

## ANKIETA OCENY BEZPIECZEŃSTWA WYKONAWCY

Nazwa Wykonawcy (dostawcy):

Przedmiot umowy:

NIP / KRS:

Nr umowy (jeśli dotyczy):

Adres siedziby:

Kategoria dostawcy:

Osoba kontaktowa:

Oceniający (TW):

Data wypełnienia:

Podpis dostawcy:

Lp.	Pytanie do dostawcy	Odpowiedź dostawcy	Ocena TW (T/N/ND/Cz)	Uwagi / dowody
I. INFORMACJE OGÓLNE O DOSTAWCY				
1	Proszę opisać profil działalności firmy, liczbę pracowników, główne rynki, na których Wykonawca działa, strukturę zatrudnienia w działach powiązanych z IT, poziom doświadczenia kluczowego personelu, rodzaj zawieranych umów z personelem.			
2	Czy Wykonawca korzysta z poddostawców przy realizacji usług objętych potencjalną umową? Jeśli tak — proszę wskazać zakres i dane poddostawców.			

3	Czy Wykonawca lub jego poddostawcy mają siedziby w państwach innych niż państwa członkowskie Unii Europejskiej lub państwa objęte Porozumieniem Światowej Organizacji Handlu w sprawie zamówień rządowych (EOG) lub objęte innymi umowami międzynarodowymi, których stroną jest Unia Europejska, gwarantującymi na zasadzie wzajemności i równości dostęp do rynku zamówień publicznych Jeśli tak — proszę wskazać lokalizacje.			
4	Czy Wykonawca wchodzi w skład grupy kapitałowej? Jeśli tak — proszę podać strukturę własnościową.			

## II. SYSTEM ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI

5	Czy Wykonawca posiada certyfikację np. ISO 27001, ISO 22301, ISO 9001, SOC 2? Jeśli tak — proszę podać zakres certyfikacji, datę ważności i jednostkę certyfikującą.			<i>(okazanie certyfikatów)</i>
6	Czy Wykonawca posiada wdrożony system zarządzania bezpieczeństwem informacji (SZBI)? Proszę opisać jego zakres.			<i>(okazanie polityki bezpieczeństwa informacji)</i>
7	Czy Wykonawca prowadzi systematyczne szacowanie ryzyka bezpieczeństwa informacji? Jaka metodyka jest stosowana?			<i>(okazanie procedury zarządzania ryzykiem oraz ostatniej oceny ryzyka dotyczącej przedmiotu Umowy)</i>
8	Czy Wykonawca przeprowadza wewnętrzne audyty bezpieczeństwa informacji? Jak często?			<i>(okazanie dowodów z dwóch ostatnich audytów)</i>
9	Czy Wykonawca posiada niezależne sprawozdania z audytu bezpieczeństwa sporządzone przez osobę trzecią?			<i>(okazanie sprawozdania)</i>

## III. KONTROLA DOSTĘPU I ZARZĄDZANIE TOŻSAMOŚCIĄ

10	W jaki sposób Wykonawca zarządza dostępem do systemów informacyjnych i danych? Czy stosowane jest uwierzytelnianie wieloskładnikowe (MFA)?			<i>(okazanie polityki lub procedury zarządzania dostępami, ewentualnie polityki MFA, jeśli stanowi ona odrębny dokument lub innego dokumentu regulującego tą kwestię)</i>
11	Czy Wykonawca stosuje zasadę najmniejszych uprawnień, i rozdziału obowiązków? Czy każdy dostęp jest rejestrowany, monitorowany i możliwy do odtworzenia?			<i>(okazanie procedury zarządzania dostępami lub innego dokumentu regulującego tą kwestię)</i>
12	W jaki sposób Wykonawca zarządza kontami uprzywilejowanymi (administratorskimi)?			<i>(okazanie procedury zarządzania dostępami lub innego dokumentu regulującego tą kwestię)</i>
13	Czy Wykonawca posiada procedurę nadawania, modyfikacji i odbierania uprawnień dostępowych? Jak szybko następuje dezaktywacja kont po zakończeniu współpracy? Czy stosowana jest blokada konta i w jakich sytuacjach?			<i>(okazanie procedury zarządzania dostępami lub innego dokumentu regulującego tą kwestię)</i>
14	Czy Wykonawca stosuje szyfrowanie danych w spoczynku i w transmisji? Jakie algorytmy i protokoły są używane?			<i>(okazanie procedury zarządzania kryptografią i szyfrowaniem lub innego dokumentu regulującego tą kwestię)</i>
15	Czy stosowana jest okresowa zmiana haseł, a jeśli tak, to z jaką częstotliwością? Czy system blokuje możliwość ponownego użycia tych samych haseł?			<i>(okazanie polityki haseł lub innego dokumentu regulującego tą kwestię)</i>
16	Jakie zasady budowania haseł stosuje Wykonawca? Czy Wykonawca korzysta z profesjonalnych rozwiązań typu Enterprise Password Manager lub PAM (Privileged Access Management) do bezpiecznego przechowywania haseł technicznych i współdzielonych?			<i>(okazanie polityki haseł lub innego dokumentu regulującego tą kwestię)</i>

