Nowy Tomyśl, dn. 12.10.2015 r.

BAiKW.1720.3.2015

# SPRAWOZDANIE

## Z ZAPEWNIAJĄCEGO ZADANIA AUDYTOWEGO W OBSZARZE RYZYKA

Zarządzanie zasobami i aktywami systemów informacyjnych

Odebrano w dn. 14.10.2015 r.

Nowy Tomyśl, październik 2015

# Spis treści

# 1 Wprowadzenie

## 1.1 Temat zadania

Zarządzanie aktywami i aktywami systemów informacyjnych

## 1.2 Cele zadania zapewniającego

Udzielenie odpowiedzi na pytania:

- Czy w UM w Nowym Tomyślu wszystkie środki przetwarzania informacji zostały zidentyfikowane?
- Czy w UM w Nowym Tomyślu sporządzono i utrzymuje się spis wszystkich ważnych środków przetwarzania informacji?
- Czy wszystkie ważne środki przetwarzania informacji mają właściciela w postaci wydzielonej części organizacji.

## 1.3 Podmiotowy zakres zadania

Urząd Miasta w Nowym Tomyślu

## 1.4 Przedmiotowy zakres zadania

Rozwiązania organizacyjne w zakresie zarządzania urządzeniami służącymi do przetwarzania informacji

## 1.5 Data rozpoczęcia zadania zapewniającego

17.07.2015 r.

## 2 Opinia Audytora wewnętrznego

W opinii Audytora wewnętrznego przeprowadzającego zadanie audytowe zebrana podczas realizacji zadania audytowego dokumentacja i przeprowadzona analiza stanu faktycznego wskazują na niski stopień adekwatności, skuteczności i efektywności systemu kontroli zarządczej w obszarze ryzyka objętym audytem.

Podczas realizacji zadania audytowego Audytor wewnętrzny przeprowadził czynności audytowe podczas których stwierdzono, że w badanym obszarze występuje ryzyko, iż nie wszystkie środki przetwarzania informacji znajdujące się w posiadaniu Urzędu Miejskiego zostały w sposób prawidłowy zidentyfikowane. Ponadto Audytor wewnętrzny stwierdził, iż w Nowym Tomyślu brakuje wyodrębnionego spisu (ewidencji) wszystkich ważnych środków przetwarzania informacji oraz stwierdził, iż nie wszystkie ważne środki przetwarzania informacji mają określonego (przypisanego) właściciela w postaci wydzielonej części organizacji (lub pracownika).

Mając na względzie powyższe ustalenia, a także uchybienia polegające na braku numerów inwentarzowych na urządzeniach służących do przetwarzania informacji, przenoszeniu sprzętu komputerowego i peryferyjnego bez powiadamiania pracowników odpowiedzialnych za ewidencjonowanie tego sprzętu, braku możliwości potwierdzenia legalności użytkowanego oprogramowania i niezgodnościach w ewidencji środków trwałych Audytor wewnętrzny zaleca niezwłoczne podjęcie działań zmierzających do usunięcia istniejących uchybień i przywrócenie funkcjonowania jednostki do stanu zgodnego z przepisami prawa.

# 3 Ustalenia stanu faktycznego wraz ze sklasyfikowanymi wynikami ich oceny według kryteriów

## 3.1 Wprowadzenie

O skuteczności działania i rozwoju instytucji (organizacji) świadczy stopień osiągania zamierzonego celu. W procesie tym bardzo ważne jest stosowanie współczesnych technik i technologii, narzędzi i systemów informatycznych oraz przetwarzania i zarządzania informacją. Informacja jest jednym z ważniejszych zasobów instytucji, na ogół decydującym o jej sukcesach. Dlatego powinna być chroniona zarówno przez kierownictwo, jak i pozostałych pracowników.

Ważne jest, aby zapewnić ochronę informacji na pożądanym poziomie, a tym samym spełnić wymagany poziom bezpieczeństwa systemów informacyjnych. W tym celu należy odpowiednio zorganizować zasoby instytucji i skutecznie nimi zarządzać, czyli mieć właściwie opracowaną i bezwzględnie przestrzeganą politykę bezpieczeństwa informacji (PBI) instytucji.

**Istota polityki bezpieczeństwa informacji instytucji**

W każdej instytucji (organizacji) znajdują się różnorodne informacje, które z reguły powinny być chronione; część ze względu na interes instytucji (np. informacje finansowe i inwestycyjne.), część zaś z mocy prawa (np. zbiory danych osobowych, informacje niejawne).

Zasadniczy zbiór informacji instytucji jest jawny i dotyczy całości problemów związanych z jej funkcjonowaniem. Nie oznacza to, że nie powinien być chroniony, wręcz przeciwnie, każda bowiem informacja jest podatna na zagrożenia (np. zniszczenie czy zafałszowanie) lub niepożądane modyfikowanie.

Celem działań w zakresie ochrony i zapewnienia bezpieczeństwa informacji w instytucji jest osiągnięcie takiego poziomu organizacyjnego i technicznego, który:
– zagwarantuje zachowanie poufności informacji chronionych;
– zapewni integralność informacji chronionych i jawnych oraz dostępność do nich;
– zagwarantuje wymagany poziom bezpieczeństwa przetwarzanych informacji;
– maksymalnie ograniczy występowanie zagrożeń dla bezpieczeństwa informacji;
– zapewni poprawne i bezpieczne funkcjonowanie systemów przetwarzania informacji;
– zapewni gotowość do podejmowania działań w sytuacjach kryzysowych.

