Nr referencyjny: KPT-DPR.270.1.09.2025

Załącznik nr 9 do SWZ

OPIS PRZEDMIOTU ZAMÓWIENIA

Przeprowadzenie 12 usług doradczych dla przedsiębiorstw z sektora MŚP w związku z realizacją usługi DORADZTWO W ZAKRESIE CYBERBEZPIECZEŃSTWA w ramach projektu „Technopark Kielce DIH" współfinansowanego ze środków Programu Cyfrowa Europa (Digital Europe) oraz Funduszy Europejskich dla Nowoczesnej Gospodarki na lata 2021-2027 (FENG).

Gmina Kielce realizuje projekt „Technopark Kielce DIH" *(zwanym dalej również TKDIH),* będący kluczową inicjatywą skierowaną na podniesienie konkurencyjności regionu świętokrzyskiego i stymulowanie jego dynamicznego rozwoju gospodarczego, opartego na innowacyjnych rozwiązaniach i postępie technologicznym. Inicjatywa ta ma na celu ustanowienie nowoczesnych standardów funkcjonowania firm, zarówno na poziomie regionalnym, jak i branżowym, poprzez wdrażanie zaawansowanych technologii cyfrowych, które pozwolą na dostosowanie się do wymagań współczesnego rynku. Jednym z kluczowych elementów projektu jest wspieranie przedsiębiorstw w procesie cyfryzacji, poprzez szeroko zakrojone szkolenia i działania edukacyjne, mające na celu podniesienie świadomości oraz rozwój umiejętności w zakresie nowoczesnych technologii cyfrowych.

Doradztwo w zakresie cyberbezpieczeństwa:
Doradztwo w zakresie analizy obecnych technologii pod kątem ich efektywności w obszarze polityki bezpieczeństwa, procedur i zasad planowania ciągłości biznesowej oraz najlepszych praktyk branżowych (najlepsze praktyki sprzedawców rozwiązań dotyczących bezpieczeństwa, wytyczne RODO i ISO 27001, NIST, COBIT i zarządzanie ryzykiem ISO 31000). Usługa doradztwa w zakresie cyberbezpieczeństwa skierowana zostanie do podmiotów sektora MŚP zakwalifikowanych do uczestnictwa w projekcie TKDIH z uwzględnieniem ich specyfiki działalności (w tym m.in. start-upów technologicznych, firm z sektora ICT i przemysłu 4.0). Doradztwo obejmuje kompleksową analizę i ocenę przedsiębiorstwa w 5 kluczowych obszarach: zgodności z regulacjami i standardami; posiadanych polityk i procedur dotyczących cyberbezpieczeństwa i zarządzaniem ryzykiem; zabezpieczeń infrastruktury fizycznej przedsiębiorstwa; zabezpieczeń wykorzystywanego oprogramowania; zabezpieczeń i zarządzania danymi; oraz określenie rekomendacji realizacyjnych na podstawie raportu z oceny.