#### IV. BEZPIECZEŃSTWO SIECI I INFRASTRUKTURY

17	Czy Wykonawca stosuje segmentację sieci i separację środowisk (produkcja, test, rozwój)?			<i>(okazanie polityki/procedury zarządzania siecią oraz bezpiecznego rozwoju oprogramowania lub innego dokumentu regulującego tą kwestię)</i>
18	W jaki sposób Wykonawca zabezpiecza połączenia sieciowe z klientami (VPN, dedykowane łącza, szyfrowanie end-to-end)?			<i>(okazanie polityki/procedury zarządzania siecią lub innego dokumentu regulującego tą kwestię)</i>
19	Czy Wykonawca prowadzi monitoring bezpieczeństwa sieci (IDS/IPS, SIEM, SOC)? Proszę opisać.			<i>(okazanie procedury rejestrowania i monitorowania lub innego dokumentu regulującego tą kwestię)</i>
20	W jaki sposób Wykonawca zarządza konfiguracją i hardeningiem systemów?			<i>(okazanie procedury zarządzania konfiguracją lub innego dokumentu regulującego tą kwestię)</i>
21	Czy Wykonawca stosuje filtrowanie ruchu webowego i ochronę przed atakami DDoS?			<i>(okazanie procedury rejestrowania i monitorowania lub innego dokumentu regulującego tą kwestię)</i>
22	Jakie zasady zarządzania środowiskiem chmurowym stosuje Wykonawca?			<i>(okazanie procedury zarządzania środowiskiem chmurowym lub innego dokumentu regulującego tą kwestię)</i>

#### V. ZARZĄDZANIE PODATNOŚCIAMI I AKTUALIZACJAMI

23	Czy Wykonawca prowadzi regularne skanowanie podatności i testy bezpieczeństwa, w tym testy penetracyjne? Jak często?			<i>(okazanie wyników dwóch ostatnich testów i skanowań)</i>
24	W jaki sposób Wykonawca zarządza wykrytymi podatnościami? Jaki jest średni czas usunięcia podatności krytycznej? Czy dostawca posiada formalny proces priorytetyzacji podatności według krytyczności i wpływu na klienta?			<i>(okazanie procedury zarządzania podatnościami lub innego dokumentu regulującego tą kwestię)</i>
25	Czy Wykonawca posiada proces zarządzania aktualizacjami i poprawkami bezpieczeństwa (patch management)? Czy poprawki i aktualizacje są pobierane wyłącznie z zaufanych źródeł? Czy dostawca prowadzi ewidencję wyjątków od terminowego wdrożenia poprawek bezpieczeństwa?			<i>(okazanie procedury zarządzania aktualizacjami i poprawkami, procedurę wyjątków lub innego dokumentu regulującego tą kwestię)</i>

26	Czy w ciągu ostatnich 24 miesięcy wykryto podatności krytyczne w produktach/usługach oferowanych przez firmę? Jeśli tak — jak zostały obsłużone?			(dowody wykrycia podatności, dowody obsługi podatności)
VI. ZARZĄDZANIE INCYDENTAMI BEZPIECZEŃSTWA				
27	Czy Wykonawca posiada udokumentowaną procedurę zarządzania incydentami bezpieczeństwa informacji? Czy procedura incydentowa określa role, odpowiedzialności, ścieżki eskalacji i zasady komunikacji kryzysowej?			(okazanie procedury zarządzania incydentami bezpieczeństwa lub innego dokumentu regulującego tą kwestię)
28	W jaki sposób Wykonawca zapewnia niezwłoczne powiadamianie klientów o incydentach bezpieczeństwa? Jaki jest gwarantowany czas notyfikacji?			(okazanie procedury zarządzania incydentami bezpieczeństwa lub innego dokumentu regulującego tą kwestię)
29	Czy w ciągu ostatnich 24 miesięcy wystąpiły incydenty bezpieczeństwa mające wpływ na dane lub usługi klientów? Jeśli tak — proszę opisać.			(okazanie opisu stwierdzonych incydentów)
30	Czy Wykonawca posiada zespół reagowania na incydenty (CSIRT/SOC) lub korzysta z usług zewnętrznego SOC? Jeśli zewnętrzny podmiot - wskazać jaki.			
31	Czy Wykonawca dokumentuje wnioski z incydentów i wdraża działania korygujące (lessons learned)?			(okazanie raportów z dwóch incydentów, rejestr incydentów lub innego dokumentu regulującego tą kwestię)
VII. CIĄGŁOŚĆ DZIAŁANIA I STRATEGIA WYJŚCIA				
32	Czy Wykonawca posiada plan ciągłości działania (BCP) i plan odtworzenia po awarii (DRP)?			(okazanie polityki/procedury BCP i DRP lub innego dokumentu regulującego tą kwestię)
33	Jak często Wykonawca testuje plany ciągłości działania? Kiedy odbyły się ostatnie testy?			(okazanie raportów z dwóch ostatnich testów)
34	Czy Wykonawca jest w stanie zapewnić bezpieczne przekazanie danych i dokumentacji do Zamawiającego lub nowego dostawcy w przypadku zakończenia współpracy?			