Najogólniej ujmując, PBI jest zbiorem dokumentów, określających metody i zasady ochrony oraz zapewnienia bezpieczeństwa informacji w instytucji. PBI jest zbiorem spójnych, precyzyjnych i zgodnych z obowiązującym prawem przepisów, reguł i procedur, według których dana instytucja (organizacja) buduje, zarządza i udostępnia zasoby oraz systemy informacyjne i informatyczne. W szczególności w PBI powinny być zdefiniowane zasoby, które należy chronić i sposoby (metody) tej ochrony.

W PBI powinny być określone zasady ochrony grup informacji, dotyczące sposobów ich przetwarzania i przechowywania, z uwzględnieniem nie tylko zagadnień bezpieczeństwa i komunikacji przetwarzanych informacji, sprzętu i oprogramowania, za pomocą których

są przetwarzane informacje, lecz również ludzi, którzy te informacje przetwarzają. Punktem wyjścia do tworzenia PBI jest wyznaczenie grup informacji, które powinny podlegać ochronie.

Polityka bezpieczeństwa informacji stanowi podłoże do tworzenia dokumentów, zawierających specyficzne wymagania dla konkretnych grup informacji, a także określających warunki, jakie muszą spełniać systemy informatyczne i papierowe je przetwarzające, z uwzględnieniem aspektów prawnych ochrony informacji i systemów informatycznych.

W praktyce są rożne metody tworzenia PBI instytucji. Jednak, bez względu na to, jakiego są to typu rozwiązania, jest ważne, aby opracowana PBI odpowiadała potrzebom danej instytucji, w zakresie skutecznej ochrony gromadzonych i przetwarzanych w niej informacji.

### 3.2 Kryteria dokonania oceny ustaleń

Wszystkie aktywa należy zinwentaryzować i wyznaczyć właściciela odpowiedzialnego za utrzymanie zabezpieczeń. Właściciel – osoba lub podmiot - ponosi kierowniczą odpowiedzialność za rozwój, utrzymanie i użytkowanie oraz bezpieczeństwo aktywów.

Właściciel aktywów jest odpowiedzialny przede wszystkim za poprawność sklasyfikowania aktywów powiązanych ze środkami przetwarzania informacji oraz zdefiniowanie i przegląd ograniczeń dostępu jak również za klasyfikacje informacji.

Przedmiotem własności może być:

- sprzęt komputerowy
- informacja,
- proces (zespół czynności, działanie),
- procedura (przepis wewnętrzny, polityka),
- aplikacja (program komputerowy),
- zbiór danych.

W skomplikowanych systemach informacyjnych zaleca się wydzielenie grup aktywów, które spełniają pełną funkcję określaną mianem usługi.

Aktywa powinny mieć przypisaną wagę. Wykaz aktywów powinien zawierać informacje niezbędne do odtworzenia po katastrofie, co najmniej:

- typy aktywów aktywa fizyczne (np. sprzęt i akcesoria komputerowe, oprogramowanie (systemowe i użytkowe), urządzenia łączności), informacje usługi (przetwarzanie, przesyłanie i usługi logistyczne), pracownicy (ich kwalifikacje umiejętności i doświadczenie), wartości niematerialne (wizerunek firmy),
- format aktywu,
- lokalizację aktywu,
- informacje o kopiach zapasowych, licencjach i wartości biznesowej.

Informacje jako typ aktywów to: bazy danych, umowy, dokumentacje systemowe, podręczniki, materiały szkoleniowe, procedury, plany ciągłości działania, plany odtworzeniowe, zapisy audytowe, informacje zarchiwizowane.

Pracownicy instytucji oraz wykonawcy powinni stosować się do zasad akceptowalnego użycia aktywów związanych ze środkami przetwarzania informacji, w szczególności korzystania z Internetu i poczty elektronicznej oraz urządzeń przenośnych.

### 3.2.1 Kryteria dokonania oceny ustaleń

**Ocena systemu kontroli zarządczej**

| Obiekt | | Ocena (1:5) |
|---|---|---|
| Zarządzanie środkami przetwarzania informacji. | Adekwatność | |
| | Skuteczność | |
| | Efektywność | |

Audytor dokonując oceny systemu kontroli zarządczej, przyjął następujące definicje pojęć i skalę ocen:
**Adekwatność** – adekwatny system kontroli zarządczej oznacza system zaprojektowany w sposób racjonalny, zgodny z przepisami prawa i zapewniający odpowiednie zasoby – finansowe, ludzkie, rzeczowe i informacyjne – w celu realizacji wyznaczonych celów i zadań. Funkcjonujące mechanizmy zostały opracowane w odpowiedzi na istotne ryzyka związane z działalnością jednostki, celem ograniczenia możliwości ich wystąpienia do akceptowalnego poziomu.
Skala ocen:
Ocena 1 – system nieadekwatny
Ocena 2 – system mało adekwatny – z licznymi / z istotnymi niezgodnościami / uchybieniami
Ocena 3 – system średnio adekwatny – ze średnią ilością/z istotnymi niezgodnościami/uchybieniami
Ocena 4 – system adekwatny z nielicznymi / mało istotnymi niezgodnościami/uchybieniami
Ocena 5 – system adekwatny
**Skuteczność** – skuteczny system kontroli zarządczej oznacza system funkcjonujący w zamierzony sposób, umożliwiający realizację wyznaczonych celów i zadań oraz pomiar stopnia zaawansowania ich realizacji. Istniejące mechanizmy kontrolne zostały zaprojektowane i są stosowane w sposób pozwalający na zminimalizowanie potencjalnego ryzyka niezrealizowania zakładanego rezultatu – ww. celów i zadań.
Skala ocen:
Ocena 1 – system nieadekwatny
Ocena 2 – system mało adekwatny – z licznymi / z istotnymi niezgodnościami / uchybieniami
Ocena 3 – system średnio adekwatny – ze średnią ilością/z istotnymi niezgodnościami/uchybieniami
Ocena 4 – system adekwatny z nielicznymi / mało istotnymi niezgodnościami/uchybieniami
Ocena 5 – system adekwatny
**Efektywność** – efektywny system kontroli zarządczej oznacza system wspierający realizację założonych celów i zadań, przy założeniu osiągnięcia najwyższych możliwych rezultatów przy wykorzystaniu jak najmniejszych możliwych nakładów. Koszty wdrożenia i funkcjonowania mechanizmów kontrolnych są odpowiednie w stosunku do uzyskiwanych w wyniku ich stosowania korzyści.
Skala ocen:
Ocena 1 – system nieadekwatny
Ocena 2 – system mało adekwatny – z licznymi / z istotnymi niezgodnościami / uchybieniami
Ocena 3 – system średnio adekwatny – ze średnią ilością/z istotnymi niezgodnościami/uchybieniami
Ocena 4 – system adekwatny z nielicznymi / mało istotnymi niezgodnościami/uchybieniami
Ocena 5 – system adekwatny

