Załącznik Nr 2 do Zapytania Ofertowego

Wytyczne Bezpieczeństwa Informacji dla Wykonawców

realizujących umowy na rzecz Pomorskiego Oddziału Regionalnego ARiMR z siedzibą w Gdyni, opracowane na podstawie Zarządzenia Nr 51/2024 Prezesa Agencji Restrukturyzacji i Modernizacji Rolnictwa z dnia 23 maja 2024 r. w sprawie bezpieczeństwa informacji w ARiMR

1. W ARiMR obowiązuje Zarządzenie Nr 51/2024 Prezesa ARiMR z dnia 23 maja 2024 r. w sprawie bezpieczeństwa informacji w ARiMR określające politykę bezpieczeństwa informacji w ARiMR (PBI).
2. Zarządzenie Nr 51/2024 Prezesa ARiMR dotyczy zasobów materialnych i niematerialnych Agencji i znajduje zastosowanie zarówno do pracowników Agencji, jak i podmiotów zewnętrznych z nią współpracujących.
3. W przypadku, kiedy w trakcie realizacji umowy, Wykonawca lub wskazana przez Wykonawcę osoba otrzyma dostęp do Lokalu zajmowanego przez Zamawiającego, Wykonawca, lub wskazana przez Niego osoba/osoby, są zobowiązani do przestrzegania przyjętych w ARiMR zasad bezpieczeństwa informacji, określony w niniejszym załączniku (stanowiących wybrane wymagania z PBI ARiMR).
4. Podstawowe pojęcia:
1) dane osobowe – dane określone w przepisach o ochronie danych osobowych,
2) incydent związany z bezpieczeństwem informacji – pojedyncze zdarzenie lub serię niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia realizacji zadań ustawowych bądź statutowych Agencji lub zagrażają bezpieczeństwu informacji,
3) informacja wrażliwa – 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,
4) przetwarzanie informacji/danych – jakiekolwiek operacje na informacji/danych, takie jak zbieranie, wytwarzanie, opracowywanie, zmienianie, przechowywanie, udostępnianie, kopiowanie, przekazywanie, archiwizowanie, usuwanie, zarówno w formie papierowej, jak i w systemach teleinformatycznych.
5. W Agencji ochronie podlega w szczególności:
1) życie i zdrowie pracowników,
2) przetwarzane informacje, niezależnie od ich formy i nośnika, na którym zostały utrwalone,
3) sprzęt oraz programy komputerowe wykorzystywane do przetwarzania, przesyłania i przechowywania informacji,
4) pomieszczenia, w których usytuowano sprzęt teleinformatyczny, a także te, w których przetwarza się informacje wrażliwe,
5) wizerunek Agencji i relacje z podmiotami zewnętrznymi, współpracującymi z Agencją.
6. Wszystkie informacje wrażliwe i środki służące do ich przetwarzania, będące własnością Agencji lub przez nią wykorzystywane, podlegają ochronie.
7. Do informacji wrażliwych w Agencji zalicza się w szczególności:
1) dane osobowe, informacje niejawne, informacje zawierające tajemnicę skarbową, bankową, itp.,
2) dokumentację techniczną systemów teleinformatycznych oraz systemów zabezpieczeń fizycznych i logicznych, w tym kody źródłowe aplikacji oraz procedury bezpieczeństwa na poziomie technologicznym,
3) wyniki typowania producentów rolnych do kontroli na miejscu,
4) wykaz obszarów przeznaczonych do kontroli metodą foto,
5) raporty z audytu i kontroli,