35	Czy Wykonawca gwarantuje bezpieczne usunięcie/zniszczenie/zwrot danych Zamawiającego po zakończeniu umowy? W jaki sposób następuje trwałe usunięcie? W jaki sposób kwestia usunięcia/zniszczenia/zwrotu została uregulowana z dostawcami Wykonawcy?			(okazanie umów z poddostawcami)
36	Czy są wykonywane kopie zapasowe? Czy są przechowywane w bezpiecznej lokalizacji? Czy przywracania danych z kopii zapasowych jest regularnie testowane o dokumentowane?			(okazanie polityki zarządzania kopiami zapasowymi ub innego dokumentu regulującego tą kwestię, wyników z dwóch ostatnich testów)
VIII. BEZPIECZEŃSTWO ŁAŃCUCHA DOSTAW				
37	W jaki sposób Wykonawca weryfikuje bezpieczeństwo swoich własnych dostawców (łańcuch dostaw)? Czy prowadzi regularne audyty? Jeśli tak — w jakich okresach?			(okazanie polityki zarządzania dostawcami ub innego dokumentu regulującego tą kwestię, wyniki z dwóch ostatnich audytów)
38	Czy Wykonawca jest uprawniony do żądania od swoich dostawców spełnienia wymagań bezpieczeństwa co najmniej równoważnych z wymaganiami stawianymi przez Zamawiającego?			(okazanie umów z poddostawcami)
39	Czy Wykonawca lub jego dostawcy podlegają jurysdykcji państw spoza UE/EOG, mogącej wpływać na bezpieczeństwo danych?			(okazanie umów z poddostawcami)
40	Czy Wykonawca posiada strategię dywersyfikacji dostawców, ograniczającą ryzyko koncentracji?			(okazanie polityki zarządzania dostawcami lub innego dokumentu regulującego tą kwestię)
IX. BEZPIECZEŃSTWO ROZWOJU OPROGRAMOWANIA I ZMIAN				
41	Czy Wykonawca stosuje zasady bezpiecznego cyklu rozwoju oprogramowania (SSDLC)? Proszę opisać.			(okazanie procedury SSDLC lub innego dokumentu regulującego tą kwestię)

42	Czy Wykonawca korzysta z programów narzędziowych, które umożliwiają obejście zabezpieczeń systemów i aplikacji? Czy podlega to kontroli? Jeśli tak — jakiej?			<i>(okazanie procedury używania uprzywilejowanych programów narzędziowych lub innego dokumentu regulującego tą kwestię)</i>
43	Jakie procedury i środki Wykonawca wdrożył w celu bezpiecznego zarządzania instalacją oprogramowania w systemach operacyjnych?			<i>(okazanie procedury zarządzania oprogramowaniem, procedury zarządzania aktywami lub innego dokumentu regulującego tą kwestię)</i>
44	Czy w procesie tworzenia lub zakupu oprogramowania uwzględnia się identyfikację, określenie i zatwierdzenie wymagań bezpieczeństwa informacji?			<i>(okazanie procedury zarządzania oprogramowaniem, procedury zarządzania aktywami lub innego dokumentu regulującego tą kwestię)</i>
45	Czy Wykonawca przeprowadza przeglądy kodu i testy bezpieczeństwa aplikacji (SAST/DAST) przed wdrożeniem? Jakie zasady bezpiecznego kodowania stosuje Wykonawca przy opracowywaniu oprogramowania?			<i>(okazanie procedury zarządzania oprogramowaniem, procedury zarządzania aktywami lub innego dokumentu regulującego tą kwestię, wyniki SAST/DAST)</i>
46	Czy środowiska testowe i deweloperskie są oddzielone od środowiska produkcyjnego? Czy procesy testowania bezpieczeństwa są zdefiniowane i wdrożone w cyklu rozwojowym?			<i>(okazanie procedury zarządzania oprogramowaniem, procedury zarządzania aktywami lub innego dokumentu regulującego tą kwestię)</i>
47	Czy Wykonawca monitoruje i przegląda prace rozwojowe nad oprogramowaniem zlecone na zewnątrz?			<i>(okazanie procedury zarządzania oprogramowaniem, procedury zarządzania aktywami lub innego dokumentu regulującego tą kwestię)</i>
48	Czy Wykonawca posiada proces zarządzania zmianami (change management) zapewniający kontrolowaną modyfikację systemów?			<i>(okazanie procedury zarządzania zmianą lub innego dokumentu regulującego tą kwestię)</i>
49	Czy Wykonawca chroni i nadzoruje dane testowe?			<i>(okazanie polityki bezpiecznego kodowania lub innego dokumentu regulującego tą kwestię)</i>
50	Czy Wykonawca prowadzi testy i inne działania obejmujące ocenę systemów operacyjnych. Czy testy są zaplanowane i uzgodnione między testerem a odpowiednim kierownictwem?			<i>(okazanie wyników testów)</i>