## 3.3 Stan faktyczny

Podczas realizacji zadania ustalono, że w Urzędzie Miejskim w Nowym Tomyślu nie prowadzi się wydzielonej ewidencji środków przetwarzania informacji (komputery, drukarki, skanery itp.) Ewidencja taka powinna zawierać co najmniej:

- wskazanie rodzaju sprzętu służącego do przetwarzania informacji,
- dokument wskazujący na nabycie sprzętu (faktura, umowa),
- nr inwentarzowy sprzętu,
- zainstalowane oprogramowanie,
- związane z oprogramowaniem licencje,

- osobę, której oddano sprzęt do użytkowania (właściciela sprzętu).

Wg informacji pozyskanych podczas audytu część niezbędnych dla prawidłowego funkcjonowania audytowanego obszaru informacji zawiera ewidencja środków trwałych Urzędu Miejskiego w Nowym Tomyślu prowadzona w programie SIGID.

Korzystając z informacji zawartych w tej ewidencji wylosowano próbkę 9 komputerów do sprawdzenia zgodności stanu ewidencyjnego ze stanem faktycznym.

W przypadku pierwszego sprawdzanego komputera stwierdzono, iż komputer użytkowany jest przez Wydział Finansowy. Jako użytkownik tego komputera został wskazany jeden z pracowników Urzędu, komputer faktycznie znajduje się w posiadaniu innego z pracowników Urzędu. Na komputerze umieszczono naklejkę z nr inwentarzowym. Nie stwierdzono występowania nielegalnego oprogramowania. Nie stwierdzono również, aby na dysku twardym tego komputera przechowywane były materiały (muzyka, filmy) objęte prawami autorskimi. Oprogramowanie operacyjne to Windows XP – system operacyjny bez wsparcia technicznego producenta podatny na infekcje – stanowiący zagrożenie dla informacji zgromadzonych i przetwarzanych na tym komputerze oraz pozostałych jednostkach funkcjonujących w tej samej sieci intranetowej. Programy użytkowe zainstalowane na badanym komputerze spełniały wymogi bezpieczeństwa. Na monitorze brak naklejki z nr inwentarzowym.

W przypadku drugiego sprawdzanego komputera stwierdzono, iż komputer użytkowany jest przez Wydział Finansowy i znajduje się w posiadaniu pracownika tego wydziału. Komputer oznaczony symbolem UM A33-1 znajdował się w pomieszczeniu nr 33. Na komputerze umieszczono nr inwentarzowy. Nie stwierdzono występowania nielegalnego oprogramowania. Nie stwierdzono również, aby na dysku twardym tego komputera przechowywane były materiały (muzyka, filmy) objęte prawami autorskimi. Oprogramowanie operacyjne to Windows XP – system operacyjny bez wsparcia technicznego producenta podatny na infekcje – stanowiący zagrożenie dla informacji zgromadzonych i przetwarzanych na tym komputerze oraz pozostałych jednostkach funkcjonujących w tej samej sieci intranetowej. Programy użytkowe zainstalowane na badanym komputerze spełniały wymogi bezpieczeństwa. Na monitorze znajduje się naklejka z nr inwentarzowym różnym od nr komputera.

W przypadku trzeciego sprawdzanego komputera stwierdzono, iż komputer użytkowany jest przez Wydział Finansowy i znajduje się w posiadaniu pracownika tego wydziału. Komputer oznaczony symbolem UM A32 znajdował się w pomieszczeniu nr 32. Na komputerze nie umieszczono nr inwentarzowego. Nie stwierdzono występowania nielegalnego oprogramowania. Nie stwierdzono również, aby na dysku twardym tego komputera przechowywane były materiały (muzyka, filmy) objęte prawami autorskimi. Oprogramowanie operacyjne i użytkowe zainstalowane na badanym komputerze spełniało wymogi bezpieczeństwa.

W przypadku czwartego sprawdzanego komputera stwierdzono, iż komputer użytkowany jest przez Wydział UiGN i znajduje się w posiadaniu pracownika tego wydziału. Komputer oznaczony symbolem UM A34-b znajdował się w pomieszczeniu nr 34. Na komputerze znajduje się naklejka z nr inwentarzowym. Nie stwierdzono występowania nielegalnego

oprogramowania. Nie stwierdzono również, aby na dysku twardym tego komputera przechowywane były materiały (muzyka, filmy) objęte prawami autorskimi. Oprogramowanie operacyjne i użytkowe zainstalowane na badanym komputerze spełniało wymogi bezpieczeństwa. Na monitorze znajduje się naklejka z innym, niż na komputerze nr inwentarzowym.

