Załącznik nr 7

WYTYCZNE
BEZPIECZEŃSTWA INFORMACJI DLA KONTRAHENTÓW I OSÓB ZEWNĘTRZNYCH

(zbiór zasad regulujących działania kontrahentów, realizujących dostawy lub świadczących usługi na rzecz ARR oraz wszystkie osoby spoza ARR, które wnioskują o dostęp do zasobów informacyjnych Agencji Rynku Rolnego na podstawie odrębnych przepisów lub umów m.in. pracowników serwisu, zewnętrznych audytorów i kontrolerów, konsultantów i programistów)

WERSJA: 3

Wytyczne Bezpieczeństwa Informacji obowiązują wszystkich kontrahentów, jednostki zewnętrzne i ich pracowników, o ile w trakcie realizacji umowy otrzymują dostęp do zasobów informacyjnych ARR.

Istotne naruszenie postanowień PBI przez osobę fizyczną zatrudniona na podstawie umowy- zlecenia lub umowy o dzieło skutkuje natychmiastowym rozwiązaniem umowy i stanowi podstawę do żądania pokrycia powstałej szkody lub zapłaty kary umownej, jeżeli taki obowiązek wynika z zawartej umowy.

Istotne naruszenie postanowień Polityki Bezpieczeństwa Informacji przez kontrahenta stanowi podstawę od odstąpienia przez ARR od umowy i żądania pokrycia powstałej szkody lub zapłaty kary umownej, jeżeli taki obowiązek wynika z zawartej umowy.

Odpowiedzialność za bezpieczeństwo informacji ARR obejmuje nie tylko siedzibę ARR, ale także wszelkie sytuacje, w których informacje związane z działalnością ARR są przetwarzane poza jej siedzibą. Obejmuje to w szczególności zdalny dostęp do sieci komputerowej ARR.

BEZPIECZEŃSTWO FIZYCZNE I ŚRODOWISKOWE

1. Powierzchnia biurowa zajmowana przez ARR jest dzielona na:
   a) strefy administracyjne,
   b) strefy bezpieczeństwa.
2. Strefa administracyjna to powierzchnia będąca w użytkowaniu ARR.
3. Na granicach strefy administracyjnej funkcjonuje elektroniczna kontrola dostępu
4. W ARR nie wydzielono obszary dostaw i załadunku. Dostęp do pomieszczeń magazynowych jest nadzorowany, prowadzona jest kontrola ruchu osobowego i materiałowego.
5. Strefa bezpieczeństwa to wydzielona część strefy administracyjnej wyposażona w dodatkowe, niezależne systemy zabezpieczeń.
6. Wstęp do strefy bezpieczeństwa jest ograniczony tylko do osób, które uzyskały stosowne uprawnienia.
7. Wejście oraz wyjście ze stref bezpieczeństwa jest rejestrowane. Rejestruje się tożsamość osób oraz czas ich wejścia i wyjścia.
8. Wnoszenie i wynoszenie do i ze stref bezpieczeństwa elektronicznych nośników informacji może mieć miejsce tylko w przypadkach wynikających z procedur eksploatacji zainstalowanego tam sprzętu informatycznego i podlega rejestracji.
9. W strefach bezpieczeństwa zabronione jest korzystanie z urządzeń fotograficznych, wideo, audio lub innych urządzeń nagrywających, np. kamer w urządzeniach przenośnych w celu rejestracji obrazu i/lub dźwięku bez upoważnienia Dyrektora BT.
10. Dopuszcza się przebywanie osób bez uprawnień dostępu do stref bezpieczeństwa tylko w wyjątkowych przypadkach, w określonym celu, w

Centrali za zezwoleniem osób odpowiedzialnych za nadzór nad poszczególnymi strefami, w OT ARR - dyrektora OT ARR. Przebywanie osób bez uprawnień dostępu do stref bezpieczeństwa możliwe jest wyłącznie pod nadzorem osoby posiadającej uprawnienia dostępu do danej strefy.

