2247) oraz przepisami prawa w obszarze bezpieczeństwa informacji (procedury wewnętrzne, zarządzenia, zasady, wytyczne, instrukcje).

Poufność - dostęp do odpowiednich informacji, danych (zarówno wejściowych, jak i wyjściowych) jest ograniczony do właściwych komórek organizacyjnych, a w ramach tych komórek do właściwych osób.

Dostępność - dostęp do odpowiednich informacji, danych (zarówno wejściowych, jak i wyjściowych) jest zapewniony uprawnionym osobom, we właściwym czasie pozwalającym na efektywną realizację danego procesu.

Za błędy istotne w badanym obszarze uznane zostaną niezgodności mające wpływ na bezpieczeństwo informacji w audytowanej jednostce takie jak:

- dane o charakterze służbowym (w tym wrażliwe - np. dane osobowe) są ogólnie dostępne dla nieuprawnionych osób, co może rodzić konsekwencje prawne lub skutkować niewłaściwym wykorzystaniem danych lub wyciekiem danych;

- niektóre dane o charakterze służbowym są dostępne dla zbyt dużej grupy osób lub niektórzy użytkownicy posiadają zbyt szerokie uprawnienia dostępu (dostęp do danych, które nie są konieczne do realizacji obowiązków służbowych), co może skutkować niewłaściwym wykorzystaniem przez te osoby danych.

Audytor dokonał klasyfikacji wyników dla poszczególnych kryteriów w oparciu o profesjonalny osąd, biorąc pod uwagę czynnik istotności ewentualnych niepożądanych zdarzeń. Zastosowano czterostopniową skale oceny adekwatności, skuteczności i efektywności podejmowanych działań lub zastosowanych mechanizmów kontrolnych:

- adekwatne,
- wystarczające,
- z zastrzeżeniami,
- nieadekwatne.

Ocena adekwatna oznaczać będzie, że istniejące mechanizmy oraz procedury w pełni odpowiadają potrzebom oraz wymogom prawa.

Ocena wystarczająca oznacza, że zidentyfikowano słabości w badanym procesie, jednakże są one nieistotne lub mają niewielki wpływ na bezpieczeństwo informacji.

Ocena z zastrzeżeniami oznacza wystąpienie istotnych słabości, jednakże proces ma miejsce, ale wymaga dużych usprawnień.

Ocena nieadekwatna oznacza, iż proces nie spełnia swojego zadania, nie służy realizacji celów postawionych przed jednostką, a badany obszar wymaga poważnych usprawnień.

Lp.	Wymóg rozporządzenia w sprawie Krajowych Ram Interoperacyjności, w odniesieniu do systemu teleinformatycznego	Ustalenia stanu faktycznego
1.	Zapewnienie aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia.	Wdrożono System Zarządzania Bezpieczeństwem Informacji (SZBI), którego głównymi elementami są: Polityka Bezpieczeństwa Informacji (PBI), Polityka ochrony danych osobowych (PODO), Instrukcja zarządzania systemem informatycznym (IZSI). Wdrożony w 2022 r. SZBI przewiduje przegląd i aktualizację polityk oraz procedur dokonywaną przez odpowiedzialne osoby w celu jak najlepszej reakcji na zagrożenia i incydenty. Przegląd tego systemu powinien zostać przeprowadzony w 2023 r. Na potrzeby SZBI zdefiniowano role mające szczególne obowiązki w obszarze ochrony informacji oraz opisano obowiązki poszczególnych ról w obszarze zarządzania bezpieczeństwem informacji dla następujących osób: Administrator Danych Osobowych, Administrator Informacji – AI, Administrator Systemów Informatycznych (ASI), Inspektor Ochrony Danych Osobowych (IOD).
2.	Utrzymywanie aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację.	Utrzymanie aktualności inwentaryzacji sprzętu jest ewidencjonowane w księdze inwentarzowej, gdzie prowadzony jest stan ilościowy i wartościowy.
3.	Przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy.	Została opracowana analiza ryzyka utraty integralności, dostępności lub poufności w zakresie bezpieczeństwa informacji (w listopadzie 2022 r.).
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.	Administrator danych zapewnia kontrolę nad tym, jakie dane osobowe, kiedy i przez kogo zostały wprowadzone do zbioru oraz komu są przekazywane. Administrator danych prowadzi ewidencję osób upoważnionych do ich przetwarzania. Ewidencja zawiera imię i nazwisko osoby upoważnionej, datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych, identyfikator, jeżeli dane są przetwarzane w systemie informatycznym, który jest unikalny i w powiązaniu z hasłem jednoznacznie identyfikuje każdego użytkownika. Użytkownicy posiadają imienne upoważnienia do przetwarzania danych osobowych. Osoby, które przetwarzają dane osobowe złożyły oświadczenie o zachowaniu tajemnicy danych, z którymi mają styczność.
5.	Bezzwłocznej zmiany uprawnień, w przypadku zmiany zadań osób, o których mowa w pkt 4.	Nie dotyczy.