W przypadku piątego sprawdzanego komputera stwierdzono, iż komputer użytkowany jest przez Wydział GUiGN i znajduje się w posiadaniu pracownika tego wydziału. Komputer oznaczony symbolem UM A36-A znajdował się w pomieszczeniu nr 35. Na komputerze nie umieszczono nr inwentarzowego. Nie stwierdzono występowania nielegalnego oprogramowania. Nie stwierdzono również, aby na dysku twardym tego komputera przechowywane były materiały (muzyka, filmy) objęte prawami autorskimi. Oprogramowanie operacyjne i użytkowe zainstalowane na badanym komputerze spełniało wymogi bezpieczeństwa.

W przypadku szóstego sprawdzanego komputera stwierdzono, iż komputer użytkowany jest przez NO i znajduje się w posiadaniu pracownika zatrudnionego na tym stanowisku. Komputer oznaczony symbolem UM A31-A znajdował się w pomieszczeniu nr 31. Na komputerze znajduje się naklejka z nr inwentarzowym. Nie stwierdzono występowania nielegalnego oprogramowania. Nie stwierdzono również, aby na dysku twardym tego komputera przechowywane były materiały (muzyka, filmy) objęte prawami autorskimi. Oprogramowanie operacyjne i użytkowe zainstalowane na badanym komputerze spełniało wymogi bezpieczeństwa. Na monitorze znajduje się inny niż na komputerze nr inwentarzowy.

W przypadku siódmego sprawdzanego komputera stwierdzono, iż komputer użytkowany jest przez Wydział Finansowy i znajduje się w posiadaniu pracownika tego wydziału. Komputer oznaczony symbolem UM A37-4 znajdował się w pomieszczeniu nr 30. Na komputerze umieszczono nr inwentarzowy. Nie stwierdzono występowania nielegalnego oprogramowania. Nie stwierdzono również, aby na dysku twardym tego komputera przechowywane były materiały (muzyka, filmy) objęte prawami autorskimi. Oprogramowanie operacyjne i użytkowe zainstalowane na badanym komputerze spełniało wymogi bezpieczeństwa. Na monitorze znajduje się naklejka z nr inwentarzowym różnym od nr komputera.

W przypadku ósmego sprawdzanego komputera stwierdzono, iż komputer użytkowany jest przez SO i znajduje się w posiadaniu pracownika tego wydziału. Komputer oznaczony symbolem UM A25-1 znajdował się w pomieszczeniu nr 25. Na komputerze znajduje się naklejka z nr inwentarzowym. Nie stwierdzono występowania nielegalnego oprogramowania. Nie stwierdzono również, aby na dysku twardym tego komputera przechowywane były materiały (muzyka, filmy) objęte prawami autorskimi. Oprogramowanie operacyjne to Windows XP – system operacyjny bez wsparcia technicznego producenta podatny na infekcje – stanowiący zagrożenie dla informacji zgromadzonych i przetwarzanych na tym komputerze oraz pozostałych jednostkach funkcjonujących w tej samej sieci intranetowej. Programy użytkowe zainstalowane na badanym komputerze spełniały wymogi bezpieczeństwa. Na monitorze znajduje się naklejka z nr inwentarzowym różnym od nr komputera.

W przypadku dziewiątego sprawdzanego komputera stwierdzono, iż komputer użytkowany jest przez KRiOŚ i znajduje się w posiadaniu pracownika tego wydziału. Komputer oznaczony symbolem UM A29-1 znajdował się w pomieszczeniu nr 29. Na komputerze znajduje się naklejka z nr inwentarzowym. Nie stwierdzono występowania nielegalnego oprogramowania. Nie stwierdzono również, aby na dysku twardym tego komputera przechowywane były materiały (muzyka, filmy) objęte prawami autorskimi. Oprogramowanie operacyjne to Windows XP – system operacyjny bez wsparcia technicznego producenta podatny na infekcje – stanowiący zagrożenie dla informacji zgromadzonych i przetwarzanych na tym komputerze oraz pozostałych jednostkach funkcjonujących w tej samej sieci intranetowej. Programy użytkowe zainstalowane na badanym komputerze spełniały wymogi bezpieczeństwa. Na monitorze znajduje się naklejka z nr inwentarzowym różnym od nr komputera.

Realizując zadanie audytowe Audytor sprawdził również czy sprzęt komputerowy (środki przetwarzania informacji) znajduje się w posiadaniu osób, które w prowadzonej ewidencji wskazane są jako osoby dysponujące tym sprzętem.

W wyniku przeprowadzonej analizy dokumentów oraz w wyniku przeprowadzonych testów stwierdzono, iż w co najmniej 12 przypadkach wskazano w ewidencji jako osobę posiadającą środki przetwarzania informacji osobę nie będącą pracownikiem Urzędu.

W co najmniej 30 przypadkach stwierdzono, iż w ewidencji w polu „osoba odpowiedzialna" nie wskazano żadnego pracownika. Nazwisko i imię pracownika dysponującego sprzętem komputerowym wskazane jest w tej ewidencji w polu „charakterystyka".

Ponadto w trakcie realizacji zadania audytowego sprawdzono, czy w ewidencji widnieją właściwe wartości środków trwałych znajdujących się w posiadaniu pracowników urzędu.

