Zarządzenie nr 113.

Prezydenta Miasta Torunia

z dnia 10.05.2023r.

w sprawie wprowadzenia Polityki Zarządzania Oprogramowaniem w Urzędzie Miasta Torunia

Na podstawie art. 33 ust. 1 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz.U. z 2023 r. poz. 40 ze zm. poz. 572) § 18 pkt 8 Regulaminu Organizacyjnego Urzędu Miasta Torunia, stanowiącego załącznik nr 1 do zarządzenia nr 378 Prezydenta Miasta Torunia z dnia 30 października 2013 r. w sprawie nadania Regulaminu Organizacyjnego Urzędowi Miasta Torunia[1] zarządza się, co następuje:

§ 1. Wprowadza się Politykę Zarządzania Oprogramowaniem w Urzędzie Miasta Torunia

§ 2. Zobowiązuje się dyrektorów działów, pracowników im podległych oraz pracowników na stanowiskach samodzielnych do zapoznania się z treścią dokumentu, o którym mowa w § 1 oraz stosowania zasad określonych niniejszym dokumentem.

§ 3. Wykonanie Zarządzenia powierza się Sekretarzowi Miasta Torunia.

§ 4. Zarządzenie wchodzi w życie z dniem podpisania.

Prezydent Miasta Torunia

Michał Zaleski

[1]Zmiany wymienionego zarządzenia wprowadzono zarządzeniami Prezydenta Miasta Torunia nr 312, nr 380 z 2014 r., nr 149, nr 273, nr 391 z 2015 r., nr 379 z 2016 r., nr 40, nr 130, nr 254, nr 319, nr 353 z 2017 r., nr 293 z 2018 r., nr 124, nr 337 z 2019 r., nr 202, nr 222, nr 230 i nr 253 z 2020 r., nr 222 i nr 290 z 2021 r., nr 7, 39, 62, 180 i 220 z 2022 r.

INSPEKTOR
Paweł Górzyński

DYREKTOR
Biura Projektów Informatycznych
Mariusz Szefera

RADCA PRAWNY
Rafał Rojek
Tr-1035

Załącznik nr 1 do Zarządzenia PMT nr 113 z dnia 10.05.2023r.

Polityka Zarządzania Oprogramowaniem w Urzędzie Miasta Torunia

Cel dokumentu: sformalizowanie zasad zarządzania licencjami na oprogramowanie użytkowane w Urzędzie Miasta Torunia.

Definicje

1. Oprogramowanie – program komputerowy lub aplikacja w ramach prawa własności intelektualnej chroniony na podstawie prawa autorskiego lub patentowego,
2. UMT – Urząd Miasta Torunia,
3. Zespół Wsparcia Technicznego - pracownicy firm zewnętrznych odpowiedzialni za obsługę informatyczną w UMT,
4. Urządzenie mobilne – telefon komórkowy, smartfon lub tablet,
5. Inventory tool – system informatyczny służący do ewidencji i weryfikacji zainstalowanego oprogramowania,
6. Metryka komputera – protokół stanowiący zestawienie oprogramowania zainstalowanego na komputerze wygenerowane z inventory tool,
7. BPI – Biuro Projektów Informatycznych,
8. BOU – Biuro Obsługi Urzędu.

§ 1.

Zakup oprogramowania przez BPI:

1. Dyrektor działu UMT występuje w formie pisemnej wraz z uzasadnieniem do dyrektora BPI z zapotrzebowaniem na zakup oprogramowania koniecznego do wykonywania obowiązków służbowych.
2. Na podstawie złożonego wniosku BPI przeprowadza przy użyciu narzędzia inventory tool analizę stanu posiadania i efektywności wykorzystania licencji oprogramowania wnioskowanego do zakupu.
3. Dyrektor BPI podejmuje decyzję o zakupie lub odmowie zakupu wnioskowanego oprogramowania i informuje o niej dyrektora działu UMT wnioskującego o zakup oprogramowania.
4. Dyrektor BPI wszczyna procedurę zakupu oprogramowania.
5. Pracownik BPI:
   a) w razie potrzeby występuje do dyrektora działu UMT składającego wniosek o zakup oprogramowania o uszczegółowienie wymagań funkcjonalnych dotyczących oprogramowania wnioskowanego do zakupu,
   b) spisuje w formie notatki służbowej wymagania dotyczące bezpieczeństwa oprogramowania i ustala warunki oceny wiarygodności potencjalnego dostawcy.
6. Po dokonaniu zakupu następuje ewidencja oprogramowania zgodnie z §3 oraz instalacja zgodnie z §4.

