Załącznik do Zarządzenia Nr 120/32/18
Prezydenta Miasta Tychy
z dnia 24 maja 2018 r.

POLITYKA BEZPIECZEŃSTWA INFORMACJI

§ 1
Wstęp

Polityka Bezpieczeństwa Informacji Urzędu Miasta Tychy została opracowana w celu spełnienia wymagań określonych w § 20 ust. 1 i 2 rozporządzenia Rady Ministrów z 12 kwietnia 2012 roku 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) oraz przepisach o ochronie danych osobowych.

§ 2
Postanowienia ogólne

1. Polityka Bezpieczeństwa Informacji powstała w związku z wykorzystywaniem:
   1) danych osobowych w rozumieniu ustawy o ochronie danych osobowych;
   2) innych, niż dane osobowe, danych (informacji) podlegających ochronie;
   3) technologii informatycznych stosowanych w Urzędzie.
2. Polityka Bezpieczeństwa Informacji jest zestawem powiązanych ze sobą dokumentów określających zasady i sposób zarządzania bezpieczeństwem aktywów informacyjnych i zasobów materialnych Urzędu. Zarządzanie to służy ochronie oraz udostępnianiu aktywów w taki sposób, aby utrzymać poufność, dostępność oraz integralność przetwarzanych informacji na odpowiednim poziomie.
3. Niniejszą Polityką Bezpieczeństwa nie jest objęta ochrona informacji niejawnych w rozumieniu ustawy o ochronie informacji niejawnych, których ochrona odbywa się na odrębnych zasadach.
4. Ochronie podlegają Zasoby Urzędu.
5. Każdy pracownik Urzędu przyjmuje na siebie obowiązek ochrony Zasobów Urzędu w zakresie uzyskanych uprawnień. Obowiązek ochrony Zasobów nie kończy się z chwilą ustania stosunku pracy lub innego stosunku prawnego stanowiącego podstawę wykonywania pracy na rzecz Urzędu w takim zakresie, jaki ustanawiają przepisy prawa. Obowiązek ochrony Zasobów w przypadku współpracy z podmiotami zewnętrznymi określany jest w ramach zawartych z nimi umów.

§ 3
Podstawowe definicje

Przez użyte w niniejszym dokumencie określenia rozumie się:

1) **dostępność –** zasób informacji jest możliwy do wykorzystania na żądanie, w założonym czasie, przez podmiot uprawniony;
2) **incydent** – pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia właściwej realizacji zadań Urzędu i zagrażają bezpieczeństwu informacji;
3) **informacja** – czynnik, któremu można przypisać określone znaczenie, aby móc go wykorzystywać do różnych celów;
4) **integralność –** informacje w formie papierowej nie zostały zmienione lub zniszczone w sposób nieautoryzowany lub zasób systemu teleinformatycznego realizuje swoją zamierzoną funkcję w sposób, wolny od nieautoryzowanej manipulacji, celowej lub przypadkowej**;**
5) **poufność –**informacje nie są udostępniane lub ujawniane nieupoważnionym osobom lub podmiotom;
6) **Urząd** – Urząd Miasta Tychy;
7) **zasób (aktywa)** – wszystko, co ma wartość dla Urzędu, w szczególności personel, budynki i budowle, sprzęt, oprogramowanie, informacja, prawa niematerialne, wizerunek.

§ 4
Deklaracja

Prezydent Miasta Tychy zobowiązuje się do podejmowania niezbędnych działań mających na celu zabezpieczenie informacji, jako zasobu podlegającego ochronie prawnej i niezbędnego do prawidłowego oraz sprawnego funkcjonowania Urzędu.