1. Zestaw komputerowy nr 2
   Monitor Belinea + zestaw komputerowy – wartość 2.982,00 zł. Data zakupu rok 2006. Oprogramowanie systemowe Windows XP. Osoba odpowiedzialna – brak. Charakterystyka – Maria Nowak. Wartość prawidłowa.
2. Zestaw komputerowy nr 6
   Monitor Belinea + zestaw komputerowy + ups – wartość 2.978,02 zł. Data zakupu rok 2007. Oprogramowanie systemowe Windows XP. Osoba odpowiedzialna – brak. Charakterystyka – Beata Kontusz-Iwańczuk. Wartość prawidłowa.
3. Zestaw komputerowy nr 7
   Monitor Belinea + drukarka + ups – wartość 2.281,92 zł. Data zakupu rok 2003, 2007 – brak jednostki centralnej – to nie jest zestaw. Osoba odpowiedzialna – brak. Charakterystyka – Elżbieta Dziubała. Wartość prawidłowa.
4. Zestaw komputerowy nr 9
   Drukarka Samsung+ Monitor Samsung+ Adobe Photoshop+ zestaw komputerowy + Corell Draw – wartość 7.533,01 zł (dodatkowo ups o wartości 498,80 i drukarka hp o wartości 1827,56 zł). Wartość zestawu wskazana w ewidencji 3.543,98 zł. Data zakupu rok 2004, 2007. Oprogramowanie systemowe Windows XP. Osoba

odpowiedzialna – brak. Charakterystyka – Marzena Kortus. Brak zgodności wartości zestawu wskazanej w ewidencji z zsumowaną wartością poszczególnych elementów zestawu.

5. Zestaw komputerowy nr 15
   Monitor Belinea + zestaw komputerowy + ups – wartość 6.032,76 zł. Data zakupu rok 2004, 2007. Oprogramowanie systemowe Windows XP Osoba odpowiedzialna – brak. Charakterystyka – Anna Gaudenzi. Wartość prawidłowa.
6. Zestaw komputerowy nr 19
   Drukarka hp+ ups+ zestaw komputerowy+ programy + monitor Belinea+ drukarka HP – wartość 9822,9 zł. Data zakupu rok 2003, 2004, 2005, 2007. Oprogramowanie systemowe Windows XP Osoba odpowiedzialna – brak. Charakterystyka – Łukasz Pilarczyk. Wartość prawidłowa.
7. Zestaw komputerowy nr 23
   Drukarka hp+ zestaw komputerowy+ programy + monitor Belinea – wartość 5.691,30zł. Data zakupu rok 2003, 2007. Oprogramowanie systemowe Windows XP Osoba odpowiedzialna – brak. Charakterystyka – Mirella Wiśniewska. Wartość prawidłowa.
8. Zestaw komputerowy nr 28
   Drukarka hp+ zestaw komputerowy + program Windows XP+ monitor Belinea – wartość 4048,30 zł. Data zakupu rok 2003, 2005, 2007. Oprogramowanie systemowe Windows XP Osoba odpowiedzialna – brak. Charakterystyka – Martyna Górna. Wartość prawidłowa.
9. Zestaw komputerowy nr 29
   Drukarka hp+ zestaw komputerowy+ + monitor Belinea + ups – wartość 3.123,3 zł. Data zakupu rok 2003, 2004, 2007. Wartość zestawu wskazana w ewidencji 2.348,50zł Oprogramowanie systemowe Windows XP Osoba odpowiedzialna – brak. Charakterystyka – Wioletta Kucz. Brak zgodności wartości zestawu wskazanej w ewidencji z zsumowaną wartością poszczególnych elementów zestawu.
10. Zestaw komputerowy nr 31
    Drukarka hp+ zestaw komputerowy+ + monitor Belinea – wartość 3.288,48 zł. Data zakupu rok 2003, 2006, 2007. Wartość zestawu wskazana w ewidencji 2710,20 zł Oprogramowanie systemowe Windows XP Osoba odpowiedzialna – brak. Charakterystyka – Adrianna Zielińska. Brak zgodności wartości zestawu wskazanej w ewidencji z zsumowaną wartością poszczególnych elementów zestawu.

*Uwagi:*
*Według informacji pozyskanych od informatyka jedynie dwa spośród opisanych wyżej zestawów (zestaw komputerowy nr 2 i zestaw komputerowy nr 31) są użytkowane przez pracowników Urzędu. Pozostałe zestawy zostały wymienione na nowe. Występują wiec rozbieżności pomiędzy informacjami zawartymi w ewidencjach księgowych jednostki a stanem faktycznym. Przyczyną tych rozbieżności jest brak Komisji Likwidacyjnej uprawnionej do likwidacji zużytych środków trwałych i wyposażenia i związany z tym brak księgowej likwidacji wyżej wskazanych środków przetwarzania informacji.*

*Wykreślenie środka trwałego z ewidencji środków trwałych może nastąpić na podstawie protokołów likwidacji środków trwałych do czyli na podstawie decyzji Komisji Likwidacyjnej.*

### 3.4 Ustalenia

Podczas realizacji zadania audytowego w obszarze zarządzania zasobami i aktywami informacyjnymi ustalono, iż w Urzędzie Miejskim w Nowym Tomyślu brak jest wydzielonej, prowadzonej przez służby informatyczne ewidencji urządzeń służących do przetwarzania informacji, zawierającej co najmniej:

- wskazanie rodzaju sprzętu służącego do przetwarzania informacji,
- dokument wskazujący na nabycie sprzętu (faktura, umowa),
- nr inwentarzowy sprzętu,
- zainstalowane oprogramowanie,
- związane z oprogramowaniem licencje,
- osobę, której oddano sprzęt do użytkowania (właściciela sprzętu).

Ewidencja taka pozwoliłaby na zgromadzenie w jednym miejscu kompletnej informacji o znajdujących się na stanie Urzędu komputerach i sprzęcie peryferyjnym, oprogramowaniu oraz pozostałych urządzeniach służących do przetwarzania informacji. To z kolei pozwoliłoby na:

- skuteczne zarządzanie zasobami informatycznymi Urzędu,
- racjonalne planowanie zakupów i wymiany sprzętu komputerowego,
- racjonalne planowanie zakupów i wymiany oprogramowania niezbędnego dla właściwego i bezpiecznego funkcjonowania Urzędu,
- ocenę ryzyk związanych z użytkowaniem tego sprzętu i podjęcie działań zapobiegających zmaterializowaniu się ryzyk krytycznych dla Urzędu,
- przypisanie odpowiedzialności za zdarzenia mające negatywny wpływ na funkcjonowanie jednostki odpowiedzialnym za ich zaistnienie użytkownikom (właścicielom) sprzętu komputerowego.