11. Pobyt osoby, która nie posiada uprawnień do przebywania w strefie bezpieczeństwa, musi zostać odnotowany przez osobę wprowadzającą w specjalnym rejestrze.
12. Ciągi komunikacyjne obiektów są zaopatrzone w tabliczki informujące o kierunku ewakuacji i w miarę potrzeby wyposażone w oświetlenie awaryjne. Zgodnie z przepisami prawa opracowane są instrukcje przeciwpożarowe.

ZARZĄDZANIE SYSTEMAMI I SIECIAMI

Dostęp do zasobów systemów informatycznych.

1. Do systemów informatycznych ARR mogą uzyskać dostęp wyłącznie uprawnieni użytkownicy.
2. Osoby niebędące pracownikami ARR nie mogą uzyskać profilu użytkownika ani uprawnień w zakresie korzystania z systemów informatycznych ARR bez uprzedniej, pisemnej zgody Gestora. Nie dotyczy to organów umocowanych prawnie.
3. Uprawnienia użytkowników niebędących pracownikami ARR nie mogą być przyznane na czas nieokreślony i muszą podlegać aktualizacji co 90 dni.
4. Warunki korzystania z połączenia wewnętrznej sieci ARR z systemami zewnętrznymi regulują podpisane umowy, szczegółowo precyzujące warunki techniczne i funkcjonalne połączenia. Umowa musi zawierać klauzulę dotyczącą przestrzegania zasad bezpieczeństwa systemów informacyjnych ARR.
5. Osoby mające dostęp do systemów informatycznych ARR a niebędące pracownikami ARR muszą podpisać zobowiązanie, że będą przestrzegać zasad opisanych w *Wytycznych bezpieczeństwa informacji dla kontrahentów.*

Dostęp do zasobów ARR z sieci innych instytucji.

1. ARR może umożliwić dostęp do sieci informatycznej osobom i podmiotom uprawnionym na mocy przepisów prawa.
2. Wniosek o dostęp do sieci ARR powinien zawierać informacje o celu podłączenia, przewidywanej liczbie podłączonych stanowisk i użytkowników, metodzie zabezpieczenia przed nieautoryzowanym dostępem.
3. Przed wydaniem decyzji o zgodzie na podłączenie do sieci ARR Prezes ARR zasięga opinii Komitetu Sterującego Bezpieczeństwa Informacji.
4. Specyfikacja techniczna połączenia musi być załącznikiem do porozumienia lub umowy zawartej pomiędzy ARR i instytucjami. Specyfikacja powinna zawierać w szczególności następujące ustalenia:

a) połączenie powinno być zaszyfrowane oraz zabezpieczone odpowiednim certyfikatem,

b) połączenie powinno być zestawiane jedynie miedzy ściśle określonymi adresami IP podłączonej sieci oraz ściśle określonymi adresami IP sieci wewnętrznej ARR oraz dla ściśle określonych portów przypisanych do adresów w sieci ARR,

c) każdorazowe zestawienie połączenia między podłączaną siecią a siecią ARR powinno być autoryzowane hasłem lub certyfikatem oraz logowane,

d) zasoby udostępniane użytkownikom z innych instytucji obejmują tylko i wyłącznie dostęp do aplikacji. Nie są udostępniane takie zasoby jak serwery plików lub poczta elektroniczna.

5. Użytkownicy z innych instytucji nie mogą posiadać praw administracyjnych.

Ochrona przed szkodliwym oprogramowaniem i kodem mobilnym.

1. Wszystkie elektroniczne nośniki informacji dostarczone z zewnątrz ARR nie mogą być użyte bez wcześniejszego sprawdzenia oprogramowaniem antywirusowym.
2. Wszystkie pliki przed wysłaniem lub przekazaniem stronom trzecim (osobom niebędącym pracownikami ARR), są testowane oprogramowaniem antywirusowym.

Odbiór systemu.