SZCZEGÓŁOWY OPIS PREDMIOTU ZAMÓWIENIA

1. Przedmiotem zamówienia są usługi doradcze dla przedsiębiorstw sektora MŚP w związku z realizacją usługi „**Doradztwo w zakresie cyberbezpieczeństwa**" skierowanej do 12 podmiotów – przedsiębiorstw MŚP, zakwalifikowanych do uczestnictwa w projekcie „Technopark Kielce DIH" z uwzględnieniem ich specyfiki działalności (w tym m.in. start-upów technologicznych, firm z sektora ICT i przemysłu 4.0).
2. Liczba podmiotów objętych kompleksowym doradztwem: **12 podmiotów z sektora MŚP**,
3. Forma świadczenia usług: **model mieszany-hybrydowy (forma stacjonarna / zdalna)** *(w zależności o etapu).*
4. Miejsce świadczenia usług: siedziba „Odbiorcy usługi" (przedsiębiorcy) i/lub siedziba Zamawiającego i/lub w inne miejsca wskazane przez „Odbiorcy usługi" (przedsiębiorcy)/Zamawiającego kluczowe w kontekście cyberbezpieczeństwa.
5. Ramy czasowe realizacji wszystkich 12 usług: **od dnia zawarcia umowy z Wykonawcą, jednak nie później do 31 marca 2026 r.,** zgodnie z załączonym harmonogramem stanowiącym załącznik nr 1 Harmonogram usług do szczegółowego opisu przedmiotu zamówienia (SOPZ). Czas trwania jednej usługi na rzecz jednego podmiotu: do 35 dni kalendarzowych.
6. Każdorazowo przedmiot zamówienia realizowany na rzecz każdego z 12 przedsiębiorstw obejmuje kompleksową usługę w zakresie cyberbezpieczeństwa skupioną w pięciu obszarach jej realizacji:
   I. ***Ocena zgodności z regulacjami i standardami,***
   II. ***Ocena polityk i procedur bezpieczeństwa,***
   III. ***Ocena poziomu bezpieczeństwa technicznego związanego z posiadaną infrastrukturą, jej funkcjonowaniem i wydajnością,***
   IV. ***Ocena poziomu bezpieczeństwa danych,***
   V. ***Ocena poziomu bezpieczeństwa wykorzystywanego oprogramowania i rozwiązań informatycznych aplikacji.***
7. Wymagania:
   a. **Profil odbiorcy** – odbiorcami będą tylko uczestnicy projektu „Technopark Kielce DIH", którzy podpisali Umowę z Uczestnikiem II na usługi: „Doradztwo w zakresie cyberbezpieczeństwa". *Procesem rekrutacji uczestników do usługi przeprowadza Zamawiający.*
   b. Doradztwo zostanie przeprowadzone na podstawie opisów usług, które wynikają z wniosku o dofinansowanie projektu „Technopark Kielce DIH":
      - **Doradztwo w zakresie cyberbezpieczeństwa**: Doradztwo w zakresie analizy obecnych technologii pod kątem ich efektywności w obszarze polityki bezpieczeństwa, procedur i zasad planowania ciągłości biznesowej oraz najlepszych praktyk branżowych (najlepsze praktyki sprzedawców rozwiązań dotyczących bezpieczeństwa, wytyczne RODO i ISO 27001, NIST, COBIT i zarządzanie ryzykiem ISO 31000).

c. **Cel zamówienia** – analiza przedsiębiorstw sektora MŚP w kompleksowym ujęciu analizy cyberbezpieczeństwa, celem weryfikacji stanu obecnego oraz wydania rekomendacji do wdrożenia najlepszych praktyk branżowych w obszarach efektywnego zarządzania polityką bezpieczeństwa, procedur i zasad planowania ciągłości biznesowej, w pięciu kluczowych obszarach cyberbezpieczeństwa w firmie: zgodności z regulacjami i standardami; posiadanych polityk i procedur dotyczących cyberbezpieczeństwa i zarządzaniem ryzykiem; zabezpieczeń infrastruktury fizycznej przedsiębiorstwa; zabezpieczeń wykorzystywanego oprogramowania; zabezpieczeń i zarządzania danymi. W efekcie realizacji usługi przedsiębiorstwa otrzymają raport końcowy ukazujący aktualny stan firmy, niezbędne do wdrożenia zmiany oraz dalsze rekomendacje rozwojowe pomocne do budowaniu bezpiecznej cyberprzestrzeni.

8. **Zakres merytoryczny usługi** – podstawowy/minimalny zakres weryfikowalnych pięciu obszarów w ramach świadczonej usług:
   - ***I. Ocena zgodności z regulacjami i standardami,***
   - ***II. Ocena polityk i procedur bezpieczeństwa,***
   - ***III. Ocena poziomu bezpieczeństwa technicznego związanego z posiadaną infrastrukturą, jej funkcjonowaniem i wydajnością,***
   - ***IV. Ocena poziomu bezpieczeństwa danych,***
   - ***V. Ocena poziomu bezpieczeństwa wykorzystywanego oprogramowania i rozwiązań informatycznych aplikacji.***

AD.