6) instrukcje do negocjacji w sprawie zawierania umów, których ujawnienie mogłoby mieć niekorzystny wpływ na dalszy tok negocjacji dla Agencji,
7) informacje przekazywane Agencji przez podmiot zewnętrzny w wyniku realizacji umowy, o ile podmiot zewnętrzny wskaże konieczność ochrony takich informacji w treści umowy lub w dokumentach stanowiących produkty realizacji umowy,
8) inne informacje, których udostępnienie osobie nieuprawnionej w ocenie Właściciela Zasobu mogłoby spowodować szkody dla Agencji lub naruszyć prawnie chroniony interes innych osób/podmiotów.
8. Powierzchnie zajmowana przez jednostki organizacyjne, podzielona jest na strefy:
a) strefę administracyjną - do której dostęp posiadają wszyscy pracownicy Agencji.
b) strefę bezpieczeństwa – wydzielona część w strefie administracyjnej lub poza strefą administracyjną (np. serwerownia, składnica akt), do których dostęp jest ograniczony do osób posiadających specjalne prawa dostępu.
c) strefę obsługi klienta – wydzielona część strefy administracyjnej, w której odbywa się obsługa interesantów, którzy mogą przebywać w tej strefie bez identyfikatorów. Strefa obsługi klienta musi być oddzielona od pozostałych części strefy administracyjnej kontrolowanymi przejściami.
9. Na granicy strefy administracyjnej odbywa się kontrola ruchu osobowego i materiałowego.
10. Wszystkie osoby przebywające w strefie administracyjnej muszą posiadać identyfikatory noszone w widocznym miejscu. Pracownicy Agencji posiadają identyfikatory zawierające: zdjęcie, imię i nazwisko, symbol lub nazwę jednostki organizacyjnej lub komórki organizacyjnej. Goście posiadają identyfikatory z napisem „Gość" i numerem identyfikatora.
11. Goście mogą poruszać się w obrębie strefy administracyjnej wyłącznie w asyście pracownika odpowiedzialnego za ich przyjęcie. Pracownik ten przed wprowadzeniem gości do strefy administracyjnej winien dopilnować pobrania przez nich w strefie obsługi klienta lub na stanowisku recepcyjnym identyfikatorów, o których mowa w punkcie 10.
12. Kontrolę ruchu osobowego i materiałowego na granicy strefy administracyjnej może sprawować pracownik ze strefy obsługi klienta lub stanowiska recepcyjnego, który wydaje identyfikatory gościom oraz jest zobowiązany do dopilnowania ich zwrotu.
13. Wstęp do poszczególnych stref, o których mowa w pkt. 8 ppkt. a) i b) jest ograniczony tylko do tych osób, które uzyskały stosowne uprawnienia.
14. W strefach bezpieczeństwa dopuszcza się przebywanie osób bez uprawnień dostępu do tych stref tylko w wyjątkowych przypadkach, za zezwoleniem kierownika danej jednostki organizacyjnej.
15. Pobyt osoby, która nie posiada uprawnień do przebywania w strefie bezpieczeństwa jest rejestrowany. Za prowadzenie rejestru odpowiedzialny jest kierownik danej jednostki organizacyjnej, a wpisy dokonywane są pod nadzorem osoby uprawnionej do przebywania w danej strefie.
16. 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.
17. Zabronione jest wnoszenie do stref bezpieczeństwa urządzeń służących rejestracji dźwięku i obrazu.
18. 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 bezpieczeństwa pożarowego.
19. Za naruszenie bezpieczeństwa informacji uważa się w szczególności:
a) naruszenie lub próby naruszenia integralności systemu przeznaczonego do przetwarzania informacji; Pomorski Oddział Regionalny ARiMR, ul. Kołłątaja 1, 81-332 Gdynia
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);

e) nieuprawniony dostęp lub próba dostępu do systemu przetwarzania informacji;
f) umożliwienie dostępu do informacji osobie nieuprawnionej;
g) nieuprawniony dostęp lub próba dostępu do pomieszczeń, gdzie przetwarza się informacje;
h) wykonanie nieuprawnionych kopii informacji – wydruki, kopie na dyskietkach itp.;
i) zamierzona lub nie zamierzona utrata poufności danych poprzez utratę: sprzętu mobilnego, klucza do podpisu elektronicznego, kopii bezpieczeństwa, nośnika danych lub innego składnika systemu informacyjnego ARiMR (w tym na skutek kradzieży);
j) brak nośnika zawierającego informacje – kradzież lub zaginięcie wydruku, kopii bezpieczeństwa, dyskietki czy dysku;
k) inne sytuacje, które wskazują lub potwierdzają naruszenie bezpieczeństwa informacji w ARiMR.

....
(miejscowość, data) (podpis i pieczęć osoby upoważnionej)