WYTYCZNE BEZPIECZEŃSTWA INFORMACJI DLA KONTRAHENTÓW

WERSJA: 5.0

Zatwierdzone przez
Zastępcę Dyrektora
Biura Audytu i Bezpieczeństwa Informacji
w dniu 11 stycznia 2017 r.

Dokument opracowano na podstawie Zarządzenia Prezesa Agencji Rynku Rolnego (ARR) Nr 224/2016/W z dnia 27.10.2016 r. w sprawie wprowadzenia „Zasad zarządzania bezpieczeństwem informacji" w Agencji Rynku Rolnego z późn. zm.
Wnioski mające na celu podniesienie poziomu bezpieczeństwa informacji należy zgłaszać do Biura Audytu i Bezpieczeństwa Informacji (BAiBI).

1. *Wytyczne bezpieczeństwa informacji dla kontrahentów* stanowią zbiór zasad obowiązujących kontrahentów, którzy realizują dostawy lub świadczą usługi na rzecz ARR oraz osoby spoza ARR, które uzyskują dostęp do zasobów informacyjnych na podstawie odrębnych przepisów lub umów. *Wytyczne* załączane są do umów z kontrahentami, którzy zapoznają się z *Wytycznymi*, zobowiązując się do ich stosowania. Za aktualizację i zatwierdzenie dokumentu odpowiada Zastępca Dyrektora BAiBI, który jest właścicielem dokumentu.
2. Naruszenie zasad bezpieczeństwa informacji przez praktykanta może skutkować natychmiastowym przerwaniem praktyki i rozwiązaniem umowy. W takim przypadku praktyka nie jest zaliczana.
3. Naruszenie zasad bezpieczeństwa informacji przez stażystę może skutkować natychmiastowym przerwaniem stażu i powiadomieniem instytucji kierującej na staż.
4. Naruszenie zasad bezpieczeństwa informacji przez osobę fizyczną zatrudnioną na podstawie umowy zlecenia lub umowy o dzieło może skutkować natychmiastowym rozwiązaniem umowy i stanowi podstawę do żądania pokrycia powstałej szkody lub zapłaty kary umownej, jeżeli taki obowiązek wynika z zawartej umowy.
5. Naruszenie bezpieczeństwa informacji przez kontrahenta stanowi podstawę do odstąpienia przez ARR od umowy i żądania pokrycia ewentualnej szkody lub zapłaty kary umownej, jeżeli taki obowiązek wynika z zawartej umowy.
6. 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. W ARR wyróżnia się następujące obszary bezpieczne:
   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. 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. Wejście oraz wyjście ze stref bezpieczeństwa jest rejestrowane. Rejestruje się tożsamość osób oraz czas ich wejścia i wyjścia.

7. Wnoszenie i wynoszenie do i ze stref bezpieczeństwa elektronicznych nośników informacji jest nadzorowane.
8. W strefach bezpieczeństwa zabronione jest korzystanie z urządzeń fotograficznych, wideo, audio lub innych urządzeń nagrywających, np. kamer w urządzeniach przenośnych w celu rejestracji obrazu lub dźwięku bez upoważnienia Dyrektora Biura Teleinformatyki (BT).
9. 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 Oddziale Terenowym (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.
10. Pobyt osoby, która nie posiada uprawnień do przebywania w strefie bezpieczeństwa podlegającej Dyrektorowi BT, musi zostać odnotowany przez osobę wprowadzającą w rejestrze, zgodnie z Księgą Procedur *Zarządzanie teleinformatyką* [KP_ZIT].
11. 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.

Dostęp do zasobów systemów informatycznych

1. Dostęp do systemu informatycznego (SI) mogą uzyskać wyłącznie uprawnieni użytkownicy.
2. Osoby niebędące pracownikami ARR nie mogą uzyskać profilu użytkownika ani uprawnień w zakresie korzystania z SI 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 zewnętrznymi SI 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 SI, a niebędące pracownikami ARR, muszą podpisać zobowiązanie, że będą przestrzegać zasad opisanych w *Wytycznych bezpieczeństwa informacji dla kontrahentów*. Zobowiązanie to powstaje przy podpisaniu umowy, do której załącznik stanowią niniejsze *Wytyczne*.

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 (KSBI).
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 szyfrowane oraz zabezpieczone odpowiednim certyfikatem;
   b) połączenie powinno być zestawiane jedynie między ściśle określonymi adresami IP podłączanej 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 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 programem 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 na rzecz 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. 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.

Naruszenia bezpieczeństwa informacji

1. Pracownicy, wykonawcy i użytkownicy reprezentujący stronę trzecią korzystający z systemów informacyjnych są zobowiązani do zgłaszania zdarzeń, które wskazują lub świadczą o naruszeniu bezpieczeństwa informacji, do pracownika ARR nadzorującego ich działania.
2. Za naruszenie bezpieczeństwa informacji (incydent) 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 SI (np. nieautoryzowane logowanie do systemu lub inny objaw wskazujący na próbę lub działanie związane z nielegalnym dostępem do SI z zewnątrz, skutkujące dostępem do informacji, do których dostęp nie powinien być możliwy);
   e) nieuprawniony dostęp lub próba dostępu do SI (np. nieuprawniona praca na koncie użytkownika);
   f) umożliwienie dostępu do informacji osobie nieuprawnionej; np. pozostawienie kopii danych (w drukarce, ksero, na stole), niezablokowanie dostępu do SI (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 (lub haszy haseł) dostępu użytkowników do SI;
   i) wykonanie nieuprawnionych kopii informacji lub wydruków;
   j) niewykonywanie kopii bezpieczeństwa;
   k) zmianę lub usunięcie informacji zapisanych na kopiach bezpieczeństwa lub kopiach archiwalnych;
   l) zamierzoną lub niezamierzoną 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;
   m) brak nośnika zawierającego informacje - kradzież lub zaginięcie wydruku, kopii bezpieczeństwa, dysku lub innego nośnika informacji;
   n) niewłaściwe niszczenie nośników informacji zawierających dane wrażliwe lub ustawowo chronione, umożliwiające ich odczyt - wyrzucanie niezniszczonych nośników (np.: wydruk, płyta CD/DVD);
   o) błędne (nadmierne) nadanie uprawnień do przetwarzania informacji lub nadanie uprawnień osobie niespełniającej wymagań;
   p) inne zdarzenia, które wskazują lub świadczą o naruszeniu bezpieczeństwa informacji.

Prawo do własności intelektualnej

W przypadku tworzenia dóbr intelektualnych na zlecenie ARR, w umowie z wykonawcą umieszcza się zapis o przekazaniu praw autorskich do dzieła.