I. Ocena zgodności z regulacjami i standardami:

1) Dokumenty odniesienia narodowe:
   a) Ustawa z dnia 10 maja 2018 roku o ochronie danych osobowych z późn. zm.,
   b) Dyrektywa w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w całej Unii Europejskiej (Dyrektywa NIS2),
   c) Ustawa z dnia 5 lipca 2018 roku o krajowym systemie cyberbezpieczeństwa z późn. zm.,
   d) Norma ISO/IEC 27001:2022 System Zarządzania Bezpieczeństwem Informacji,
   e) Norma ISO/IEC 27002 Praktyczne zasady zabezpieczania informacji.
2) Dokumenty odniesienia i standardy międzynarodowe:
   a) NIST Cybersecurity Framework 2.0,
   b) NIST SP 800-61r2 Computer Security Incident Handling Guide,
   c) NIST SP 800-209 Security Guidelines for Storage Infrastructure,
   d) NIST SP 800-92 Guide to Computer Security Log Management,
   e) NIST SP 800-223 High-Performance Computing Security,
   f) NIST SP 800-88 Guidelines for Media Sanitization.

II. Ocena polityk i procedur bezpieczeństwa:

1) Polityka dostępów,
2) Polityka autoryzacji i haseł,
3) Polityka monitorowania zasobów,
4) Polityk w zakresie reagowania na zdarzenia bezpieczeństwa i incydenty komputerowe,
5) Polityk odzyskiwania,
6) Polityk szkoleń personelu,
7) Polityki bezpieczeństwa informacji i zarządzania ryzykiem w cyberbezpieczeństwie,
8) Inne - niezbędne przepisami prawa lub/i wynikające z profilu działalności.

III. Ocena poziomu bezpieczeństwa technicznego związanego z posiadaną infrastrukturą, jej funkcjonowaniem i wydajnością:

1) Inwentaryzacja zasobów - stacja robocza, serwer sprzętowy, maszyna wirtualna, system operacyjny, oprogramowanie, urządzenia sieciowe, drukarki, urządzenia VoIP, IoT, usługi od dostawców zewnętrznych,
2) Weryfikacja zabezpieczeń i ocena urządzeń końcowych (laptopów, komputerów, urządzeń mobilnych) i serwerów,
3) Weryfikacja i ocena funkcjonującej sieci - konfiguracji urządzeń sieciowych, mechanizmów bezpieczeństwa sieci, segmentacji sieci, innych,
4) Weryfikacja i ocena funkcjonującej komunikacji i zasobów IoT, IIoT w przypadku rozwiązań przemysłu 4.0,
5) Weryfikacja i ocena fizycznych dostępów do zasobów sprzętowych i pomieszczeń ich przechowywania,
6) Weryfikacja i ocena fizycznych zabezpieczeń zasobów sprzętowych i pomieszczeń ich przechowywania.

IV. Ocena poziomu bezpieczeństwa danych:

1) Inwentaryzacja rodzaju przechowywanych i przetwarzanych danych,
2) Weryfikacja i ocena dostępów do baz oraz rejestrów danych,
3) Weryfikacja i ocena metod przechowywania i przetwarzania danych,
4) Weryfikacja i ocena mechanizmów kopii bezpieczeństwa,
5) Weryfikacja i ocena mechanizmów odzyskiwania danych.

V. Ocena poziomu bezpieczeństwa wykorzystywanego oprogramowania i rozwiązań informatycznych aplikacji:

1) Inwentaryzacja zasobów oprogramowania i rozwiązań informatycznych – rozwiązania wewnętrzne/zewnętrzne, rodzaj licencjonowania, rodzaj funkcjonowania, inne,
2) Weryfikacja zabezpieczeń i ocena przechowywania danych w zidentyfikowanych rozwiązaniach,
3) Weryfikacja i ocena reguł autoryzacyjnych i dostępów do zidentyfikowanych rozwiązań,

4) Weryfikacja i ocena funkcjonującej komunikacji międzysystemowej wewnętrznej oraz zewnętrznej,
5) Weryfikacja i ocena konfiguracji rozwiązań w kontekście ich maintenance, aktualizacji, planów awaryjnych, wsparcia, innych.

9. Harmonogram współpracy:

a) Przygotowanie dokumentacji usług,

b) *Rekrutacja przedsiębiorstw „odbiorcy usług" – zadanie Zamawiającego*,

c) Podpisanie umów na realizację usług,

d) Harmonogram realizacji usług,

e) Realizacja usług na rzecz przedsiębiorstw,

f) Rozliczenia usług.