Lp.	Wymóg rozporządzenia w sprawie Krajowych Ram Interoperacyjności, w odniesieniu do systemu teleinformatycznego	Ustalenia stanu faktycznego
6.	Zapewnienie 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.	Dokonane ustalenia potwierdzają, że zapewniono szkolenia dla osób zaangażowanych w proces przetwarzania informacji. Szkolenie przeprowadzono w dniu 07.11.2022 r.
7.	Zapewnienie 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.	W systemie informatycznym służącym do przetwarzania danych osobowych stosuje się mechanizmy kontroli dostępu do tych danych. Zapewnia się, aby w systemie informatycznym rejestrowany był dla każdego użytkownika odrębny identyfikator. Zapewnia się, aby dostęp do danych był możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia. System informatyczny służący do przetwarzania danych osobowych zabezpiecza się, przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego.
8.	Ustanowienie podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość.	Nie dotyczy.
9.	Zabezpieczenie informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie.	Dyski, które nie będą wykorzystywane są składowane.
10.	Zawieranie w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji.	W zawartych przez jednostkę umowach serwisowych uwzględniono bezpieczeństwo informacji. Dokumentacja licencyjna jest przechowywana w zamkniętym pomieszczeniu, do którego dostęp mają wyłącznie osoby upoważnione.
11.	Ustalanie zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych.	Ekrany monitorów ustawiono w taki sposób, żeby uniemożliwić odczyt wyświetlanych danych osobowych osobom nieupoważnionym. W razie konieczności opuszczenia stanowiska pracy, które jest przyłączone do sieci informatycznej lub stanowiska służącego do przetwarzania danych użytkownik ma ustawioną konfigurację wygaszacza ekranu lub blokady ekranu w taki sposób, by normalna praca była możliwa wyłącznie po podaniu hasła.

Lp.	Wymóg rozporządzenia w sprawie Krajowych Ram Interoperacyjności, w odniesieniu do systemu teleinformatycznego	Ustalenia stanu faktycznego
12.	Zapewnienie 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.	Brak zabezpieczenia systemu informatycznego służącego do przetwarzania danych osobowych przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej (np. urządzenia typu UPS). Powyższe stwierdzono w 6 przypadkach. Dyrektor Miejskiej Biblioteki Publicznej w Koluszkach jako Administrator Danych Osobowych jest zobowiązany do zabezpieczenia systemu informatycznego przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej. W tym celu należy wykorzystać system podtrzymywania lub awaryjnego zasilania np. urządzenia typu UPS. Dane osobowe przetwarzane w systemie informatycznym zabezpiecza się przez wykonywanie kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych. Kopie zapasowe przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem. System informatyczny służący do przetwarzania danych osobowych zapewnia odnotowanie identyfikatora użytkownika wprowadzającego dane osobowe do systemu. Na stanowiskach zainstalowano oprogramowanie antywirusowe i jest aktywna ochrona antywirusowa.
13.	Bezzwłoczne zgłaszanie incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących.	W badanym okresie nie były zgłaszane przypadki naruszenia bezpieczeństwa danych osobowych.

Ocena według kryteriów przyjętych w programie.

Audytor ocenia pozytywnie badany proces, biorąc pod uwagę przyjęte kryteria w zakresie:

- *poufności* - dostęp do odpowiednich informacji, danych (zarówno wejściowych, jak i wyjściowych) jest ograniczony do właściwych komórek, a w ramach komórek do właściwych osób.

- *dostępności* - dostęp do odpowiednich informacji, danych (zarówno wejściowych, jak i wyjściowych) jest zapewniony uprawnionym osobom, we właściwym czasie pozwalającym na efektywną realizację danego procesu.

