**Załącznik nr 10 do SWZ**

***Wytyczne bezpieczeństwa informacji dla Wykonawców***

WYTYCZNE BEZPIECZEŃSTWA INFORMACJI DLA WYKONAWCÓW REALIZUJĄCYCH DOSTAWY LUB ŚWIADCZĄCYCH USŁUGI NA RZECZ MAZOWIECKIEGO ODDZIAŁU REGIONALNEGO ARIMR

*(wyciąg z Zarządzenia Prezesa ARIMR Nr 78/2019 z dnia 03 czerwca 2019 r.*

*w sprawie bezpieczeństwa informacji w ARiMR z późn. zm.)*

Bezpieczeństwo Informacji w ARIMR

1. Polityka Bezpieczeństwa Informacji obowiązuje wszystkich wykonawców, jednostki zewnętrzne i ich pracowników, o ile w trakcie realizacji Umowy otrzymują dostęp do zasobów lub stref informacyjnych Mazowieckiego Oddziału Regionalnego Agencji Restrukturyzacji i Modernizacji Rolnictwa (Mz OR ARiMR).
2. Wykonawca zobowiązuje się do przestrzegania przyjętych w ARiMR zasad bezpieczeństwa informacji, których treść jest określona w Zarządzeniu nr 78/2019 Prezesa ARiMR z dnia 03 czerwca 2019 r. w sprawie bezpieczeństwa informacji w ARiMR z późn. zm., a przedstawiona w obecnych wytycznych.
3. Zarządzenie dotyczy zasobów materialnych i niematerialnych Agencji i znajduje zastosowanie zarówno do pracowników Agencji, jak i podmiotów zewnętrznych z nią współpracujących lub wykonujących usługi.
4. Wykonawca potwierdza fakt zapoznania się z **wytycznymi własnoręcznym** podpisem na umowie lub oświadczeniu, przedłożonym przez ARiMR.
5. Wszystkie informacje wrażliwe i środki służące do ich przetwarzania, do których Wykonawca będzie miał dostęp i są własnością Agencji lub są przez nią wykorzystywane, podlegają ochronie.
6. Informacja prawnie chroniona oraz każda informacja, której utrata, ujawnienie lub udostępnienie osobie/podmiotowi nieuprawnionemu mogłoby spowodować szkodę materialną lub niematerialną dla Agencji lub naruszyć prawnie chroniony interes innych osób/podmiotów podlega szczególnej ochronie.
7. W przypadku, gdy Wykonawca przypadkowo wszedł w posiadanie dokumentów lub innych materiałów stanowiących informację prawnie chronioną dla ARIMR, ma obowiązek natychmiastowego przekazania jej Kierownikowi jednostki organizacyjnej lub Inspektorowi Bezpieczeństwa Informacji w ARiMR.
8. Wykonawca zobowiązuje zapoznać pracowników i osoby trzecie realizujące objęte Umową zadania, w zakresie zachowania zasad bezpieczeństwa informacji określonych w Wytycznych bezpieczeństwa informacji.
9. Odpowiedzialność za bezpieczeństwo informacji MzOR ARiMR obejmuje nie tylko siedzibę oddziału i biur powiatowych, ale także wszelkie sytuacje, w których Wykonawca może mieć dostęp do informacji prawnie chronionych będących własnością ARIMR.
10. Informacje związane z działalnością Agencji są przetwarzane także poza jej siedzibą. Obejmuje to także i w szczególności zdalny dostęp do sieci komputerowej Agencji.

Bezpieczeństwo fizyczne i środowiskowe

1. **Strefa administracyjna** w ARIMR to powierzchnia będąca w użytkowaniu Agencji i służąca do poruszania się w niej tylko pracowników ARIMR.
2. Na granicach strefy administracyjnej funkcjonuje elektroniczna kontrola dostępu.
3. W Agencji wydzielono obszary dostaw i załadunku dla Wykonawców i jest to strefa obsługi dostępna ogólnie dla Wykonawców i beneficjentów ARIMR.
4. **Strefa bezpieczeństwa**
5. Pobyt osoby - Wykonawcy, która nie posiada uprawnień do przebywania w strefie bezpieczeństwa jest rejestrowany i może się odbywać tylko z osobą posiadającą uprawnienia do tej strefy.
6. Wszelkie prace w strefie bezpieczeństwa wykonywane zarówno przez podmioty nieuprawnione jak i uprawnione do przebywania w strefie bezpieczeństwa mogą się odbywać tylko przy ciągłej obecności osoby uprawnionej do tej strefy
7. Pobyt osoby, która nie posiada uprawnień do przebywania w strefie bezpieczeństwa, musi zostać odnotowany na podstawie dokumentu tożsamości.

Wykonywanie usługi – dostawy na terenie MzOR/BP

1. Wykonawca może poruszać się w strefie obsługi i strefie administracyjnej (w obecności uprawnionego pracownika ARIMR), w godzinach: **730-1530 PN-PT**.
2. Wszystkie osoby przebywające w strefie administracyjnej muszą posiadać identyfikatory noszone w widocznym miejscu. Wykonawcy posiadają identyfikatory z napisem „Gość” i numerem identyfikatora, w które zostaną zaopatrzeni przez ochronę obiektu MzOR lub upoważnionego pracownika w BP.
3. Wejście osoby – firmy zewnętrznej (administrator obiektu, serwisant, dostawca, firma wykonująca remont, usługę, dostawę) po godzinach pracy MzOR/BP na teren obiektu jest możliwe jedynie z upoważnionym pracownikiem MzOR/BP i po wcześniejszym pisemnym wystąpieniu o zgodę na wejście na teren obiektu MzOR/BP.
4. Zgodę na wejście w/w na teren MzOR/BP w formie pisemnej wyraża Administrator Zabezpieczeń Fizycznych i Środowiskowych MzOR/BP.
5. Merytoryczny pracownik MzOR/BP odpowiada za pobyt Wykonawcy od momentu wejścia na teren obiektu i przez cały czas wykonywanych przez niego prac, aż do momentu opuszczenia przez niego MzOR/BP. Wychodząc z siedziby MzOR /BP, Wykonawca obowiązany jest do zwrotu identyfikatora, a pracownik recepcji**-**ochrony lub upoważniony pracownik BP potwierdza w Książce ruchu osobowego **godzinę opuszczenia MzOR ARIMR.**

Naruszenie bezpieczeństwa informacji

1. Naruszenie postanowień Polityki Bezpieczeństwa Informacji przez Wykonawcę stanowi podstawę do odstąpienia przez Agencję od Umowy i żądania pokrycia powstałej szkody lub zapłaty kary umownej, jeżeli taki obowiązek wynika z zawartej Umowy.
2. Naruszenie przepisów bezpieczeństwa informacji oraz o ochronie danych osobowych jest zagrożone sankcjami karnymi określonymi w Ustawie z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. 2018 r. Nr 101 poz. 1000 z późn. zm.); w Rozporządzeniu 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) oraz w Kodeksie karnym.