§ 2.

Zakup oprogramowania przez inne działy UMT

1. Dyrektor działu UMT występuje w formie pisemnej do dyrektora BPI o zaopiniowanie planowanego zakupu oprogramowania. Wniosek musi zawierać opis wymagań funkcjonalnych i warunki oceny wiarygodności potencjalnego dostawcy tego oprogramowania.
2. Dyrektor BPI:
   a) przekazuje dyrektorowi działu UMT odpowiedzialnemu za zakup oprogramowania wymagania dodatkowe dotyczące zakupu oprogramowania,
   b) informuje dyrektora działu UMT odpowiedzialnemu za zakup oprogramowania o konieczności dostarczenia wymaganych informacji niezbędnych do wprowadzenia oprogramowania do ewidencji,
   c) przekazuje wymagania dotyczące bezpieczeństwa oprogramowania.
3. Po przeprowadzonym zakupie dyrektor działu UMT odpowiedzialnego za zakup oprogramowania przekazuje informacje niezbędne do wprowadzenia oprogramowania do ewidencji do BPI.
4. Po dokonaniu zakupu następuje ewidencja oprogramowania zgodnie z §3 oraz instalacja zgodnie z §4.

§ 3.

Ewidencja oprogramowania oraz zasady przechowywanie dokumentacji i wersji instalacyjnych

1. Ewidencję oprogramowania użytkowanego w UMT na komputerach stacjonarnych, przenośnych i serwerach prowadzi BPI w systemie inventory tool.
2. Papierowe wersje dokumentów licencyjnych oraz nośniki instalacyjne oprogramowania pozyskane w procesie zakupu, świadczące o legalności zakupionego oprogramowania, przechowywane są w sposób bezpieczny w zamkniętej szafie przez BPI do czasu wycofania oprogramowania z eksploatacji i przeprowadzenia likwidacji niematerialnego środka trwałego.
3. BPI sporządza coroczny raport:
   a) stanu ilościowego użytkowanego w UMT oprogramowania nie później niż do końca stycznia roku następnego,
   b) stanu efektywności użytkowanego w UMT oprogramowania dla kilku losowo wybranych stacji roboczych nie później niż do końca stycznia roku następnego.
4. Ewidencję oprogramowania użytkowanego w UMT na urządzeniach mobilnych prowadzi BOU w systemie inventory tool.
5. BOU sporządza coroczny raport stanu ilościowego użytkowanego w UMT oprogramowania nie później niż do końca stycznia roku następnego.
6. Raporty, o których mowa w ust.3 i ust.5 przekazywane są wraz z wnioskami do Sekretarza Miasta Torunia najpóźniej do końca stycznia roku, w którym zostały sporządzone.

7. BPI oraz BOU będą weryfikować z częstotliwością roczną, nie później niż do końca stycznia roku następnego, czy warunki licencyjne oprogramowania bezpłatnego dopuszczonego do użytku komercyjnego nie uległy zmianie.
8. BPI przeprowadza coroczny przegląd nieużytkowanego oprogramowania pod kątem możliwości jego dalszego wykorzystania w UMT i na tej podstawie wnioskuje o przeprowadzenie likwidacji składników majątkowych zgodnie z przyjętymi Zarządzeniami w tym zakresie.
9. Na podstawie protokołu z likwidacji składników majątkowych pracownik BPI usuwa zlikwidowane oprogramowanie z ewidencji oprogramowania.

