

Sprawozdanie

z
przeprowadzonego zadania audytowego
pn.

Polityka bezpieczeństwa Informacji – Legalność oprogramowania

Spis treści

1	Wprowadzenie	3
1.1	Temat zadania	3
1.2	Cele zadania zapewniającego	3
1.3	Podmiotowy zakres zadania	3
1.4	Przedmiotowy zakres zadania	3
1.5	Data rozpoczęcia zadania zapewniającego	3
2	Opinia Audytora wewnętrznego	4
3	Ustalenia stanu faktycznego wraz ze sklasyfikowanymi wynikami ich oceny według kryteriów	4
3.1	Kryterium – Legalność oprogramowania	4
3.2	Stan faktyczny	5
3.3	Ocena mechanizmów kontrolnych	9
4.	Uchybienia.....	10
5.	Zalecenia.....	10
	Pouczenie	10

1 Wprowadzenie

1.1 Temat zadania

Polityka bezpieczeństwa informacji – legalność oprogramowania

1.2 Cele zadania zapewniającego

Udzielenie odpowiedzi na pytanie czy oprogramowanie użytkowane na terenie Urzędu Miejskiego w Nowym Tomyszu jest oprogramowaniem używanym w sposób legalny.

1.3 Podmiotowy zakres zadania

Urząd Miejski w Nowym Tomyszu.

1.4 Przedmiotowy zakres zadania

Ocena legalności oprogramowania użytkowanego na terenie Urzędu Miejskiego w Nowym Tomyszu.

1.5 Data rozpoczęcia zadania zapewniającego

18.10.2017 r.

2 Opinia Audytora wewnętrznego

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

Podczas realizacji zadania audytowego ustalono, iż w badanym obszarze zidentyfikowano uchybienie polegające na wystąpieniu braku części dowodów zakupów potwierdzających legalność użytkowanych na terenie Urzędu Miejskiego w Nowym Tomyślu programów komputerowych (oprogramowania systemowego i użytkowego).

Skutkiem wyżej wskazanego uchybienia jest występowanie ryzyka braku możliwości bezspornego potwierdzenia legalności oprogramowania użytkowanego na terenie Urzędu Miejskiego w Nowym Tomyślu przy braku jednego z pozostałych atrybutów – nośników, naklejek (etykiet), kluczy licencyjnych.

Należy jednak podkreślić, iż w przyjętej do badania próbie (komputerów i oprogramowania) **nie stwierdzono występowania oprogramowania nielegalnego.**

Biorąc pod uwagę specyfikę audytowanej jednostki, organizację służb informatycznych, obowiązujące przepisy wewnętrzne, zaprojektowane i wdrożone mechanizmy kontrolne oraz zastosowane rozwiązania organizacyjne techniczne i prawne należy stwierdzić, iż prawdopodobieństwo wystąpienia ryzyk mogących w sposób istotny zagrozić prawidłowemu funkcjonowaniu audytowanego obszaru **jest niskie.**

Mając jednak na względzie wagę audytowanego obszaru działania zmierzające do wyeliminowania wskazanych przez Audytora uchybień powinny zostać podjęte w racjonalnie krótkim terminie.

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

3.1 Kryterium – Legalność oprogramowania

Wszystkie użytkowane w Urzędzie licencjonowane programy komputerowe powinien być użytkowane zgodnie z warunkami opisanymi w umowie licencyjnej.

Każdej kopii płatnej aplikacji zainstalowanej na komputerach w Urzędzie musi towarzyszyć dokument poświadczający posiadanie odpowiedniej licencji. Urząd powinien posiadać faktury zakupy, umowy licencyjne, etykiety z numerem seryjnym. 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.

W przypadku licencji OEM do kompletu dowodów potwierdzających legalność wykorzystywanego oprogramowania zalicza się dowody zakupu, umowy licencyjne, etykiety z numerem seryjnym (w przypadku licencji OEM brak jest nośników oprogramowania).

3.2 Stan faktyczny

W Urzędzie Miejskim w Nowym Tomyślu w roku 2016 wprowadzono do stosowania Politykę Bezpieczeństwa Informacji.

