MBP.021.8.2020.AG

ZARZĄDZENIE nr 8/2020
Dyrektora Miejskiej Biblioteki Publicznej w Bornem Sulinowie
z dnia 14 kwietnia 2020r.
w sprawie powołania Administratora Systemów Informatycznych
w Miejskiej Bibliotece Publicznej w Bornem Sulinowie

Na podstawie art. 52 ust. 1 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2019r., poz. 742 z późn. zm.) oraz art. 24 ust. 1 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U. UE. L. 119.1 z 04.05.2016) w związku z § 6 ust. 1 Statutu Miejskiej Biblioteki Publicznej w Bornem Sulinowie wprowadzonego Uchwałą Rady Miejskiej Nr XXVIII/350/2013 z dnia 19 lutego 2013 r. i § 14 ust. 1 pkt 2 Regulaminu organizacyjnego Miejskiej Biblioteki Publicznej w Bornem Sulinowie stanowiącego załącznik do zarządzenia Nr 3 Dyrektora Miejskiej Biblioteki Publicznej w Bornem Sulinowie z dnia 30 maja 2018r. oraz zarządzam, co następuje:

§ 1. Wyznaczam Pana Daniela Graszkę do pełnienia obowiązków Administratora Systemów Informatycznych w Miejskiej Bibliotece Publicznej w Bornem Sulinowie.

§ 2. Zakres czynności wykonywanych przez Administratora Systemów Informatycznych stanowi załącznik do niniejszego zarządzenia.

§ 3. Zarządzenie wchodzi w życie z dniem podpisania.

Dyrektor
Miejskiej Biblioteki Publicznej
(-) Anna Gałązka

Załącznik
do Zarządzenia numer 8/2020

Dyrektora Miejskiej Biblioteki Publicznej w Bornem Sulinowie
z dnia 14 kwietnia 2020r.
w sprawie powołania Administratora Systemów Informatycznych
w Miejskiej Bibliotece Publicznej w Bornem Sulinowie

Zakres czynności
Administratora Systemów Informatycznych
w Miejskiej Bibliotece Publicznej w Bornem Sulinowie

Administrator Systemów Informatycznych (ASI) w Miejskiej Bibliotece Publicznej w Bornem Sulinowie:

1) odpowiada za bieżące prowadzenie przetwarzania danych osobowych i bezpieczeństwo danych w systemach informatycznych,
2) prowadzi ewidencję oprogramowania i zarządza licencjami oprogramowania,
3) odpowiada za instalowanie, odinstalowywanie oraz obsługę techniczną oprogramowania,
4) odpowiada za bezpieczeństwo danych osobowych w systemie informatycznym,
5) administruje serwerami służącymi przetwarzaniu danych i zarządza sieciami,
6) podejmuje działania przeciwdziałające szkodliwemu oprogramowaniu i wdraża zabezpieczenia systemów informatycznych,
7) identyfikuje potencjalne zagrożenia i podatności dla systemów informatycznych,
8) wykrywa nieautoryzowany dostęp do systemów i zapewnia zachowanie ciągłości ich funkcjonowania,
9) sprawuje nadzór nad zgłaszanymi oraz możliwymi do wystąpienia incydentami oraz podejmuje działania korygujące oraz zapobiegające wystąpieniu incydentu,
10) zakłada i konfiguruje konta użytkowników oraz nadaje im uprawnienia w systemie informatycznym,
11) zarządza skrzynkami e-mailowymi wykorzystywanymi przez pracowników,
12) przeciwdziała dostępowi osób niepowołanych do systemu, w którym przetwarzane są dane osobowe,
13) podejmuje odpowiednie działania w przypadku wykrycia naruszeń w systemie zabezpieczeń,
14) dba o zapewnienie awaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych,
15) sprawuje nadzór nad fizycznym zabezpieczeniem pomieszczeń, w których przetwarzane są dane osobowe oraz kontrolą przebywających w nich osób,
16) pilnuje, aby komputery przenośne, w których przetwarzane są dane osobowe zabezpieczone były hasłem dostępu przed nieautoryzowanym uruchomieniem oraz aby nie były one udostępniane osobom nieupoważnionym do przetwarzania danych osobowych,
17) zapewnia zgodny z Polityką Bezpieczeństwa Informacji nadzór nad serwisowaniem urządzeń, prowadzeniem napraw, konserwacją oraz likwidacją urządzeń komputerowych na których zapisane są dane osobowe,
18) zarządza hasłami użytkowników i sprawuje nadzór nad przestrzeganiem procedur określających częstotliwość ich zmiany zgodnie z wytycznymi,
19) zapewnia wykonywanie kopii bezpieczeństwa (awaryjnych), ich przechowywanie oraz okresowe sprawdzanie pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu
20) sprawuje nadzór nad przeglądami, konserwacjami oraz uaktualnieniami systemów służących do przetwarzania danych osobowych oraz wszystkimi innymi czynnościami wykonywanymi na bazach danych osobowych,
21) sprawuje nadzór nad systemem komunikacji w sieci komputerowej oraz przesyłaniem danych za pośrednictwem urządzeń teletransmisji,
22) sprawuje nadzór nad obiegiem oraz przechowywaniem dokumentów i wydawnictw zawierających dane osobowe generowane przez system informatyczny,
23) sprawuje nadzór nad funkcjonowaniem mechanizmów uwierzytelniania użytkowników w systemie informatycznym przetwarzającym dane osobowe oraz kontrolą dostępu do danych osobowych,
24) ustala identyfikatory użytkowników,

25) pilnuje, aby hasła użytkowników były zmieniane zgodnie z wytycznymi,
26) dba, aby dostęp do danych osobowych przetwarzanych w systemie był możliwy wyłącznie po podaniu identyfikatora i właściwego hasła,
27) dba, aby hasła użytkowników były trzymane w tajemnicy,
28) dba, aby identyfikatory osób, które utraciły uprawnienia do przetwarzania danych osobowych zastały natychmiast wyrejestrowane, a ich hasła unieważnione,
29) dba, aby ekrany monitorów stanowisk komputerowych, na których przetwarzane są dane osobowe, automatycznie wyłączały się po upływie ustalonego czasu nieaktywności użytkownika,
30) podejmuje natychmiastowe działania zabezpieczające stan systemu informatycznego w przypadku otrzymania informacji o naruszeniu zabezpieczeń systemu informatycznego lub informacji o zmianach w sposobie działania programu lub urządzeń wskazujących na naruszenie bezpieczeństwa danych,
31) analizuje sytuacje, okoliczności i przyczyny, które doprowadziły do naruszenia bezpieczeństwa danych (jeśli takie wystąpiło) i przygotowuje oraz przedstawia administratorowi danych odpowiednich zmian do instrukcji zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych,
32) wdraża narzędzia, metody pracy oraz sposoby zarządzania systemem informatycznym, które wzmocnią bezpieczeństwo przetwarzania danych,
33) zarządza programami antywirusowymi,
34) zachowuje tajemnicę lub poufność co do wykonywania swoich zadań – zgodnie z prawem Unii Europejskiej lub prawem państwa członkowskiego.