AD:

a) **Przygotowanie dokumentacji usług** – celem realizacji usługi Wykonawca opracuje dokumentację bazową, obejmującą m.in.: „Personalizowany plan usługi", „Kwestionariusz oceny" oraz wzór „Raportu końcowego z usług". Bazowa dokumentacja zostanie wypracowana przez Wykonawcę usługi, na bazie „Opisu przedmiotu zamówienia", własnego doświadczenia, w porozumieniu i akceptacji z Zamawiającym.
   - „Personalizowany plan usługi", to dokument niezbędny do realizacji przez eksperta usługi doradztwa w zakresie cyberbezpieczeństwa, zawierającej badane obszary i zagadnienia, zgodnie z wyznaczonymi pięcioma obszarami świadczenia usługi – zakresem merytorycznym usług.
   - „Kwestionariusz oceny" – formularz weryfikacji przygotowania podmiotu na wyzwania cyberbezpieczeństwa i jego obszarów oddziaływania.
   - „Raport końcowy z usług" – dokument ukazujący szablon raportu końcowego, który po zakończeniu świadczenia usługi przekazywany zostanie jako efekt wyświadczonej usług w firmie (odbiorcy usługi) oraz dla Zamawiającego TKDIH.

a) Rekrutacja przedsiębiorstw „odbiorcy usług" – *rekrutacja po stronie Zamawiającego TKDIH*.
Na potrzeby wyświadczenia 12 usług doradczych w zakresie cyberbezpieczeństwa, przez Wykonawcę, Zamawiający przeprowadzi proces rekrutacji firm, zgodnie z wyznaczonym założeniami projektu TKDIH.
Zamawiający na bieżąco wskazywał będzie Wykonawcy przedsiębiorstwa, na rzecz których Wykonawca będzie świadczył przedmiotowe usługi, aż do osiągnięcia

liczby 12 podmiotów, informując Wykonawcę o obowiązku rozpoczęcia świadczenia usługi z co najmniej tygodniowym wyprzedzeniem, pisemnie lub pocztą elektroniczną.

b) Podpinanie umów na realizację usług – *dokument trójstronny*
Celem realizacji 12 usług, każdorazowo z zrekrutowaną firmą podpisane zostaną trójstronne umowy o realizacji usługi na linii: Odbiorca usługi (przedsiębiorca) – Wykonawca usług – Zamawiający. Umowa określać będzie zakres merytoryczny usługi, zgodny z przedmiotem zamówienia tj. usługa doradztwo w zakresie cyberbezpieczeństwa, ramy czasowe realizacji, zobowiązania, formę rozliczenia oraz konieczne i niezbędne zobowiązania stron.

c) Harmonogram realizacji usług – uszeregowany wykaz odbiorców usług, z wyznaczonymi czasowymi ramami realizacji usługi na rzecz przedsiębiorców („Odbiorcy usług"). Dokument aktualizowany w procesie świadczenia usług. Ramy czasowe świadczonych usług ustalane zgodnie z założeniami procesu świadczenia usług, konsultowane/wyznaczane będą w porozumieniu trójstronnym i wynikać będą z zawartej z „Odbiorcy usług" umowy.

- **Realizacja usług na rzecz przedsiębiorstw** – cykliczna zgodna z harmonogramem realizacja 12 usług na rzecz Odbiorcy usług (MŚP) przez Wykonawcę. Czas trwania wszystkich usług powinien się zamknąć w czasowych ramach: **od dnia zawarcia umowy z Wykonawcą, jednak nie później do 31 marca 2026 r.** Czas trwania jednej usługi na rzecz jednego podmiotu wyniesie do 35 dni kalendarzowych.

d) Rozliczenia usług - celem rozliczenia finansowego usługi, Wykonawca przedłoży do Zamawiającego zaakceptowany przez przedsiębiorcę raport końcowy z usługi wraz z protokołem zdawczo-odbiorczym potwierdzającym prawidłowo realizację usługi, poświadczony trójstronnym podpisami przez strony Odbiorca usługi (przedsiębiorca) - Wykonawca – Zamawiający. Przedstawienie raportu końcowego wraz z protokołem odbioru usługi, stanowić będzie podstawę do finansowego rozliczenia miedzy stronami.