W załączniku nr 1 do Polityki „Procedura zarządzania infrastrukturą techniczną” wskazano, iż:

[Aktywa (zasoby)informacyjne]

„Wszystkie aktywa mające wartość dla Urzędu Miejskiego w Nowym Tomyślu w zakresie informacji są rejestrowane (ewidencjonowane) i inwentaryzowane w Urzędzie Miejskim w Nowym Tomyślu.

W Urzędzie Miejskim w Nowym Tomyślu zidentyfikowano podstawowe i wspierające rodzaje aktywów. Do podstawowych aktywów zalicza się aktywa informacyjne obejmujące: (...) licencje oprogramowania.

Katalog aktywów wspierających tworzą: sprzęt (inaczej: aktywa fizyczne), oprogramowanie, sieci, ludzie i siedziby.

W grupie aktywów „Oprogramowanie” znajdują się wszystkie programy uczestniczące w operacjach przetwarzania danych tj.: systemy operacyjne, oprogramowanie narzędziowe, pakiety oprogramowania m.in: oprogramowanie do zarządzania bazą danych, oprogramowanie do poczty elektronicznej, oprogramowanie serwera webowego, aplikacje.

[Zasady korzystania z infrastruktury technicznej]

Pracodawca powierza pracownikowi do użytkowania komputer wraz z oprogramowaniem i inne aktywa informacyjne do wykonywania zadań w ramach realizacji obowiązków służbowych. Pracodawca zastrzega, że komputer wraz z oprogramowaniem może być używany tylko do celów służbowych.

Pracownik jest odpowiedzialny za bezpieczeństwo i legalność wykorzystywanego oprogramowania (..).

Na komputerach może być zainstalowane tylko legalne oprogramowanie (...).

[Ewidencjonowanie (rejestrowanie) aktywów]

Komputery, laptopy, notebooki, netbooki, palmtopy, tablety, oprogramowanie, drukarki, monitory, urządzenia np. skanery i inne urządzenia peryferyjne są ewidencjonowane w systemie IT Manager oraz w ewidencji księgowej środków trwałych prowadzonej w wyznaczonej do tego komórce Urzędu.

Wszystkie licencje oprogramowania przechowywane są u Pełnomocnika ds. Bezpieczeństwa Informacji. Licencję nowo zakupionego oprogramowania należy przekazać do Pełnomocnika ds.

Bezpieczeństwa Informacji. Pełnomocnik ds. Bezpieczeństwa Informacji prowadzi rejestr licencji oprogramowania.

[Inwentaryzacja aktywów (zasobów) informacyjnych]

Inwentaryzacja zasobów informatycznych w Urzędzie Miejskim w Nowym Tomyszu jest realizowana przy wykorzystaniu aplikacji IT Manager. Za pomocą tej aplikacji w czasie rzeczywistym (online) zbierane są m.in. informacje na temat cech identyfikacyjnych komputera, logowań i pracujących na nim użytkowników, sieci w której działa komputer, dane na temat konfiguracji technicznej, tj. sprzętu (urządzeń) składowych, alertów wykorzystania pamięci, oprogramowanie, które jest na komputerze zainstalowane, licencji oraz aktualizacji oprogramowania.

Inwentaryzację oprogramowania przeprowadza się również w oparciu o przepisy ustawy o rachunkowości.

W załączniku nr 6 do Polityki Bezpieczeństwa Informacji wskazano, iż:

[Kontrola legalności oprogramowania]

Do kontroli legalności oprogramowania wprowadza się system IT Manager. Na każdym komputerze musi być zainstalowany agent, nadzorujący pracę komputera. Zakazuje się użytkownikom odinstalowania agenta.

Co najmniej raz w roku Pełnomocnik ds. Bezpieczeństwa Informacji przeprowadza kontrolę legalności oprogramowania. Z systemu IT Manager wykonuje się raport zainstalowanego oprogramowania i sprawdza czy ilość posiadanych licencji odpowiada ilości licencji zainstalowanych. Raport przedkłada Burmistrzowi Nowego Tomysza.

Podczas realizacji zadania audytowego Audytor wewnętrzny, przy pomocy informatyków zatrudnionych w Urzędzie sprawdził działanie zakupionego na potrzeby kontroli i inwentaryzacji program IT Manager.

