Warunki dostępu Osoby Trzeciej do Systemów lub Zasobów Teleinformatycznych w Zespole Szkół Technicznych w Pleszewie

I. Zasady dostępu Kontrahenta do Systemów lub Zasobów Teleinformatycznych.

1. Dostęp Kontrahenta do Systemów lub Zasobów Teleinformatycznych może odbywać się wyłącznie na zasadach określonych w niniejszych Warunkach.
2. Kontrahent, który w ramach wykonywania umowy głównej posiada dostęp do danych osobowych musi przed uzyskaniem dostępu podpisać umowę o powierzeniu danych osobowych do przetwarzania danych.
3. Kontrahent zobowiązany jest wykorzystywać przyznany dostęp do Systemów lub Zasobów Teleinformatycznych wyłącznie w celach i w zakresie uzasadnionym realizacją zadań wynikających z przedmiotu umowy, zgodnie z umową oraz obowiązującymi przepisami prawa.
4. Kontrahent zobowiązany jest zapewnić właściwą ochronę udostępnionych mu Systemów lub Zasobów Teleinformatycznych, polegającą w szczególności na zapewnieniu zespołu środków organizacyjnych, technicznych i prawnych stosowanych w celu zapewnienia Bezpieczeństwa Informacji.
5. Kontrahent w związku z dostępem do Systemów lub Zasobów Teleinformatycznych ma obowiązek stosować się do zaleceń oraz wymagań mających na celu zapewnienie Bezpieczeństwa Informacji, w tym m.in. zapoznać Użytkowników i zapewnić przestrzeganie wskazanych przez Administratora Danych zasad bezpiecznego użytkowania Systemu Teleinformatycznego oraz zasad bezpiecznego użytkowania środowiska biurowego. Kontrahent jednocześnie zapewnia, że dostęp do Systemów lub Zasobów Teleinformatycznych Administratora Danych będą posiadać wyłącznie uprawnieni i przeszkoleni Użytkownicy, w zakresie i na czas niezbędny do realizacji przez nich przedmiotu Umowy.
6. Wszelkie oprogramowanie wykorzystywane w ramach realizacji przedmiotu umowy musi być użytkowane z poszanowaniem praw własności intelektualnej, w szczególności zgodnie z ustawą o prawie autorskim i prawach pokrewnych.
7. Kontrahent ponosi pełną odpowiedzialność za działania Użytkowników w Systemach lub Zasobach Teleinformatycznych Administratora Danych oraz za wszelkie szkody powstałe w związku z korzystaniem przez Kontrahenta z dostępu do Systemów lub Zasobów Teleinformatycznych w sposób sprzeczny z niniejszymi Warunki.
8. Brak dostępu do Systemów lub Zasobów Teleinformatycznych Administratora Danych po stronie Kontrahenta, wynikający z przyczyn leżących po jego stronie, nie wyłącza odpowiedzialności Kontrahenta z tytułu prawidłowego wykonania Umowy.

II. Incydenty bezpieczeństwa.

1. Kontrahent zobowiązany jest do niezwłocznego zgłaszania wszelkich zauważonych zdarzeń, które noszą znamiona lub są Incydentami Bezpieczeństwa do Opiekuna Kontrahenta oraz udzielania wszelkich niezbędnych informacji oraz wsparcia pracownikom Administratora Danych zaangażowanym, z racji pełnionych obowiązków, w proces obsługi Incydentów Bezpieczeństwa.

2. Administrator Danych zastrzega sobie prawo do zbierania i zabezpieczania wszelkich dowodów wskazujących na wystąpienie i powstanie skutków Incydentu Bezpieczeństwa, w szczególności prawo do wystąpienia do każdego z Użytkowników z pisemnym żądaniem niezwłocznego włączenia się w obsługę Incydentu Bezpieczeństwa, w tym niezwłocznego podania wszelkich niezbędnych informacji w zakresie badanego Incydentu Bezpieczeństwa.

III. Uprawnienia kontrolne.

1. Administrator Danych zastrzega sobie prawo do przeprowadzenia kontroli zastosowanych przez Kontrahenta rozwiązań organizacyjno-technicznych, zgodności zaimplementowanych mechanizmów bezpieczeństwa z obowiązującym prawem i niniejszymi Warunkami oraz sposobu korzystania przez Użytkowników z udostępnionych im Systemów lub Zasobów Teleinformatycznych.
2. Kontrola może być przeprowadzona w dniach roboczych w godz. 8.00 – 15.00, w terminie ustalonym przez Administratora Danych i przekazanym pisemnie do wiadomości Kontrahenta, z co najmniej 1 - dniowym wyprzedzeniem.
3. Kontrahent zobowiązany jest do umożliwienia przeprowadzenia kontroli w szczególności poprzez:
    1) umożliwienie osobom kontrolującym wstępu do pomieszczeń, w których jest wykonywana działalność związana z umową,
    2) zapewnienie osobom kontrolującym dostępu do wszelkich wymaganych informacji, urządzeń oraz Systemów Teleinformatycznych wykorzystywanych do realizacji umowy oraz Użytkowników i dokumentów Kontrahenta w zakresie wynikającym z niniejszej Umowy,
    3) udzielanie osobom kontrolującym przez osoby zaangażowane w realizację umowy ze strony Kontrahenta wyjaśnień w żądanej formie - pisemnej lub ustnej w zakresie wynikającym z realizacji przedmiotu niniejszej Umowy.
4. W przypadku stwierdzenia uchybień w zakresie objętym kontrolą, Administrator Danych ma prawo wezwać Kontrahenta do podjęcia działań w celu ich usunięcia w wyznaczonym terminie. Nie usunięcie uchybień w wyznaczonym terminie, może stanowić podstawę do wypowiedzenia umowy.