10. Realizacja usług w zakresie cyberbezpieczeństwa na rzecz przedsiębiorstwa:

Personalizowany plan usługi	T+7 dni
Szczegółowa analiza i ocena w przedsiębiorstwie	T+15 dni
Przygotowanie raportu z usługi wraz z rekomendacjami	T+25 dni
Przekazanie raportu końcowego	T+35 dni

AD.

a) Personalizowany plan usługi – w ramach każdej, pojedynczej świadczonej usługi Wykonawca przedstawi personalizowany plan szczegółowy realizacji, zgodnie z podejściem adekwatności i miarodajności proponowanych działań według indywidualnych możliwości oraz wymagań konkretnego podmiotu ocenianego. Indywidulany plan realizacji usług na rzecz odbiorcy usługi (firmy), wyznaczać będzie obszary, ramy oraz etapy analizy w przedsiębiorstwie konieczne i niezbędne do prawidłowej analizy firmy pod kątem cyberspołeczeństwa w kontekście analizy pięciu obszarów wyznaczonych usługą. Plan usługi zostanie przygotowany przez Wykonawcę i następnie skonsultowany oraz zatwierdzony przez Odbiorcę usługi i Zamawiającego.

Forma realizacji: spotkania bezpośrednie w siedzibie Odbiorcy usługi i/lub w innych miejscach kluczowych w kontekście cyberbezpieczeństwa *(lub jeśli to konieczne w formie zdalnej),* kontakt email/tel. *(jako forma uzupełniająca kontakt).*

b) **Szczegółowa analiza i ocena w przedsiębiorstwie** – ocena przedsiębiorcy przeprowadzana zgodnie z wyznaczonym „Personalizowanym planem usługi" oraz na bazie ustalonego „kwestionariusz oceny".

Każdorazowo w procesie świadczenia usługi Wykonawca określi m.in.:

- Ilość wszystkich zasobów (m.in. stacja robocza, serwer sprzętowy, maszyna wirtualna, system operacyjny, oprogramowanie, urządzenia sieciowe, drukarki, urządzenia VoIP, IoT, usługi od dostawców zewnętrznych) - określana każdorazowo przez Wykonawcę w ramach jednej usługi, indywidualnie dla każdego z zakwalifikowanych do wsparcia podmiotów „Odbiorcy usługi".
- Ilość wszystkich pracowników objętych analizą i oceną w ramach kompleksowego doradztwa: określana każdorazowo w ramach jednej usługi, indywidualnie dla każdego z zakwalifikowanych do wsparcia podmiotów „Odbiorcy usługi".
- Ilość i rodzaj rozwiązań informatycznych (oraz ich technologie) objętych analizą i oceną w ramach kompleksowego doradztwa: określana każdorazowo w ramach jednej usługi, indywidualnie dla każdego z zakwalifikowanych do wsparcia podmiotów.

Forma realizacji: spotkania bezpośrednie w siedzibie Odbiorcy usługi i/lub w innych miejscach kluczowych w kontekście cyberbezpieczeństwa *(lub jeśli to konieczne lub możliwe w formie zdalnej),* kontakt email/tel. *(jako forma uzupełniająca kontakt).* Forma współpracy zależeć będzie od indywidulanego personalizowanego planu usługi.

c) **Przygotowanie raportu z usługi wraz z rekomendacjami** - każdorazowo jako efekt przeprowadzonej usługi na rzecz przedsiębiorcy, Wykonawca na podstawie zebranych informacji ze spotkań/kontaktu z Odbiorcą usługi, przygotuje „Raport końcowy z usługi" ukazujący przebieg usługi, analizę, ocenę i rekomendacje, zgodnie z personalizowanym planem usługi. Dokument ukaże stan obecny przedsiębiorstwa w analizowanych pięciu obszarach cyberbezpieczeństwa, w tym luki wdrożeniowe, analizę zasobów i rozwiązań informatycznych, wykaz rekomendacji koniecznych i możliwych do wdrożenia, jak również dalsze zalecenia dla rozwoju.
Forma realizacji: praca wewnętrzna/samodzielna wykonawcy *(doszczegółowienie informacji, jeśli wymaga – spotkanie bezpośrednie w siedzibie Odbiorcy usługi i/lub w innych miejscach kluczowych w kontekście cyberbezpieczeństwa, praca zdalna/hybrydowej, kontakt email/tel.).*