Ewidencja taka może być prowadzona w funkcjonującym w Urzędzie Miejskim w Nowym Tomyślu programie IT Manager – przy wykorzystaniu odpowiednich funkcjonalności tego oprogramowania.

Podczas realizacji zadania audytowego stwierdzono także, iż duża część sprzętu komputerowego nie posiada naklejek z nadanym im numerem inwentarzowym. Brak takich naklejek (numerów) skutkuje dużymi trudnościami w zarządzaniu i w kontroli sprzętu komputerowego oraz urządzeń peryferyjnych, utrudnia identyfikację sprzętu, utrudnia przypisanie konkretnego urządzenia do pracownika, który powinien za przypisane sobie urządzenie odpowiadać.

Uwaga: Z informacji podanych przez pracowników Urzędu wynika, iż brak naklejek na części sprawdzonego sprzętu komputerowego jest skutkiem wybranego sposobu oznaczania urządzeń przetwarzania informacji – papierowe naklejki z numerem inwentarzowym często, pod wpływem czynników zewnętrznych ulegały „odklejeniu" i zagubieniu.

Realizując zadanie audytowe, bazując na podstawie informacji przekazanych przez pracowników Urzędu, sporządzono kwestionariusz kontroli, który miał pomóc w ustaleniu czy komputery oznaczone nr identyfikacyjnymi znajdują się w pomieszczeniach wskazanych w prowadzonych ewidencjach. Na 27 sprawdzonych komputerów 9 nie znajdowało się w pomieszczeniach wskazanych jako miejsce posadowienia sprzętu komputerowego. Podobnie kształtuje się z sytuacja z urządzeniami peryferyjnymi (skanery, drukarki). Na 20 sprawdzonych urządzeń peryferyjnych 5 nie znajdowało się we wskazanym miejscu posadowienia (kwestionariusz kontroli nr 2).

Z wyjaśnień złożonych przez pracowników Urzędu wynika, iż fakt, że urządzenia służące do przetwarzania informacji (komputery i sprzęt peryferyjny) w części znajdują się w pomieszczeniach innych, niż wskazane w ewidencji wynika ze zmian organizacyjnych i personalnych jakie miały miejsce w Urzędzie oraz z niedoskonałości programu wykorzystywanego do prowadzenia ewidencji (SIGID). Mankamentem programu jest to, iż po wprowadzeniu do ewidencji środka trwałego lub wyposażenia i po wskazaniu nr pomieszczenia, w którym urządzenia te są umiejscowione, brak jest możliwości zmiany zapisu w polu z numerem pomieszczenia - w przypadku przeniesienia sprzętu komputerowego do innego pomieszczenia. Po przeniesieniu sprzętu komputerowego do innego, niż pierwotnie zaplanowane pomieszczenia jedyną możliwością wskazania nowej lokalizacji jest zamieszczenie informacji o przeniesieniu urządzeń w polu z informacjami dodatkowymi.

Uwaga: Rozbieżności pomiędzy zapisami w ewidencji środków trwałych dotyczące miejsca przechowywania środków przetwarzania informacji a stanem faktycznym wynikają z ułomnej konstrukcji technicznej programu do ewidencji środków trwałych i braku możliwości dokonania zmiany miejsca przechowywania środka trwałego czy wyposażenia po pierwszym jego wskazaniu (np. raz podany numer pokoju, w którym przechowywany jest komputer zostaje „zaszyty" w bazie danych i po fizycznym przeniesieniu komputera nie ma możliwości uwidocznienia tej zmiany w ewidencji środków trwałych).

W ramach prowadzonego zadania audytowego Audytor dokonał wybiórczej kontroli dysków twardych na komputerach znajdujących się w posiadaniu Urzędu Miejskiego w Nowym Tomyślu. W wyniku prowadzonej kontroli nie stwierdzono, aby na komputerach znajdujących się w posiadaniu pracowników jednostki znajdowały się treści chronione prawami autorskimi. Nie odnaleziono plików filmowych (*.avi, *.mp4), ani plików muzycznych (*.mp3, *.wmv) nie związanych z wykonywanymi w ramach świadczonej pracy czynnościami.

Audytor próbował również dokonać sprawdzenia legalności oprogramowania zainstalowanego na komputerach Urzędu. *(Aby stwierdzić czy oprogramowanie jest legalne należy sprawdzić, czy każdej kopii płatnej aplikacji zainstalowanej na komputerach znajdujących się w posiadaniu jednostki towarzyszy dokument poświadczający posiadanie odpowiedniej licencji. Należy posiadać faktury zakupu, ale to za mało. Komercyjne oprogramowanie firm takich jak Microsoft, Symantec (m.in. pakiety Norton) czy Adobe (Photoshop, Acrobat) jest zwykle dostarczane w pakietach zawierających oryginalny nośnik (płyta CD), etykietę z numerem seryjnym i dodatkową dokumentację (instrukcje obsługi, itd.). Zarówno oryginalny nośnik jak i etykieta z numerem seryjnym są traktowane jako dokumenty będące dowodem na legalność posiadanego oprogramowania.)* Jednak w trakcie

wykonywania czynności audytowych Audytor otrzymał informację, iż wiele faktur potwierdzających zakup sprzętu i oprogramowania jest zarchiwizowanych (w Urzędzie używany jest sprzęt zakupiony nawet 12 lat temu) oraz cześć dokumentów licencji przechowywanych jest różnych lokalizacjach i ich odnalezienie nastręczałoby wiele trudność. Ponadto licencje związane z sprzętem i oprogramowaniem zakupionym ponad 6-7 lat temu mogły zostać utracone.