§ 4.

Instalacja oprogramowania

1. Instalację oprogramowania na komputerze stanowiącym własność UMT może przeprowadzić wyłącznie pracownik BPI lub Zespołu Wsparcia Technicznego.
2. Przed zainstalowaniem oprogramowania osoba odpowiedzialna za instalację musi przeprowadzić analizę ilości posiadanych licencji oraz zapoznać się z warunkami licencji.
3. Po każdorazowej instalacji na komputerze oprogramowania pracownik BPI zobowiązany jest do sporządzenia aktualnej metryki komputera, przekazania jej do podpisu użytkownikowi tego komputera, a następnie jej archiwizacji.

§ 5.

Zasady użytkowania oprogramowania

1. Pracownicy mogą korzystać z komputerów służbowych i oprogramowania dostarczonego przez UMT wyłącznie w celu wykonywania obowiązków służbowych oraz podnoszenia kwalifikacji na zajmowanym stanowisku.
2. Nie jest dopuszczalne wykorzystywanie oprogramowania dostarczonego przez UMT do celów prywatnych, w szczególności do tworzenia, edycji, przechowywania lub rozpowszechniania materiałów niezwiązanych z wykonywaną pracą.
3. Każdy z pracowników użytkujących przypisany sobie imiennie komputer zobowiązany jest do podpisania metryki komputera.
4. W przypadku komputerów, do których nie jest przypisany na stałe jeden konkretny użytkownik, lecz np. zespół użytkujących go naprzemiennie osób, osobą odpowiedzialną za dany komputer jest dyrektor działu, w którym zlokalizowany jest komputer, lub osoba przez niego wyznaczona.
5. Pracownicy nie mogą przechowywać na służbowych lub prywatnych przenośnych nośnikach danych (pendrive, płyty CD/DVD, karty pamięci, dyski przenośne, telefony itp) podłączanych do komputerów służbowych, prywatnych kopii oprogramowania zarówno w wersjach instalacyjnych, jak i wersjach „portable", których uruchamianie nie wymaga instalacji.
6. Pracownicy UMT nie mogą pobierać z Internetu za pomocą komputerów służbowych, przechowywać na dyskach twardych tych komputerów, bądź na służbowych lub

prywatnych przenośnych nośnikach danych (pendrive, płyty CD/DVD, karty pamięci, dyski przenośne, telefony itp.) podłączanych do komputerów służbowych oraz przesyłać za pomocą poczty elektronicznej, nielicencjonowanego oprogramowania i innych utworów w rozumieniu ustawy o prawie autorskim i prawach pokrewnych (tekst jednolity Dz. U. 2022, poz. 2509) chronionych prawem autorskim (w tym w szczególności utworów muzycznych, filmów, grafiki, gier komputerowych i tym podobnych).

§ 6.

Praca zdalna

1. Pracownik pozyskując komputer przeznaczony do użytku poza miejscem pracy, w przypadku potrzeby skonfigurowania dostępu do wybranych systemów zlokalizowanych w sieci UMT zobowiązany jest do zgłoszenia tego zamiaru do BPI w celu określenia możliwości technicznych zapewnienia dostępu do tych systemów, wygenerowania licencji VPN oraz instalacji aplikacji służącej do dostępu zdalnego do sieci UMT.
2. Każdy komputer przekazywany do pracy zdalnej BPI zabezpiecza mechanizmem szyfrowania dysków oraz zastosowaniem silnych haseł dostępu, zgodnych z przyjętą polityką przetwarzania danych.
3. Przekazanie sprzętu następuje w formie protokołu zawierającego numer inwentarzowy przekazanego komputera oraz zestawienie zainstalowanego w nim oprogramowania.

§ 7.