Wg informacji wyselekcjonowanych z programu IT Manager, na potrzeby Urzędu Miejskiego zakupiono m.in. następujące licencjonowane oprogramowanie:

LP	Oprogramowanie	Ilość licencji
1	Windows 10 Pro	85
2	Windows 10 Home	1
3	IT Manager Agent	100
4	IT Manager Console	1
5	ID Protect Client	2
6	Microsoft Office 2013 dla Użytkowników Domowych i Małych Firm	11
7	Microsoft Office 2016 dla Użytkowników Domowych i Małych Firm	17

Ponadto wykorzystując program IT Manager dokonano sprawdzenia (inwentaryzacji) aplikacji i programów zainstalowanych na poszczególnych komputerach użytkowanych w Urzędzie Miejskim w Nowym Tomyszu.

Przeprowadzona próba dała następujące wyniki:

LP	Oprogramowanie	Ilość licencji	Uwagi
1	IT Manager Agent	84	Liczba dostępnych licencji 100
2	IT Manager Console	1	Liczba dostępnych licencji 1
3	Embassy Security Center	1	Liczba dostępnych licencji 1
4	Private Information Manager	1	Liczba dostępnych licencji 1
5	ID Protect Client	2	Liczba dostępnych licencji 2
6	Microsoft Office 2013 dla Użytkowników Domowych i Małych Firm	10	Liczba dostępnych licencji 11
7	Microsoft Office 2016 dla Użytkowników Domowych i Małych Firm	16	Liczba dostępnych licencji 17
8	e-PFRON Offline 1.7.0	1	Brak informacji w wykazie licencji

Program IT Manager podczas przeprowadzonej inwentaryzacji oprogramowania zidentyfikował program e-PFRON Offline 1.7.0 nie wskazane w wykazie zakupionego licencjonowanego oprogramowania.

Po przedstawieniu „Wstępnych ustaleń” z prowadzonego audytu służby informatyczne Urzędu złożyły następujące wyjaśnienia:

„Jest to stara wersja obecnie użytkowanej aplikacji internetowej e-PFRON2. Po konsultacji telefonicznej z działem technicznym Państwowego Funduszu Rehabilitacji Osób Niepełnosprawnych uzyskałem informację iż e - PFRON OffLine 1.7.0 było aplikacją całkowicie darmową. Program IT Manager dysponuje błędnie wprowadzoną bazą sygnatur. Właściciel oprogramowania, firma INFONET, został poinformowany o zaistniałym błędzie”.

Ponadto podczas realizacji zadania audytowego porównano informacje zawarte w programie IT Manager dotyczące oprogramowania zainstalowanego na poszczególnych komputerach użytkowanych w Urzędzie Miejskim w Nowym Tomyszu z informacjami pozyskanymi przez Audytora podczas przeprowadzanego fizycznego przeglądu oprogramowania zainstalowanego na wybranych w losowaniu komputerach.

Do przeglądu wylosowano 11 komputerów.

Porównanie danych zawartych w programie IT Manager oraz informacji z przeprowadzonego przeglądu wykazało, iż program IT Manager wykazuje oprócz aktualnie zainstalowanego oprogramowania programy zainstalowane i odinstalowane przed datą przeprowadzenia inwentaryzacji co może prowadzić do chaosu informacyjnego i wykazywania wycofanych z użytku programów komputerowych.

W związku z powyższym należy rozważyć taką zmianę ustawień systemowych programu IT Manager, aby do inwentaryzacji wyselekcjonowywał wyłącznie programy faktycznie zainstalowane na poszczególnych komputerach w dacie prowadzonego przeglądu.

Podczas prowadzonego przeglądu Audytor wewnętrzny podjął również zakończone niepowodzeniem próby zainstalowania oprogramowania pobranego z sieci Internet. Brak powodzenia takiej instalacji świadczy o dobrym zabezpieczeniu sprzętu komputerowego użytkowanego w Urzędzie Miejskim (instalacja oprogramowania dokonywana jest wyłącznie przez administratorów systemów).

