ZESPÓŁ SZKÓŁ PODSTAWOWEJ I MUZYCZNEJ
w Nowym Mieście Lubawskim
ul. Tysiąclecia 33, tel. 56 474 26 93
NIP 8771474504, Regon 281091045

Znak sprawy :

ZSz.S.021.13..2020

Nowe Miasto Lubawskie,10.03.2020r.

Zarządzenie nr 13 /ZSz/ 2020

Dyrektora Zespołu Szkół Podstawowej i Muzycznej w Nowym Mieście Lubawskim
z dnia 10.03.2020r.
w sprawie powołania Administratora Systemu Informatycznego

Podstawa prawna :
Art. 24, 32 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) z dnia 27 kwietnia 2016 r. (Dz. Urz. UE. L Nr 119, str. 1) wskazuje, że Administrator powinien zapewnić odpowiednie środki techniczne oraz organizacyjne gwarantujące bezpieczeństwo przetwarzanych danych osobowych.

W związku z powyższym wyznaczam z dniem 10.03.2020r. Krzysztofa Lange na Administratora Systemu Informatycznego w Zespole Szkół Podstawowej i Muzycznej w Nowym Mieście Lubawskim.

§ 1

Zakres czynności dla Administratora Systemu Informatycznego stanowi załącznik nr 1 do niniejszego zarządzenia.

§ 2

Zarządzenie wchodzi w życie z dniem podpisania

DYREKTOR
ZESPOŁU SZKÓŁ
mgr Zbigniew Domżalski

Załącznik nr 1 do Zarządzenia nr..13/Z.Sz./2020
Dyrektora Zespołu Szkół Podstawowej i Muzycznej w Nowym Mieście Lubawskim
z dnia 10.03.2020r.

Zakres czynności Administratora Systemu Informatycznego w Zespole Szkół Podstawowej i Muzycznej w Nowym Mieście Lubawskim.:

Nadzór nad stosowaniem środków zapewniających bezpieczeństwo przetwarzania danych osobowych w systemach informatycznych, a w szczególności przeciwdziałających dostępowi osób niepowołanych do tych systemów (administrowanie system informatycznym).

1. Wspieranie Administratora przy wdrażaniu dokumentacji z zakresu ochrony danych osobowych, w szczególności w kwestiach zarządzania systemem informatycznym.
2. Nadzorowanie działania mechanizmów uwierzytelnienia użytkowników oraz kontroli dostępu do systemu informatycznego.
3. Nadawanie haseł użytkownikom.
4. Prowadzenie monitoringu przetwarzania danych osobowych.
5. Kontrolowanie zastosowanych środków technicznych i organizacyjnych zapewniających ochronę danych osobowych przetwarzanych w systemach informatycznych w tym m.in. systemu antywirusowego, awaryjnego zasilania komputerów, konserwacja oraz uaktualnianie systemów informatycznych.
6. Podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń, identyfikacja i analiza zagrożeń oraz ocena ryzyka, na które może być narażone przetwarzanie danych osobowych w systemach informatycznych i tradycyjnych.
7. Sprawowanie nadzoru nad przechowywanymi kopiami zapasowymi.
8. Inicjowanie i nadzór nad wdrażaniem nowych narzędzi, procedur organizacyjnych oraz sposobów zarządzania systemami informatycznymi, które mają doprowadzić do wzmocnienia bezpieczeństwa przy przetwarzaniu danych osobowych.
9. Opracowanie planów awaryjnych w zakresie zapewnienia ciągłości działania i odtwarzania systemów informatycznych, między innymi przez systematyczne wykonywanie kopii zapasowych.
10. Podejmowanie działań służących zapewnieniu niezawodności zasilania urządzeń wraz z zapewnieniem awaryjnego źródła zasilania oraz zabezpieczeń przed zakłóceniami w sieci zasilającej.
11. Prowadzenie ewidencji sprzętu teleinformatycznego oraz oprogramowania.
12. Nadzorowanie napraw, konserwacji oraz likwidacji urządzeń komputerowych, na których zapisane są dane osobowe.
13. Informowanie na bieżąco Administratora o przypadkach awarii programów wynikających z posługiwania się przez użytkowników nieautoryzowanym oprogramowaniem, nie przestrzegania zasad używania programów antywirusowych, niewłaściwego wykorzystywania sprzętu komputerowego.
14. Prowadzenie dziennika zdarzeń w systemie informatycznym, w szczególności w zakresie prowadzonych prac interwencyjnych, aktualizacji, konserwacji oraz prowadzonych działań sprawdzających lub kontrolujących.
15. Poinformowanie Inspektora Ochrony Danych, w sytuacji stwierdzenia naruszenia zabezpieczeń systemu o danym naruszeniu i współpraca z Inspektorem Ochrony Danych przy usuwaniu naruszenia.
16. Dokonywanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji.
17. Przeprowadzenie co najmniej raz w roku audytu sprawdzającego stan zabezpieczenia Placówki, pomieszczeń, programów oraz zabezpieczeń sieci informatycznej.