d) **Przekazanie raportu końcowego** - celem zakończenia usługi, Wykonawca przedłoży do przedsiębiorcy (odbiorcy usługi) raport końcowy z usługi. Dokument zaprezentowany zostanie przez Wykonawcę w formie spotkania bezpośredniego lub zdalnego, wraz z wyjaśnieniem szczegółowej analizy, wyników, spostrzeżeń oraz wynikających z realizacji usługi rekomendacji do wdrożenia. W przypadku błędów w Raporcie wynikających z niedopatrzeń Wykonawcy, Wykonawca zobowiązany będzie do uzupełnienia /poprawy raportu i ponownej prezentacji raportu w terminie nieprzekraczanym 5 dni roboczych. Zaakceptowany przez Odbiorcę usług Raport końcowy przekazany zostanie do Zamawiającego wraz z protokołem zdawczo-odbiorczym potwierdzającym prawidłowo realizację usługi, poświadczony trójstronnym podpisami przez strony umowy. Przedstawienie raportu końcowego wraz z protokołem odbioru usługi, stanowić będzie podstawę do finansowego rozliczenia miedzy stronami.
Forma realizacji: spotkania bezpośrednie w siedzibie Odbiorcy usługi i/lub w innych miejscach kluczowych w kontekście cyberbezpieczeństwa / siedzibie Zamawiającego, lub jeśli proces to umożliwia lub jest konieczny w formie zdalnej.

11. Dodatkowe informacje, niezbędne w procesie świadczenia usługi:

a) **Wykonawca w okresie promocji usług doradczych przez Zamawiającego (zdanie: *Rekrutacji przedsiębiorstw „odbiorców usług")* lub/i w okresie ich świadczenia już przez Wykonawcę, zobowiązuje się do udziału w minimum dwóch spotkaniach informacyjnych dot. oferowanej usługi, w charakterze prelekcji o zakresie świadczonej usługi i wyzwaniach przestrzeni cyberbezpieczeństwa w przedsiębiorstwach. Termin spotkań ustalany będzie na bieżąco w Wykonawcą. Miejsca spotkań: siedziba Zamawiającego lub miejsce wskazane przez Zamawiającego w obszarze woj. Świętokrzyskiego.**

b) Wykonawca zapewni sprawne dokumentowanie przebiegu realizacji usług, w tym egzekwowanie ustaleń wynikających procesu, harmonogramu oraz obiegu dokumentów. Zamawiający wymaga, aby Wykonawca przeprowadził przedmiotowe zamówienie we współpracy z Zamawiającym, tzn. informował Zamawiającego o postępie prac. Wszelka korespondencja pomiędzy Wykonawcą a odbiorcami usług tj. przedsiębiorstwami, kierowana będzie również do Zamawiającego w formie kopii do wiadomości.

c) W przypadku formy pracy zdalnej - online, doradca/Wykonawca łączyć się będzie ze swojego miejsca zatrudnienia lub miejsca zamieszkania. Zamawiający wymaga, aby obiekt/pomieszczenie, z którego będzie łączył się doradca/Wykonawca było pomieszczeniem wolnym od hałasu. Nie dopuszczalnym jest obecność osób trzecich „w tle" (wizja i dźwięk) podczas prowadzenia usługi.

d) Wymagania techniczne dla świadczenia usługi w trybie pracy zdalnej - online:
   - Wykonawca jest zobowiązany do posiadania komputera/tabletu z dostępem do Internetu wyposażonego w mikrofon, opcjonalnie słuchawki.
   - Po stronie Wykonawcy jest zapewnienie oprogramowania, sprzętu wymaganego na potrzeby realizacji doradczej.

12. Obowiązki Zmawiającego i Wykonawcy:

a) Zamawiający przekaże Wykonawcy (a Wykonawca zobowiązuje się do ich stosowania) komplet materiałów graficznych, obejmujący zestaw logotypów, a także papier projektowy, szablon protokołu zdawczo-odbiorczego i inne wymagane dokumenty oraz elementy identyfikacji wizualnej zgodnie z wymogami projektu Technopark Kielce DIH. Wszystkie dokumenty, prezentacje, agendy, raporty oraz materiały doradcze, jak również wszelkie inne materiały wytworzone przez Wykonawcę, muszą zawierać przekazane logotypy i spełniać wytyczne dotyczące ich stosowania, które znajdują się na portalu: https://www.funduszeeuropejskie.gov.pl/media/127192/Podrecznik_wnioskodawcy_i_beneficjenta_FE_2021_27w_zakresie_informacji_i_promocji.pdf Wykonawca zobowiązany jest do ścisłego przestrzegania tych zasad.