W trakcie prowadzonego przeglądu nie stwierdzono, aby na kontrolowanych komputerach zainstalowano oprogramowanie (sprawdzono wylosowane do audytu oprogramowanie systemowe i użytkowe), na użytkowanie którego Urząd Miejski w Nowym Tomyślu nie posiadał „licencji”.

W trakcie prowadzonego przeglądu nie stwierdzono, aby na dyskach twardych audytowanych komputerów znajdowały się treści (pliki filmowe, muzyczne lub inne), których użytkowanie mogłoby naruszać prawa autorskie lub pokrewne.

Prowadząc przegląd oprogramowania Audytor wewnętrzny dokonał także kontroli fizycznych atrybutów poświadczających legalność oprogramowania – na poddanych badaniu komputerach zostały naklejone etykiety potwierdzające legalność oprogramowania użytkowanego programu.

W celu potwierdzenia legalności oprogramowania użytkowanego w Urzędzie Miejskim w Nowym Tomyślu Audytor wewnętrzny dokonał także sprawdzenia umów i faktur stanowiących kolejne atrybuty poświadczające legalność użytkowanego oprogramowania.

Realizując zadanie audytowe Audytor wewnętrzny dokonał sprawdzenia faktur potwierdzających zakup losowo wybranych programów komputerowych.

Lp	Faktura	Program	Ilość licencji
1	F/158/03/17	Office 2016 (dla firm)	17
2	F/001505/16	Windows 10	15
3	F/002358/16	Windows 10	23
4	FA VAT 219/2006	AVG AntiVirus	75
5	FA VAT 0058/09/2017/MG	Rejestr zaangażowania środków budżetowych	1
6	FA VAT 0004/07/2016/MG	Planowanie i realizacja budżetu JST	13
7	F/002232/15	Office 2013	5
8	F/000614/15	Office 2013	4
9	F/000591/17	Windows 10	1
10	F/001013/17	Windows 10	2

Zgodnie z informacjami przekazanymi przez służby informatyczne Urząd Miejski znajduje się w posiadaniu 86 licencji systemu operacyjnego Windows 10 (system operacyjny zakupiono lub pozyskano z uwagi na wcześniejsze użytkowanie systemów Windows 7, 8 i in.). Przedstawione do audytu faktury dokumentują zakup 41 licencji systemu operacyjnego Windows 10.

Brak jest udokumentowania fakturami lub innymi dokumentami faktu zakupu 45 licencji.

Urząd Miejski w Nowym Tomyślu znajduje się w posiadaniu 11 licencji pakietu Office 2013 i 17 licencji pakietu Office 2016 tymczasem fakturami zakupu udokumentowano zakup 17 licencji pakietu Office 2016 i 9 licencji pakietu Microsoft Office 2013. Brak jest faktur potwierdzających zakup 2 licencji pakietu Office 2013.

Urząd Miejski w Nowym Tomyślu zakupił licencję na 75 stanowisk komputerowych programu AVG AntiVirus z uwagi na to, że IT Manager nie inwentaryzuje tego programu brak jest możliwości zdalnego ustalenia na ilu stanowiskach komputerowych użytkowany jest program antywirusowy.

Urząd Miejski w Nowym Tomyślu zakupił licencję na 1 stanowisko komputerowe programu „Rejestr zaangażowania środków budżetowych”, z uwagi na to, że IT Manager nie inwentaryzuje tego programu brak jest możliwości zdalnego ustalenia na ilu stanowiskach komputerowych użytkowany jest przedmiotowy program.

Urząd Miejski w Nowym Tomyślu zakupił licencję na 13 stanowisko komputerowe programu „Planowanie i realizacja budżetu JST”, z uwagi na to, że IT Manager nie inwentaryzuje tego programu brak jest możliwości zdalnego ustalenia na ilu stanowiskach komputerowych użytkowany jest przedmiotowy program.

W związku z faktem braku inwentaryzacji wskazanych wyżej programów komputerowych należy podjąć działania mające na celu taką konfigurację programu systemu IT Manager, aby ewidencjonował wszystkie zakupione i zainstalowane na komputerach wykorzystywanych w Urzędzie Miejskim w Nowym Tomyślu programy komputerowe.