§ 5

Cel polityki bezpieczeństwa informacji

Celem Polityki jest w szczególności:

1) zapewnienie standardów bezpieczeństwa informacji w oparciu o obowiązujące przepisy prawa;
2) określenie ról i zakresów odpowiedzialności związanych z bezpieczeństwem i ochroną informacji;
3) minimalizowanie ryzyka w obszarze bezpieczeństwa fizycznego, teleinformatycznego, organizacyjno – prawnego oraz osobowego;
4) ochrona informacji przed nieautoryzowanym dostępem, zmianą, utratą, uszkodzeniem, zniszczeniem lub zatajeniem;
5) stałe podnoszenie umiejętności i kwalifikacji pracowników Urzędu w dziedzinie bezpieczeństwa informacji;
6) zaangażowanie wszystkich pracowników w ochronę informacji;
7) wspieranie Kierownictwa Urzędu w zakresie utrzymania odpowiedniego poziomu bezpieczeństwa informacji poprzez zarządzanie ryzykiem, zarządzanie zmianami, zarządzanie ciągłością pracy Urzędu;
8) ochrona wizerunku Urzędu i Miasta Tychy;
9) stworzenie podstaw dla Systemu Zarządzania Bezpieczeństwem Informacji.

§ 6

Zakres obowiązywania polityki bezpieczeństwa informacji

Polityka Bezpieczeństwa Informacji:

1) jest zbiorem zasad, które obowiązane są stosować osoby posiadające dostęp do zasobów informacyjnych;
2) określa zasady ochrony zasobów;
3) dotyczy wszystkich pracowników Urzędu, a także innych osób mających dostęp do informacji chronionych (np. pracowników firm zewnętrznych realizujących prace);
4) ma zastosowanie do wszystkich informacji chronionych niezależnie od formy, w jakiej są przechowywane (papierowej, elektronicznej i innej).

§ 7

Struktura dokumentacji Polityki Bezpieczeństwa Informacji

W skład Polityki wchodzą:

1) zasady zarządzania bezpieczeństwem danych, w tym danych osobowych;
2) procedury, instrukcje, regulaminy oraz inne dokumenty, które regulują szczegółowe zasady korzystania z zasobów informacyjnych Urzędu, a także użytkowania systemów informatycznych.

§ 8

Podstawowe zasady bezpieczeństwa informacji

Do podstawowych zasad bezpieczeństwa informacji należą następujące zasady:

1) **chronienia pomieszczeń** – pod nieobecność osoby uprawnionej w pomieszczeniach (poza ogólnodostępnymi typu korytarze) nie mogą przebywać osoby postronne, po opuszczeniu pomieszczenia osoba odpowiedzialna zamyka je na klucz (bez pozostawiania kluczy w zamkach – wyjątek stanowi ewakuacja), w przypadku zamków z kontrolą dostępu ważna jest dbałość o prawidłowe domknięcie (zatrzaśnięcie) drzwi;
2) **czystego biurka** – zarówno dokumentów papierowych, jak i jakichkolwiek innych nośników informacji (płyt CD, DVD, pamięci flash, oraz innych typów pamięci przenośnych), nie pozostawia się bez nadzoru;
3) **czystej drukarki** – wszyscy pracownicy, praktykanci i stażyści zobowiązani są do zabierania dokumentów z drukarek zaraz po ich wydrukowaniu (dotyczy to zwłaszcza drukarek usytuowanych w miejscach ogólnie dostępnych);
4) **czystego ekranu (pulpitu)** – każdorazowe opuszczenie pomieszczenia w godzinach pracy powinno zostać poprzedzone zablokowaniem komputera; na wszystkich stacjach aktywny jest wygaszasz ekranu zabezpieczony hasłem, który aktywuje się automatycznie po przekroczeniu max. 15 minut braku aktywności. Każdy użytkownik systemu zobowiązany jest zadbać, aby po zakończeniu pracy sprzęt został poprawnie wyłączony;
5) **czystego kosza** – nieprzydatne dokumenty, brudnopisy, zbędne kopie muszą zostać trwale zniszczone w sposób uniemożliwiający odtworzenie zawartych w nich informacji. Zasada ta dotyczy również informacji zapisanych w innej niż papierowa formie – na nośnikach elektronicznych. Do kosza na śmieci nie wyrzuca się płyt CD/DVD oraz innych nośników informacji, powinny one zostać zniszczone w specjalistycznych niszczarkach;