Nie stwierdzono w badanym obszarze niezgodności mających wpływ na bezpieczeństwo informacji w audytowanej jednostce, takich jak:

- dane o charakterze służbowym (w tym wrażliwe - np. dane osobowe) są ogólnie dostępne dla

nieuprawnionych osób, co może rodzić konsekwencje prawne lub skutkować niewłaściwym wykorzystaniem danych lub wyciekiem danych;
- niektóre dane o charakterze służbowym są dostępne dla zbyt dużej grupy osób lub niektórzy użytkownicy posiadają zbyt szerokie uprawnienia dostępu (dostęp do danych, które nie są konieczne do realizacji obowiązków służbowych), co może skutkować niewłaściwym wykorzystaniem przez te osoby danych.

III. ZALECENIA

1. Zgodnie z obowiązującą Polityką Bezpieczeństwa Informacji zaleca się powołanie w jednostce organizacyjnej Administratora Systemów Informatycznych (ASI), którego celem będzie nadzorowanie i realizowanie zasad bezpieczeństwa przetwarzania i ochrony danych w systemach informatycznych, zabezpieczenie sprzętu komputerowego przed nieuprawnionym dostępem oraz przeprowadzanie analizy ryzyka uwzględniającej realne zagrożenia dla systemu informatycznego. Szczegółowy zakres działania ASI został określony w treści wprowadzonego Systemu Zarządzania Bezpieczeństwem Informacji (SZBI).
2. W Polityce Bezpieczeństwa Informacji należy określić w jakich zaplanowanych odstępach czasu powinien być wykonany przegląd Systemu Zarządzania Bezpieczeństwem Informacji oraz wskazać osoby odpowiedzialne za dokonywanie corocznego przeglądu SZBI. Należy sprecyzować procedurę, iż w regularnych odstępach czasu, nie rzadziej niż raz w roku, cała dokumentacja SZBI powinna zostać objęta przeglądem pod względem aktualności i adekwatności. Przeglądu należy dokonać również, gdy wystąpią istotne zmiany. Zaleca się, aby do każdej polityki przypisana była osoba odpowiedzialna za dokonanie przeglądu np. przeglądu Polityki Bezpieczeństwa Informacji, Polityki ochrony danych osobowych będzie dokonywał IOD, natomiast przegląd Instrukcji zarządzania systemami informatycznymi przeprowadzi ASI. Powyższe zalecenie wynika z Normy PN-EN ISO/IEC 27001 załącznika A oraz PN-EN ISO/IEC 270012 (A.5.1.2 – Przegląd polityk bezpieczeństwa informacji).
3. Wprowadzić dodatkową procedurę dotyczącą przeglądów Systemu Zarządzania Bezpieczeństwem Informacji, która będzie zawierać wzór dokonywanego corocznie przeglądu np. poprzez wprowadzenie tzw. *„Karty przeglądu SZBI”* lub wprowadzić stosowne zapisy w celu sprecyzowania, iż wymagany przegląd swoim zakresem będzie obejmował odniesienie się do 114 punktów kontrolnych na podstawie Polskich Norm PN-ISO/IEC 27001 i PN-ISO/IEC 27002.

4. Rozważyć wprowadzenie do Systemu Zarządzania Bezpieczeństwem Informacji dodatkowej procedury, która będzie określać termin i metodykę analizy ryzyka utraty integralności, dostępności lub poufności informacji. Mając na uwadze, iż zgodnie z zapisami Polityki Bezpieczeństwa Informacji to Administrator Informacji (kierownik jednostki organizacyjnej) wspólnie z Inspektorem Ochrony Danych analizuje ryzyko bezpieczeństwa informacji dla zasobów w zakresie, których sprawuje nadzór. Natomiast Administrator Systemów Informatycznych (ASI) wspólnie z Inspektorem Ochrony Danych (IOD) analizuje ryzyko bezpieczeństwa informacji dla danych osobowych przetwarzanych w systemach teleinformatycznych oraz analizuje ryzyko bezpieczeństwa informacji dla zasobów w zakresie których sprawuje nadzór. Wskazane jest w procedurze zastosować wzór np. karty ryzyka bezpieczeństwa informacji, którą będzie wypełniać AI, IOD i ASI w celu określenia zagrożenia, podatności, wpływu i prawdopodobieństwa ryzyka w otoczeniu fizycznym, infrastruktury technicznej, sprzętu, teleinformatyki, dokumentacji i personelu. Procedura będzie pomocna do udokumentowania przeprowadzonej analizy ryzyka utraty integralności, dostępności lub poufności informacji, mając na uwadze § 20 ust. 2 pkt 3 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 (t.j. Dz. U. z 2017 r., poz. 2247), Polskich Norm PN-ISO/IEC 27001, PN-ISO/IEC 27002, PN-ISO/IEC 27005.