1. Przed przekazaniem do użytkowania oprogramowania opracowanego w ARR, osoby je opracowujące muszą usunąć wszystkie specjalne ścieżki dostępu tak, aby dostęp był możliwy jedynie z zastosowaniem zasad bezpieczeństwa ARR. Oznacza to, że muszą być usunięte wszystkie nieudokumentowane funkcje pozwalające ominąć system zabezpieczeń. Muszą zostać również usunięte wszystkie uprawnienia systemowe ustanowione dla potrzeb prowadzenia prac nad oprogramowaniem, lecz zbędne w środowisku produkcyjnym.
2. W przypadku podjęcia decyzji o przechowywaniu kodu źródłowego pisanego na zamówienie ARR poza siedzibą ARR, konieczne jest również zawarcie umów depozytowych dotyczących takiego kodu źródłowego z podmiotami niezależnymi od dostawcy oprogramowania (code escrow). Umowy te powinny określać niezależny podmiot, któremu twórca oprogramowania dostarczy kod źródłowy i wszystkie jego aktualizacje. Powinny też określać sytuacje, w których kod źródłowy zostanie udostępniony ARR, jak na przykład upadłość lub likwidacja dostawcy oprogramowania lub niewywiązywanie się przez niego z postanowień umowy dotyczących aktualizacji oprogramowania.

Naruszenie bezpieczeństwa informacji.

1. Za naruszenie bezpieczeństwa informacji uważa się, w szczególności:
   a) naruszenie lub próby naruszenia integralności systemu przeznaczonego do przetwarzania informacji;
   b) naruszenie lub próby naruszenia integralności informacji w systemie przetwarzania - wszelkie modyfikacje (dodanie, zmiana, usunięcie), zniszczenie lub próby ich dokonania przez osoby nieupoważnione lub upoważnione działające w złej wierze lub jako błąd osoby uprawnionej (np. zmiana zawartości danych, utrata całości lub części danych);
   c) naruszenie poufności poprzez celowe lub nieświadome przekazanie informacji osobie nieuprawnionej do ich otrzymania;
   d) naruszenie ochrony informacji w systemie (np. nieautoryzowane logowanie do systemu lub inny objaw wskazujący na próbę lub działanie związane z nielegalnym dostępem do systemu z zewnątrz, skutkujące dostępem do informacji, do których dostęp nie powinien być możliwy);
   e) nieuprawniony dostęp lub próba dostępu do systemu przetwarzania informacji (np. nieuprawniona praca na koncie użytkownika);
   f) umożliwienie dostępu do informacji osobie nieuprawnionej; np.: pozostawienie kopii danych (w drukarce, ksero, na stole), nie zablokowanie dostępu do systemu (podczas nieobecności osoby uprawnionej), brak nadzoru nad serwisantami i innymi osobami nieuprawnionymi;
   g) nieuprawniony dostęp lub próba dostępu do pomieszczeń, gdzie przetwarza się informacje;
   h) ujawnienie indywidualnych haseł dostępu użytkowników do systemu przetwarzającego informacje;
   i) wykonanie nieuprawnionych kopii informacji lub wydruków;
   j) zmianę lub usunięcie informacji zapisanych na kopiach bezpieczeństwa lub kopiach archiwalnych;
   k) zamierzoną lub nie zamierzoną utratę poufności danych poprzez utratę: sprzętu mobilnego, klucza do podpisu elektronicznego, kopii bezpieczeństwa, nośnika danych lub innego składnika systemu informacyjnego ARR (w tym na skutek kradzieży) i niepodjęcie w stosownym czasie odpowiednich działań neutralizujących;
   l) brak nośnika zawierającego informacje - kradzież lub zaginięcie wydruku, kopii bezpieczeństwa, dyskietki czy dysku lub innego nośnika informacji.
   m) niewłaściwe niszczenie nośników informacji zawierających dane wrażliwe lub ustawowo chronione, umożliwiające ich odczyt - wyrzucanie niezniszczonych nośników (np.: wydruk, dyskietka);
   n) inne zdarzenia, które wskazują lub świadczą o naruszeniu bezpieczeństwa informacji.