ZAKŁAD GOSPODARKI
KOMUNALNEJ I MIESZKANIOWEJ
67-407 Szlichtyngowa, Rynek nr 10
tel. 65-549-23-45
NIP 6971011601, REG. 410006034

ZARZĄDZENIE Nr 1/2021

Dyrektora Zakładu Gospodarki Komunalnej i Mieszkaniowej

w Szlichtyngowej

z dnia **31.03.2021 r.**

w sprawie: **wprowadzenia Procedury dot. Bezpieczeństwa Informacji**

Na podstawie art. 24 ust. 2 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 osobowych).

Zarządza się, co następuje:

§ 1

Wprowadzam do Polityki Ochrony Danych Osobowych wraz z Procedurami i Regulaminem Ochrony Danych Osobowych w ZGKiM w Szlichtyngowej, wprowadzonej rozporządzeniem Dyrektora ZGKiM w Szlichtyngowej nr 1/2019 z dnia 29.03.2019 roku, procedurę dot. Bezpieczeństwa Informacji, jako 13 punkt do załącznika C, do Polityki Ochrony Danych Osobowych, którego treść stanowi załącznik nr 1 do zarządzenia.

§ 2

Każdy pracownik, zgodnie z wykazem, jest obowiązany zapoznać się z treścią załącznika nr 1.

§ 3

Pracodawca zobowiązuje wszystkich pracowników do przestrzegania Procedury dot. Bezpieczeństwa Informacji pod groźbą konsekwencji służbowych, przewidzianych prawem.

§ 4

Zarządzenie wchodzi w życie z dniem ogłoszenia.

DYREKTOR
Justyna Urbaniak

Procedura dot. Bezpieczeństwa Informacji

1.1 Kontrola uprawnień

Informatyk zatrudniony na świadczenie usług przeprowadza okresową kontrolę uprawnień i kont użytkowników co najmniej raz na kwartał, w celu weryfikacji czy użytkownicy posiadają uprawnienia adekwatne do wykonywanej pracy w systemach informatycznych. Z przeprowadzonej kontroli ww. osoba sporządza notatkę służbową wg wzoru stanowiącego załącznik nr 1 do niniejszej procedury.

1.2 Inwentaryzacja sprzętu i oprogramowania służącego do przetwarzania informacji

Informatyk zatrudniony na świadczenie usług jest odpowiedzialny za prowadzenie inwentaryzacji sprzętu komputerowego i oprogramowania przynajmniej raz w roku oraz utrzymywanie jej w aktualności.
Z przeprowadzonej inwentaryzacji sporządzony jest protokół.

1.3 Ochrona przetwarzanych informacji

Monitorowanie dostępu do informacji może być realizowane za pomocą: logów aplikacji dziedzinowych oraz logów systemów operacyjnych. Informacje te zawierają: identyfikator i/lub adres IP komputera, dokładną datę, zakres dostępu (przydzielony/odrzucony) oraz opis wykonanej lub zablokowanej akcji.

Czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji realizowane są przez ochronę antywirusową.

Wprowadzenie blokady bezpośredniego dostępu stacji roboczych do sieci Internet:

1) umożliwia zablokowanie bezpośredniego połączenia złośliwego oprogramowania z sieci Internet,
2) utrudnia ominięcie systemów zabezpieczeń,
3) umożliwia kontrolę dostępu i rozliczalność działań użytkowników.

1.4. Zapisy definiujące obowiązek zachowania w tajemnicy informacji dostępowych.

1) Osoby zajmujące się zamówieniami publicznymi oraz osoby zawierające umowy muszą zwracać uwagę na istotne elementy przy podpisywaniu umów tj. muszą być w umowie zapisy definiujące obowiązek zachowania w tajemnicy informacji dostępowych.