6) **legalności oprogramowania** – zabrania się samodzielnego instalowania oprogramowania, a także przechowywania na komputerach treści naruszających prawo;
7) **monitoringu** – każde stanowisko komputerowe może zostać objęte monitorowaniem działania użytkowników i oprogramowania;
8) **nadzorowania kluczy** – pobrane klucze do pomieszczeń powinny być w każdym czasie pod kontrolą. Ponadto pracownicy odpowiedzialni są za należyte zabezpieczenie kluczy do ich biurek stanowiskowych oraz szaf biurowych, w których przechowywane są dokumenty;
9) **odpowiedzialności za zasoby (aktywa)** – każdy, kto przetwarza informacje jest odpowiedzialny za zapewnienie ich dostępności, poufności i integralności poprzez przestrzeganie procedur ich bezpiecznego przetwarzania oraz ochronę przyznanych zasobów, w tym za szkody wyrządzone w systemie informatycznym przez nieautoryzowane oprogramowanie lub niewłaściwe korzystanie z urządzeń systemu informatycznego;
10) **świadomej konwersacji** – polega na tym, że „nie zawsze i wszędzie trzeba mówić co się wie, ale zawsze i wszędzie trzeba wiedzieć co, gdzie i do kogo się mówi";
11) **świadomości zbiorowej** – wszyscy są świadomi konieczności ochrony zasobów, zapewnienia ich dostępności, poufności, integralności i aktywnie w tym procesie uczestniczą;
12) **weryfikacji przenośnych nośników informacji** – każdy komputer wymusza przeprowadzenie skanowania przez system antywirusowy zewnętrznych nośników informacji przed ich uruchomieniem, na stacjach roboczych pracujących w sieci Urzędu wprowadza się blokowanie portów USB, które uniemożliwiało będzie korzystanie z nośników, które nie zostały ujęte w ewidencji zewnętrznych nośników informacji dopuszczonych do użytkowania;
13) **wiedzy koniecznej** – w myśl której dostęp do informacji ograniczony jest do tych, które są niezbędne do prawidłowego wykonywania obowiązków na danym stanowisku;
14) **zgłaszania zdarzeń, incydentów, nieprawidłowej pracy sprzętu** – każdy użytkownik systemu zobowiązany jest do zgłaszania wszelkich zauważonych nietypowych zdarzeń, incydentów oraz nieprawidłowej pracy sprzętu.

§ 9
Dobór zabezpieczeń

1. Cele stosowania zabezpieczeń i zabezpieczenia powinny być dobierane adekwatnie do wymagań prawnych i wyników analizy ryzyka dla bezpieczeństwa informacji.
2. Zabezpieczenia fizyczne, techniczne i organizacyjne powinny uzupełniać się wzajemnie zapewniając wspólnie wymagany poziom bezpieczeństwa informacji.
3. W doborze celów stosowania zabezpieczeń i zabezpieczeń należy kierować się zaleceniami Polskiej Normy PN-ISO/IEC 27002.

§ 10
Sankcje za naruszenie zasad bezpieczeństwa informacji

Nieprzestrzeganie zasad zawartych w dokumentach Polityki Bezpieczeństwa Informacji, jest naruszeniem obowiązków pracowniczych wynikających w szczególności z ustaw o pracownikach samorządowych oraz ustawy Kodeks Pracy i może pociągnąć za sobą skutki dyscyplinarne oraz spowodować pociągnięcie do odpowiedzialności wynikającej z przepisów prawa i Regulaminu Pracy.

§ 11
Zasady rozpowszechniania dokumentu

1. Polityka Bezpieczeństwa Informacji i dokumenty z nią związane będą dostępne na Platformie Informacyjnej i Szkoleniowej Urzędu (UrzędAs).
2. Podmiotom zewnętrznym Polityka Bezpieczeństwa Informacji udostępniona jest w Biuletynie Informacji Publicznej Urzędu.

Zatwierdzam

Prezydent Miasta Tychy

/-/ mgr inż. Andrzej Dziuba

……..……..
(data i podpis Prezydenta Miasta)

24 maja 2018 r.