Ponadto dokonując sprawdzenia oprogramowania zainstalowanego na „urzędowych" komputerach stwierdzono, iż w wielu przypadkach systemem operacyjnym jest system Windows XP. Producent tego oprogramowania (Microsoft) zaprzestał wspierania tego systemu w dniu 8 kwietnia 2014. Od 6 maja 2014 r system ten nie jest aktualizowany. Brak wsparcia producenta, brak aktualizacji i dostarczania „łatek" do systemu powoduje, iż system ten staje się potencjalnie niebezpieczny dla użytkownika. Brak wsparcia skutkuje ciągle zwiększającą się podatnością tego systemu na ataki z zewnątrz i generuje ryzyko zainfekowania używanych komputerów złośliwym oprogramowaniem, co może doprowadzić do uszkodzenia lub zniszczenia zasobów (lub ich części) informacyjnych Urzędu.

Uwaga: Z wywiadów przeprowadzonych z pracownikami Urzędu wynika, iż konieczność wymiany oprogramowania systemowego (Windows XP) na nowsze – w sposób adekwatny zabezpieczające zasoby informacyjne Gminy - była zgłaszana już w roku 2013.

Analizując, otrzymane w czasie prowadzonego audytu dokumenty Audytor dokonał sprawdzenia wartości zestawów komputerowych wskazanych w ewidencji środków trwałych. W wyniku przeprowadzonej kontroli stwierdzono, iż ogólna wartość zestawów komputerowych wskazana w ewidencji środków trwałych nie jest zgodna z zsumowaną wartością poszczególnych składników zestawu komputerowego (niezgodności wystąpiły w 3 na 10 sprawdzonych zestawów).

### 3.5 Klasyfikacja ustalenia

Ustalenia poczynione podczas realizacji zadania audytowego czyli: brak wyodrębnionej ewidencji środków przetwarzania informacji, brak numerów inwentarzowych na tych urządzeniach, przenoszenie sprzętu komputerowego i peryferyjnego bez powiadamiania pracowników odpowiedzialnych za ewidencjonowanie tego sprzętu, brak możliwości potwierdzenia legalności użytkowanego oprogramowania, niezgodności w ewidencji środków trwałych dają podstawę do klasyfikacji ustalenia, jako **uchybienia obarczonego średnim ryzykiem.** Reakcja Kierownictwa uzależniona powinna być niezwłoczna. Wskazane jest szybkie podjęcie działań naprawczych w celu doprowadzenia działalności do zgodności z polityką bezpieczeństwa informacji oraz ze standardami kontroli zarządczej.

### 3.6 Ocena systemu kontroli zarządczej

| Obiekt | Ocena | (1:5) |
|---|---|---|
| Zarządzanie środkami przetwarzania informacji | Adekwatność | 3 |
| | Skuteczność | 3 |
| | Efektywność | 3 |

## 4 Podsumowanie

### 4.1 Wskazanie słabości kontroli zarządczej oraz analiza ich przyczyn

**Słabości:**

Podstawowe słabości audytowanego obszaru to: brak wyodrębnionej ewidencji środków przetwarzania informacji, brak działającego systemu identyfikowania środków trwałych i wyposażenia, brak możliwości potwierdzenia legalności oprogramowania, brak przypisania urządzeń służących do przetwarzania informacji pracownikom, który sprzęt ten został powierzony, brak możliwości przypisania odpowiedzialności za powierzony sprzęt komputerowy i urządzenia peryferyjne.

**Przyczyny:**

Przyczyną występujących w audytowanym obszarze słabości jest brak polityki bezpieczeństwa informacji w Urzędzie i brak funkcjonującego systemu zarządzania środkami przetwarzania informacji w Urzędzie.

## 5 Skutki lub ryzyka wynikające ze wskazanych słabości kontroli zarządczej

### 5.1 Skutki wskazanych słabości kontroli zarządczej

Skutkiem istniejących, wskazanych przez Audytora wewnętrznego, słabości systemu kontroli zarządczej mogą być uchybienia polegające na nieprawidłowym zarządzaniu zasobami informatycznymi urzędu, braku możliwości potwierdzenia legalności oprogramowania, zainstalowaniu nielegalnego oprogramowania lub zainstalowaniu treści objętych ochroną praw autorskich, zainfekowaniu urzędowych systemów złośliwym oprogramowaniem i utracie zasobów informacyjnych Urzędu, niewłaściwie przeprowadzona inwentaryzacja środków przetwarzania informacji.

## 6 Zalecenia w sprawie wyeliminowania słabości kontroli zarządczej lub wprowadzenia usprawnień

1. Opracowanie systemu zarządzania urządzeniami służącymi do przetwarzania informacji.

   *W opinii Audytora system powinien zostać skonstruowany w taki sposób, aby kompletna wiedza o zasobach informatycznych Urzędu (komputerach, urządzeniach peryferyjnych, oprogramowaniu) skoncentrowana była na jednym stanowisku pracy w Urzędzie (informatyk). O wszelkich zakupach sprzętu służącego do przetwarzania informacji powinna być informowana osoba odpowiedzialna za system. Należy rozważyć rozwiązanie polegające na tym, iż nie będzie możliwości dokonania sprzętu komputerowego bez wiedzy i aprobaty osoby odpowiedzialnej za system zarządzania* środkami przetwarzania informacji. *Podobnie powinno być w przypadku zmiany miejsca użytkowania takiego sprzętu. O każdej zmianie miejsca powinna być informowana osoba odpowiedzialna za system, a zmiana mogłaby być dokonana po wydaniu przez nią zgody. Powyższe regulacje powinny dotyczyć także zakupu oprogramowania wykorzystywanego w Urzędzie.*

2. W ramach systemu zarządzania środkami przetwarzania informacji założenie wyodrębnionej ewidencji urządzeń służących do przetwarzania informacji.