51	W jaki sposób jest przetrzymywany kod źródłowy do oprogramowania dostarczanego w ramach Umowy? Jakie procedury deponowania, odtwarzania oraz dostępu są stosowane?			(okazanie procedury bezpiecznego kodowania lub innego dokumentu regulującego tą kwestię)
52	Czy i jakie techniki maskowania danych są wykorzystywane?			(okazanie polityki maskowania danych lub innego dokumentu regulującego tą kwestię)

#### X. BEZPIECZEŃSTWO FIZYCZNE

53	Czy lokalizacje, w których przetwarzane są dane klienta, posiadają fizyczną kontrolę dostępu (karty, biometria, monitoring CCTV)?			(okazanie polityki bezpieczeństwa fizycznego lub innego dokumentu regulującego tą kwestię)
54	Czy Wykonawca wydzielił obszary bezpieczne i wdrożył środki bezpieczeństwa? Jakież?			(okazanie polityki bezpieczeństwa fizycznego lub innego dokumentu regulującego tą kwestię)
55	W jaki sposób Wykonawca zabezpiecza sprzęt IT zawierający dane klientów (serwery, nośniki danych)?			(okazanie polityki bezpieczeństwa fizycznego, procedury zarządzania nośnikami lub innego dokumentu regulującego tą kwestię)
56	Czy Wykonawca posiada procedurę bezpiecznego usuwania danych z nośników i utylizacji sprzętu?			(okazanie polityki usuwania i niszczenia informacji, polityki retencji (okazanie polityki bezpieczeństwa fizycznego lub innego dokumentu regulującego tą kwestię)
57	Czy centra danych Wykonawcy posiadają certyfikacje (np. Tier III/IV, EN 50600)? Proszę podać lokalizacje.			(okazanie certyfikatów)

#### XI. KADRY I ŚWIADOMOŚĆ BEZPIECZEŃSTWA



58	Czy Wykonawca przeprowadza weryfikację przeszłości pracowników mających dostęp do danych klientów?			<i>(okazanie procedury weryfikacji pracowników (okazanie polityki bezpieczeństwa fizycznego lub innego dokumentu regulującego tą kwestię)</i>
59	Czy Wykonawca prowadzi regularne szkolenia z zakresu bezpieczeństwa informacji dla pracowników? Czy Wykonawca prowadzi regularne szkolenia z zakresu cyberbezpieczeństwa i cyberhigieny? Czy bierze w nich udział personel poddostawcy?			<i>(okazanie planu szkoleń)</i>
60	Czy Wykonawca posiada procedurę dyscyplinarną za naruszenie zasad bezpieczeństwa informacji?			<i>(okazanie procedury)</i>
61	Jakie zasady bezpieczeństwa obowiązują pracowników firmy pracujących zdalnie? Czy pracownicy Wykonawcy pracujący zdalnie mogą wykonywać pracę zdalną poza Polską i/lub EOG?			<i>(okazanie procedury pracy zdalnej (okazanie polityki bezpieczeństwa fizycznego lub innego dokumentu regulującego tą kwestię)</i>

## XII. DOSTAWCA WYSOKIEGO RYZYKA / REKOMENDACJE PEŁNOMOCNIKA ds. CYBERBEZPIECZEŃSTWA

62	Czy Wykonawca dostarcza lub dostarczał produkty ICT, usługi ICT, procesy ICT, które zostały wskazane w rekomendacji Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa, stwierdzającej negatywny wpływ takich produktów ICT, usług ICT lub procesów ICT na podstawowy interes bezpieczeństwa państwa?			
63	Czy wobec Wykonawcy toczy się lub toczyło postępowanie w sprawie uznania za dostawcę wysokiego ryzyka?			
64	Czy produkty ICT, usługi ICT lub procesy ICT oferowane przez Wykonawcę były przedmiotem decyzji o uznaniu za dostawcę wysokiego ryzyka? Jeśli tak - jakie?			