Zasady użytkowania prywatnego komputera do celów służbowych

1. Dopuszcza się możliwość użytkowania komputera prywatnego do celów służbowych.
2. Pracownik chcący użytkować komputer prywatny do celów służbowych, w tym do uzyskania za jego pomocą zdalnego dostępu do wybranych systemów zlokalizowanych w sieci UMT, zobowiązany jest do zgłoszenia tego zamiaru do BPI w celu określenia możliwości technicznych zapewnienia dostępu do tych systemów, wygenerowania licencji VPN oraz instalacji aplikacji służącej do dostępu zdalnego do sieci UMT.
3. Pracownik chcący użytkować komputer prywatny do celów służbowych jest zobowiązany:
   a) utworzyć na tym komputerze osobny profil zabezpieczony hasłem uniemożliwiający dostęp do przechowywanych tam danych osobom postronnym, a po zakończeniu użytkowaniu profil ten usunąć,
   b) zainstalować na tym komputerze program antywirusowy charakteryzujący się regularną aktualizacją baz sygnatur wirusów oraz monitorować jego działanie, w szczególności skuteczność regularnej aktualizacji baz sygnatur wirusów,
   c) posiadać na tym komputerze aktualne wsparcie producenta systemu operacyjnego oraz bieżące aktualizacje systemu operacyjnego.

4. Na komputerze prywatnym użytkowanym do celów służbowych nie jest możliwa instalacja oprogramowania komercyjnego na licencji stanowiącej własność UMT (np. pakietu Microsoft Office).
5. Pracownik BPI zweryfikuje spełnienie warunków uzyskania zdalnego dostępu do sieci UMT.

§ 8.

Zasady użytkowania służbowych urządzeń mobilnych

1. Przekazanie pracownikowi służbowego urządzenia mobilnego następuje na podstawie protokołu zawierającego w szczególności zasady opisane w niniejszym paragrafie.
2. Pracownik korzystający ze służbowego urządzenia mobilnego jest zobowiązany do:
   a) należytej dbałości o przekazane mu w użytkowanie urządzenie,
   b) podjęcia wszelkich starań w celu zabezpieczenia urządzenia przed jego kradzieżą lub zagubieniem,
   c) korzystania z urządzenia nie naruszając przy tym przepisów obowiązującego prawa, w tym nieprzechowywania w pamięci urządzenia lub na karcie pamięci w służbowym urządzeniu mobilnym plików muzycznych, graficznych, video z nielegalnych źródeł oraz naruszających prawa autorskie.
3. Zabrania się:
   a) udostępniania urządzenia innym osobom,
   b) instalowania w jego pamięci aplikacji bez uzgodnienia z BOU,
   c) dokonywania samodzielnych napraw i modernizacji urządzenia,
   d) rekonfiguracji oprogramowania systemowego mającej wpływ na bezpieczeństwo systemu.
4. Pracownik ponosi odpowiedzialność za przekazane mu do użytkowania urządzenie mobilne na zasadach odpowiedzialności za mienie powierzone. Fakt utraty, uszkodzenia lub zniszczenia urządzenia należy niezwłocznie zgłosić bezpośredniemu przełożonemu.
5. W przypadku utraty urządzenia pracownik jest zobowiązany do zmiany wszelkich haseł dostępowych.

§ 9.

Kontrola oprogramowania

1. BPI prowadzi przeglądy losowo wybranych służbowych komputerów stacjonarnych, przenośnych i serwerów pod kątem zainstalowanego lub przechowywanego na nich oprogramowania oraz występowania dokumentów lub utworów mogących naruszać prawo autorskie.
2. BOU prowadzi przeglądy losowo wybranych służbowych telefonów pod kątem zainstalowanego lub przechowywanego na nich oprogramowania oraz występowania dokumentów lub utworów mogących naruszać prawo autorskie.
3. Z przeprowadzonych kontroli należy sporządzić protokół zawierający opis rezultatów kontroli, który zostanie przedstawiony Sekretarzowi Miasta Torunia.

INSPEKTOR
Paweł Górzyński

DYREKTOR
Biura Projektów Informatycznych
Mariusz Szefera