   *Ewidencja taka powinna zawierać co najmniej:*
   - *wskazanie rodzaju sprzętu służącego do przetwarzania informacji,*
   - *dokument wskazujący na nabycie sprzętu (faktura, umowa),*
   - *nr inwentarzowy sprzętu,*
   - *zainstalowane oprogramowanie,*
   - *związane z oprogramowaniem licencje,*
   - *osobę, której oddano sprzęt do użytkowania (właściciela sprzętu).*

   *Do założenia takiej ewidencji można wykorzystać znajdujący się w posiadaniu Urzędu program IT Manager.*

   *W ramach opracowanego systemu zarządzania urządzeniami służącymi do przetwarzania informacji należy wskazać, iż wszelkie licencje, nośniki oprogramowania i kopie faktur związanych z zakupem tych urządzeń i oprogramowania znajdować się będą u osoby zarządzającej systemem.*

3. Oznaczenie wszystkich środków przetwarzania informacji numerami inwentarzowymi zgodnie z zasadami obowiązującymi na terenie Urzędu Miejskiego w Nowym Tomyślu.

4. Uruchomienie nowej ewidencji środków trwałych.

   *Po uruchomieniu nowej (znajdującej się w posiadaniu Urzędu Miejskiego w Nowym Tomyślu) ewidencji środków trwałych wprowadzenie do niej wszystkich niezbędnych do właściwego zarządzania sprzętem komputerowym informacji, czyli wskazanie:*

- *opisu sprzętu (charakterystyka sprzętu),*
- *jego wartości,*
- *daty przyjęcia do użytkowania,*
- *nr inwentarzowego,*
- *miejsca użytkowania,*
- *osoby odpowiedzialnej za przedmiotowe urządzenie,*
- *stopy amortyzacji.*

5. W ramach kontroli wskazanych w Polityce bezpieczeństwa informacji obowiązującej w Urzędzie (polityka do opracowania) dokonywać co najmniej raz w roku porównania informacji dotyczących sprzętu komputerowego i oprogramowania zawartych w ewidencji środków trwałych z danymi zgromadzonymi w wyodrębnionej ewidencji prowadzonej w ramach systemu zarządzania środkami służącymi do przetwarzania informacji.

6. W celu zapewnienia prawidłowego funkcjonowania systemu zarządzania bezpieczeństwem informacji, w tym m.in. w celu efektywnego zarządzania zasobami informatycznymi Urzędu i prawidłowej realizacji zadań niezbędnych do wykonania w audytowanym obszarze należy rozważyć powierzenie obowiązków związanych z bieżącym utrzymaniem sieci, systemów i oprogramowania firmie zewnętrznej – zobowiązując ją do prawidłowej realizacji wskazanych w umowie zadań w adekwatnym dla Urzędu czasie, zabezpieczyć realizację tych zadań systemem odpowiednich kar wskazanych w umowie a Informatykowi zatrudnionemu w Urzędzie powierzyć zadania związane z bezpieczeństwem informacji w Gminie wskazane w polityce bezpieczeństwa informacji obowiązującej w Nowym Tomyślu,

ewentualnie

zatrudnienie w Urzędzie Miejskim w Nowym Tomyślu dodatkowego informatyka i podział zadań związanych z utrzymaniem sieci, systemów i oprogramowania i zadań związanych z bezpieczeństwem informacji nałożonych na jednostki sektora finansów publicznych obowiązującymi przepisami prawa.

***Pouczenie:*** *Kierownik audytowanej jednostki w terminie 14 dni od dnia otrzymania sprawozdania może zgłosić na piśmie Kierownikowi jednostki, w której przeprowadzane jest zadanie zapewniające swoje stanowisko wobec przedstawionego sprawozdania.*
*Zgodnie z § 27 Rozporządzenia MF z dnia 1.02.2010 r. w sprawie przeprowadzania i dokumentowania audytu wewnętrznego Kierownik komórki audytowanej w przypadku uznania, że zalecenia zawarte w sprawozdaniu są zasadne, wyznacza osoby odpowiedzialne za ich realizację oraz ustala sposób i termin ich realizacji, powiadamiając o tym pisemnie audytora wewnętrznego oraz kierownika jednostki - w terminie 14 dni kalendarzowych od dnia otrzymania sprawozdania.*
*W przypadku odmowy realizacji zaleceń kierownik komórki audytowanej powiadamia pisemnie audytora wewnętrznego oraz kierownika jednostki o przyczynach odmowy w terminie 14 dni kalendarzowych od dnia otrzymania sprawozdania.*
*W przypadku gdy kierownik komórki audytowanej nie dokona czynności wymienionych w ust. 1 Rozporządzenia lub odmówi realizacji zaleceń, kierownik jednostki - w przypadku uznania, że zalecenia zawarte w sprawozdaniu są zasadne - wyznacza osoby odpowiedzialne za ich realizację oraz ustala termin ich realizacji, powiadamiając o tym audytora wewnętrznego.*

12.10.2015

.....

*data sporządzenia sprawozdania*

AUDYTOR WEWNĘTRZNY
CIA nr 120833, CGAP nr 1619
Tomasz Dąbrówny

.....

*podpis Audytora Wewnętrznego*

Otrzymują:

1. Pan Włodzimierz Hibner - Burmistrz Nowego Tomyśla
2. Pan Damian Wieczorek – Starszy Informatyk
3. Pani Marzena Starkowska - Inspektor