3.3 Ocena mechanizmów kontrolnych

W celu zapewnienia, iż użytkowane na terenie Urzędu oprogramowanie komputerowe jest oprogramowaniem legalnym w Urzędzie Miejskim w Nowym Tomyślu zaprojektowano i wdrożono cztery mechanizmy kontrolne:

1. Polityka bezpieczeństwa informacji.
2. Dokumentacja potwierdzająca legalność oprogramowania.
3. Inwentaryzacja licencji i oprogramowania.
4. Przeglądy

Biorąc pod uwagę wyniki przeprowadzonego zadania audytowego Audytor wewnętrzny stwierdził, iż zaprojektowane dla danego obszaru mechanizmy kontrolne są wystarczające dla zapewnienia prawidłowości jego funkcjonowania. Jednak w celu wyeliminowania ryzyka związanego z brakiem możliwości potwierdzenia legalności zakupionego oprogramowania należy zmodyfikować mechanizm kontrolny „dokumentacja potwierdzająca legalność oprogramowania” w taki sposób, aby atrybuty potwierdzające legalność oprogramowania – nośniki, klucze programowe, faktury – po zakupie gromadzone i przechowywane były przez służby Informatyczne Urzędu Miejskiego w Nowym Tomyślu. Faktury zakupu będące dowodami księgowymi powinny być przechowywane przez informatyków w formie kopii papierowej lub skanu dokumentu (forma elektroniczna).

Należy także dokonać zmian ustawień (aktualizacji, modyfikacji) programu IT Manager w taki sposób, aby podczas przeglądów czy inwentaryzacji program ten pobierał informacje o wszystkich zainstalowanych na użytkowanych w Urzędzie Miejskim w Nowym Tomyślu programach informatycznych.

4. Uchybienia

Brak części dowodów zakupów potwierdzających legalność użytkowanych na terenie Urzędu Miejskiego w Nowym Tomyślu programów komputerowych.

Skutkiem wyżej wskazanego uchybienia jest występowanie ryzyka braku możliwości bezspornego potwierdzenia legalności oprogramowania użytkowanego na terenie Urzędu Miejskiego w Nowym Tomyślu przy braku jednego z pozostałych atrybutów – nośników, naklejek (etykiet), kluczy licencyjnych.

5. Zalecenia

Służby informatyczne Urzędu (Pełnomocnik ds. Bezpieczeństwa Informacji) powinny przechowywać dowody potwierdzające legalność wykorzystywanego oprogramowania (dowody zakupów - faktur, umowy licencyjne, etykiety z numerem seryjnym, nośniki oprogramowania – gdy zostały dołączone przez producenta).

W dacie zakupu faktury potwierdzające nabycie licencji mogą być kopiowane lub skanowane i przechowywane w formie papierowej i/lub elektronicznej przez służby informatyczne w sposób przyjęty (opisany w PBI). Pozostałe atrybuty potwierdzające legalność oprogramowania (umowy licencyjne, klucze licencyjne, nośniki programów) również powinny być przechowywane przez służby informatyczne urzędu w sposób przyjęty (opisany w PBI).

Pouczenie

Kierownik komórki audytu wewnętrznego przekazuje sprawozdanie audytowanemu i kierownikowi jednostki. Audytowany, w terminie 14 dni kalendarzowych od dnia otrzymania sprawozdania, ustala sposób i termin realizacji zaleceń oraz wyznacza osoby odpowiedzialne za realizację zaleceń, powiadamiając o tym na piśmie kierownika komórki audytu wewnętrznego i kierownika jednostki. W przypadku odmowy realizacji zaleceń audytowany przedstawia, w terminie 7 dni kalendarzowych od dnia otrzymania sprawozdania, pisemne stanowisko kierownikowi jednostki i audytorowi wewnętrznemu. W przypadku, o którym mowa w ust. 3, kierownik jednostki podejmuje decyzję dotyczącą realizacji zaleceń, informując o tym audytowanego i kierownika komórki audytu wewnętrznego.

02.12.2017 r.

.....
data sporządzenia wstępnych ustaleń
CIA nr 120833, CGAP nr 1619

Tomasz Dąbrówny
Tomasz Dąbrówny

.....
podpis Audytora Wewnętrznego