5. Zapewnić przeprowadzenie w 2023 r. przez Inspektora Ochrony Danych tzw. audytów RODO (audytów ochrony danych osobowych) mając na uwadze art. 39 ust. 1 lit. b) rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE, z którego wynika, iż jednym z głównych obowiązków wyznaczonego w organizacji Inspektora Ochrony Danych jest monitorowanie przestrzegania niniejszego rozporządzenia, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty.

6. Zabezpieczyć system informatyczny służący do przetwarzania danych osobowych przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej (np.

poprzez zakup urządzenia typu UPS) dla komputerów stacjonarnych.

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

Audyt bezpieczeństwa informacji został przeprowadzony jako audyt zgodności z przepisami 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. z 2017 r., poz. 2247). Minimalne wymagania odnośnie systemów teleinformatycznych zostały określone w § 20 ust. 2 w/w rozporządzenia.

Stwierdzono spełnienie przez Miejską Bibliotekę Publiczną w Koluszkach wymagań określonych w § 20 ust. 3 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. z 2017 r., poz. 2247). System zarządzania bezpieczeństwem informacji w jednostce został opracowany na podstawie Polskiej Normy PN-ISO/IEC 27001, a ustanawianie zabezpieczeń, zarządzanie ryzykiem oraz audytowanie odbywa się na podstawie Polskich Norm związanych z tą normą, w tym:

1) PN-ISO/IEC 27002 - w odniesieniu do ustanawiania zabezpieczeń;
2) PN-ISO/IEC 27005 - w odniesieniu do zarządzania ryzykiem;
3) PN-ISO/IEC 24762 - w odniesieniu do odtwarzania techniki informatycznej po katastrofie w ramach zarządzania ciągłością działania.

Zgodnie z § 20 ust. 1 ww. rozporządzenia podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali SZBI zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność. Wymagania dotyczące SZBI zostały określone w § 20 ust. 1 i 2 ww. rozporządzenia. Jednocześnie ust. 3 stanowi, że w przypadku, gdy zobowiązany podmiot opracuje stosowany przez siebie SZBI na podstawie Polskiej Normy PN-ISO/IEC 27001 (...), to stosowanie takiego SZBI przez ten podmiot uznaje się za spełnienie wymogów określonych w § 20 ust. 1 i 2 ww. rozporządzenia. Ww. rozporządzenie stanowi akt wykonawczy do ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2021 r. poz.

2070), wydany na podstawie art. 18 tej ustawy. W związku z powyższym przepisy ww. rozporządzenia stosuje się do podmiotów określonych w art. 2 ww. ustawy.

Nie stwierdzono w audytowanej jednostce niezgodności mających wpływ na bezpieczeństwo informacji, które mogą bezpośrednio powodować konsekwencje prawne lub skutkować niewłaściwym wykorzystaniem danych lub wyciekiem danych.

W związku z uzyskanymi rezultatami badań wydano 6 zaleceń w celu wyeliminowania słabości kontroli zarządczej oraz wprowadzenia usprawnień w badanym obszarze.

Mając na uwadze dokonane ustalenia, zidentyfikowane słabości w badanym procesie, stwierdza się, iż ogólna ocena adekwatności, skuteczności i efektywności kontroli zarządczej w obszarze działalności jednostki objętym zadaniem została wydana jako ocena pozytywna z zastrzeżeniami.*

Na tym badanie zakończono.

AUDYTOR WEWNĘTRZNY

[redacted]

mgr Przemysław Wójcik

27.12.2022 r. .....

(data, podpis)

Niniejsze sprawozdanie zostało sporządzone w trzech jednobrzmiących egzemplarzach, które otrzymują:

1. Pan Waldemar Chałat – Burmistrz Koluszek
2. Pan Jarosław Woźniak – Dyrektor Miejskiej Biblioteki Publicznej
3. akta bieżące zadania audytowego AW.1720.4.74.2022

Ocena adekwatna oznacza, że istniejące mechanizmy oraz procedury w pełni odpowiadają potrzebom oraz wymogom prawa.

Ocena wystarczająca oznacza, że zidentyfikowano słabości w badanym procesie, jednakże są one nieistotne lub mają niewielki wpływ na bezpieczeństwo informacji.

*Ocena z zastrzeżeniami oznacza wystąpienie istotnych słabości, jednakże proces ma miejsce, ale wymaga dużych usprawnień.

Ocena nieadekwatna oznacza, iż proces nie spełnia swojego zadania, nie służy realizacji celów postawionych przed jednostką, a badany obszar wymaga poważnych usprawnień.