

**ZARZĄDZENIE NR 99/21**  
**BURMISTRZA MIASTA I GMINY SZLICHTYNGOWA**

z dnia 18 października 2021 r.

**w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji w Urzędzie Miasta i Gminy Szlichtyngowa.**

Na podstawie art. 33 ust. 3 i 5 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (t.j. Dz. U. z 2021 r. poz.1372 ze zm. ), oraz 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.** Wprowadza się do stosowania Politykę Bezpieczeństwa Informacji w Urzędzie Miasta i Gminy Szlichtyngowa jak w brzmieniu załącznika do zarządzenia.

**§ 2.** Wykonanie zarządzenia powierza się Zastępcy Burmistrza Miasta i Gminy Szlichtyngowa.

**§ 3.** Zarządzenie wchodzi w życie z dniem podpisania.

Burmistrz Miasta i Gminy  
Szlichtyngowa

**Jolanta Wielgus**

## **Polityka Bezpieczeństwa Informacji w Urzędzie Miasta i Gminy Szlichtyngowa.**

### **1. Kontrola uprawnień**

ASI przeprowadza okresową kontrolę uprawnień i kont użytkowników co najmniej raz na pół roku, 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.

### **2. Inwentaryzacja sprzętu i oprogramowania służącego do przetwarzania informacji**

ASI jest odpowiedzialny za prowadzenie inwentaryzacji sprzętu komputerowego i oprogramowania przynajmniej raz w roku oraz utrzymywanie jej w aktualności. Z przeprowadzonej inwentaryzacji sporządzony jest protokół.

### **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.

### **4. Zapisy definiujące obowiązek zachowania w tajemnicy informacji dostępowych.**

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.

### **5. Zwiększenie bezpieczeństwa teleinformatycznego**

ASI zobowiązany jest do przeprowadzania raz w roku szkolenia korzystania z systemów komputerowych w ramach zwiększenia bezpieczeństwa teleinformatycznego. Ze szkolenia sporządzany jest protokół.

## Protokół przeprowadzenia kontroli

W związku z kontrolą uprawnień i kont użytkowników z dnia ..... stwierdzam co następuje:

1. Użytkownicy pracują na systemach zgodnych z ich uprawnieniami TAK / NIE.

Jeśli NIE, należy wskazać pracowników którym należy nadać lub zabrać upoważnienia:

.....  
.....

2. Użytkownicy posiadają na stacjach roboczych oprogramowanie na które jednostka posiada licencje TAK / NIE.

Jeśli NIE, należy wykazać to oprogramowania oraz nazwy stacji roboczych, na których się ono znajduje

.....  
.....

3. Na stacjach roboczych pracowników znajduje się oprogramowanie nie związane z pracą służbową np. komunikatory społecznościowe, aplikacje służące do wymiany lub pobierania plików, czytniki prywatnej poczty, oprogramowanie umożliwiające dostęp do prywatnej chmury z danymi itp. portalami społecznościowymi TAK / NIE.

Jeśli TAK należy wskazać pracowników oraz stacje robocze, na których zostało zidentyfikowane wyżej wymienione ..... oprogramowanie:

.....  
.....

4. Czy na stacjach roboczych pracowników znajdują się dokumenty i korespondencja nie związana z czynnościami służbowymi TAK / NIE.

Jeśli TAK należy wskazać pracowników oraz stacje robocze na której niezgodności występują:

.....  
.....

5. Wnioski i zalecenia pokontrolne:

.....  
.....  
.....

.....

(podpis kontrolującego)