ZARZĄDZENIE Nr 225/2019
Prezydenta Miasta Ciechanów
z dnia 25 listopada 2019 r.
w sprawie wyznaczenia Administratora Systemów Informatycznych (ASI).

Na podstawie artykułem 24 ustęp 1 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz. U. EL. L. z 2016 r. numer 119, strona 1 z 2018 roku NR 127, str. 2) zarządzam, co następuje:

Paragraf 1

Wyznaczam do pełnienia obowiązków Administratora Systemów Informatycznych: **Tomasza Mielnickiego, Pawła Żochowskiego** oraz **Mateusza Fila –** Pracowników Referatu ds. Procesów IT.

Paragraf 2

Wykonanie zarządzenia powierzam Sekretarzowi Miasta Ciechanów.

Paragraf 3

Traci moc Zarządzenie nr 58/2008 Prezydenta Miasta Ciechanów z dnia 01.07.2008 r. w sprawie powierzenie obowiązków w zakresie ochrony danych osobowych.

Paragraf 4

Zarządzenie wchodzi w życie z dniem podpisania.

Prezydent Miasta Ciechanów
Krzysztof Kosiński

Zakres zadań i uprawnień Administratora Systemów Informatycznych w Urzędzie Miasta Ciechanów

1. Administrator Systemów Informatycznych, zwany dalej ASI, wykonuje zadania w zakresie niniejszego Zarządzenia oraz upoważnień i pełnomocnictw nadanych przez Administratora Danych Osobowych.
2. Celem działania ASI jest nadzorowanie i realizowanie zasad bezpieczeństwa przetwarzania
   i ochrony danych osobowych w systemach informatycznych Urzędu Miasta Ciechanów.
3. ASI, realizując swoje zadania współpracuje z IOD w Urzędzie Miasta Ciechanów.
4. Do zakresu zadań ASI należy w szczególności:
   1) monitorowanie:
      a) zbierania, przechowywania, przekazywania i udostępniania danych osobowych przetwarzanych w systemach informatycznych,
      b) zabezpieczeń systemów informatycznych w zakresie stosowania:
         - IPS/Firewall/VPN oraz programów antywirusowych,
         - szyfrowania dysków i środków ochrony kryptograficznej,
         - mechanizmów autoryzacji i kontroli dostępu do danych (uwierzytelnianie użytkowników, hasła),
         - zabezpieczenia przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do baz danych osobowych,
   2) nadzorowanie:
      a) zakładania, blokowania, zawieszania i uaktywniania kont w systemie informatycznym,
      b) umów i procedur przekazywania podmiotowi zewnętrznemu dostępu do systemów informatycznych oraz elektronicznych nośników informacji zawierających dane osobowe,
      c) tworzenia kopii zapasowych zbiorów danych osobowych,
      d) zasad ochrony, przekazywania i niszczenia kopii zapasowych zbiorów danych osobowych oraz programów zastosowanych do ich przetwarzania,
   3) realizowanie przedsięwzięć w zakresie:
      a) wyjaśniania i dokumentowania, wspólnie z IOD, przypadków naruszenia zasad bezpieczeństwa systemów informatycznych,
      b) kontrolowania, wspólnie z IOD, pracowników w zakresie przestrzegania zasad bezpieczeństwa i ochrony danych osobowych poprzez prowadzone sprawdzenia (kontrole lub audyty).
      c) prowadzenia ewidencji osób upoważnionych do przetwarzania danych osobowych w systemach informatycznych,