b) Jeśli spotkania lub/i usługi doradcze świadczone będą w siedzibie Zamawiającego, udostępni on sale spotkań biznesowych w Kieleckim Parku Technologicznym, przy ul. Olszewskiego 6, 26-663 Kielce. Zapewnienie dostępności sal wynikać będzie z wcześniejszych ustaleń terminu i czasu między Zamawiającym a Wykonawcą.

c) Opieka nad „Odbiorcą usługi" – Zamawiający oraz Wykonawca odpowiedzialni będą za bieżącą komunikację z przedsiębiorcami korzystającymi z usługi, odpowiadając na ich pytania oraz zapewniając informacje organizacyjne dotyczące harmonogramu, czasu, miejsca, formy doradztwa oraz postępu merytorycznego prac związanych z usługą.

13. **Doświadczenie dotyczące Wykonawcy:**

Minimum 5 usług w zakresie realizacji projektów oceny cyberbezpieczeństwa dla pięciu różnych podmiotów, w tym:

a) **Minimum 1 usługa** w zakresie realizacji projektów oceny cyberbezpieczeństwa dla przedsiębiorstwa funkcjonującego na rynkach międzynarodowych,

b) **Minimum 3 usługi** w zakresie realizacji projektów oceny cyberbezpieczeństwa dla przedsiębiorstwa o statusie MSP,

c) **Minimum 1 usługa** w zakresie realizacji projektów oceny cyberbezpieczeństwa dla podmiotu jednej z branż (podmioty kluczowe wg. NIS2): energetyka, transport, bankowość, infrastruktura rynków finansowych, ochrona zdrowia, woda pitna, ścieki, infrastruktura cyfrowa, administracja publiczna oraz przestrzeń kosmiczna.

Przy czym każda z wyżej wymienionych usług, wykazanych jako doświadczenie Wykonawcy, powinna zawierać informację o wykonaniu oceny cyberbezpieczeństwa dla przynajmniej 3 z 5 wymienionych obszarów (obszary zgodne z zakresem merytorycznym usługi będące przedmiotem zamówienia niniejszego postępowania):

1. Ocena zgodności z regulacjami i standardami,
2. Ocena polityk i procedur bezpieczeństwa,
3. Ocena poziomu bezpieczeństwa infrastruktury,
4. Ocena poziomu bezpieczeństwa danych,
5. Ocena poziomu bezpieczeństwa wykorzystywanego oprogramowania i rozwiązań informatycznych aplikacji.

14. **Doświadczenie, kompetencje i zespół doradców realizujących usługi po stronie Wykonawcy:**
Minimum 2 osoby, przy czym każda z nich z doświadczeniem w zakresie realizacji projektów cyberbezpieczeństwa, w tym:

a) **Minimum jedna osoba** z minimum 5 letnim doświadczeniem w realizacji usług w zakresie cyberbezpieczeństwa w sektorze prywatnym lub/i publicznym dla infrastruktury krytycznej i/lub podmiotów branż kluczowych (związane z NIS/NIS2) posiadający np. certyfikację zabezpieczeń oprogramowania (Balasys, FUDO, Mc Afee - Trellix, CompTIA) oraz certyfikację zabezpieczeń infrastruktury sieciowej (CISCO CCNA; CompTIA Network+; CompTIA Security+) lub równoważne,

b) **Minimum jedna osoba** z minimum 2 letnim doświadczeniem w branży IT w sektorze prywatnym lub/i publicznym, posiadający np. certyfikację zabezpieczeń infrastruktury sieciowej (CISCO CCNA; CompTIA Network+; CompTIA Security+) lub/i posiadający certyfikację zabezpieczeń oprogramowania (Balasys, FUDO, Mc Afee - Trellix, CompTIA) lub równoważne.

Załączniki:

Załącznik nr 1 Harmonogram usług do szczegółowego opisu przedmiotu zamówienia (SOPZ)**.**