Załącznik nr 2
do Zarządzenia Nr 373/17
Prezydenta Miasta Łomża
z dnia 22 listopada 2017 r.

Zakres zadań Administratora Systemów Informatycznych w Urzędzie Miejskim w Łomży

1. Głównym zadaniem Administratora Systemu Informatycznego (ASI) jest kontrola przestrzegania zasad ochrony danych osobowych pod kątem zabezpieczeń teleinformatycznych.
2. ASI w zakresie zadań wykonywanych dla zapewnienia systemom informatycznym przetwarzającym dane osobowe, bezpieczeństwa zgodnego z celami i metodologią obowiązujących w Urzędzie regulacji wewnętrznych ADO w obszarze przetwarzania danych osobowych, współpracuje bezpośrednio z Administratorem Bezpieczeństwa Informacji (ABI).
3. Do podstawowych zadań Administratora Systemu Informatycznego należy:
   1) Dostosowanie wszystkich systemów informatycznych służących do przetwarzania danych osobowych do wymogów przepisów prawa. Monitorowanie zbierania, przechowywania, przekazywania i udostępniania danych osobowych przetwarzanych w systemach informatycznych.
   2) Nadzorowanie logicznych i fizycznych zabezpieczeń systemów informatycznych w zakresie przepływu informacji pomiędzy systemami a siecią publiczną, działań inicjowanych z sieci i z systemów informatycznych, umów i procedur przekazywania podmiotowi zewnętrznemu dostępu do systemów informatycznych oraz elektronicznych nośników informacji zawierających dane osobowe.
   3) Nadzorowanie realizacji decyzji ADO odnośnie nadania pracownikom uprawnień dostępu do danych i wybranych funkcji narzędzi służących do ich przetwarzania, w środowisku IT Urzędu tj.:
      a) zakładania, blokowania, zawieszania i uaktywniania kont użytkowników w systemie IT,
      b) przypisywania do kont startowych haseł uwierzytelniających użytkowników tych kont,
      c) resetowania utraconych haseł,
      d) usuwania kont i uprawnień dla kont osób, które zakończyły pracę w Urzędzie,
      e) prowadzenie i aktualizacja rejestru nadanych uprawnień dostępu.
   4) Nadzorowanie naprawy oraz likwidacji urządzeń komputerowych lub innych elektronicznych nośników informacji zawierających dane osobowe.
   5) Zapewnienie zabezpieczenia pomieszczenia serwerowni przed dostępem osób nieuprawnionych, w tym zabezpieczenia fizyczne, techniczne, środowiskowe, personalne i organizacyjne
   6) Zapewnienia ciągłości działania systemu poprzez systematyczne wykonywanie kopii zapasowych oprogramowania i danych.
   7) Zapewnienie awaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych osobowych.
   8) Zapewnienie serwerom i stacjom roboczym niezbędnych licencji programowych oraz monitorowanie legalności oprogramowania wykorzystywanego na stacjach roboczych.
   9) Dokonywanie oceny zgodności programów z przepisami bezpieczeństwa przetwarzania danych osobowych i zapewnienie im adekwatnych i systematycznie aktualizowanych zabezpieczeń.
   10) Zapewnienie eksploatowanym systemom opieki serwisowej producenta – zawieranie umów regulujących formy tej opieki oraz systematyczne ich aktualizowanie.
   11) Podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń.
   12) Współpraca z ABI przy przygotowaniu, wdrażaniu i aktualizowaniu dokumentacji ochrony danych osobowych, w szczególności instrukcji zarządzania systemem teleinformatycznym.
   13) Współpraca z ABI przy kontrolowaniu pracowników w zakresie przestrzegania zasad bezpieczeństwa i ochrony danych osobowych oraz przy przeprowadzaniu okresowych planów sprawdzeń zastosowanych środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a także przy wyjaśnianiu i dokumentowaniu przypadków naruszenia zasad bezpieczeństwa systemów informatycznych.