

Pisz, dnia 12 sierpnia 2025 r.

ZAPYTANIE OFERTOWE

Powiat Piski zaprasza do składania ofert na **Usługę przeprowadzenia szkoleń w formie on-line dot. Części 1 – 6 oraz stacjonarnie w siedzibie Zamawiającego tj. Starostwie Powiatowym w Pisz** dot. Części 7, zgodnie z przedstawionymi wymogami:

I. Informacje ogólne dotyczące przedmiotowej procedury:

1. Dane Zamawiającego:

Powiat Piski z siedzibą w Starostwie Powiatowym w Pisz
12-200 Pisz, ul. Warszawska 1
NIP 849-150-34-23
Tel. (87) 425-47-00
e-mail: sekretariat@powiat.pisz.pl

2. Ilekroć w dalszej części zapytania ofertowego jest mowa o:

- **Bazie Konkurencyjności lub BK2021** - strona internetowa prowadzona przez Ministra Właściwego do spraw rozwoju regionalnego przeznaczona do umieszczania zapytań ofertowych zgodnie z zasadą konkurencyjności, <https://bazakonkurencyjnosci.funduszeuropejskie.gov.pl>
- **Ustawie sankcyjnej** - Ustawa z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego (t.j. Dz. U. z 2025 r. poz. 514),
- **Wykonawcy** – podmiot, który ubiega się o wykonanie zamówienia, złoży ofertę na wykonanie zamówienia albo zawrze z Zamawiającym umowę w sprawie wykonania zamówienia,
- **Wytycznych** - Wytyczne z 18 listopada 2022 r. dotyczące kwalifikowalności wydatków na lata 2021-2027 wydanych przez Ministerstwo Funduszy i Polityki Regionalnej.
- **Zamawiającym** – Powiat Piski
- **Zapytaniu ofertowym** - zaproszenie do składania ofert - opis szczególnych zasad udziału w postępowaniu wraz z warunkami umownymi realizacji zamówienia o wartości szacunkowej poniżej 130 000 zł netto, do którego nie stosuje się przepisów ustawy Prawo zamówień publicznych.

3. Tryb udzielenia zamówienia:

Niniejsze postępowanie prowadzone jest zgodnie z zachowaniem zasady konkurencyjności, jawności i równego traktowania Wykonawców, które zostały określone w podrozdziale 3.2 Wytycznych.

4. Zamawiający informuje, iż zamówienie, o którym mowa w Dziale II Zapytania ofertowego jest realizowane w ramach konkursy grantowego „Cyberbezpieczny Samorząd” o nr FERC.02.02-CS.01-001/23 współfinansowanego ze środków Unii Europejskiej w ramach programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 (FERC), Priorytetu II: Zaawansowane usługi cyfrowe, Działania 2.2. - Wzmocnienie krajowego systemu cyberbezpieczeństwa, w ramach projektu „Wzmocnienie Systemu Cyberbezpieczeństwa w Starostwie Powiatowym w Pisz uwzględniając rozwiązania organizacyjne, kompetencyjne i techniczne”.

II. Opis przedmiotu zamówienia

1. Przedmiot zamówienia:

Część 1 zamówienia:

- 1) Szkolenie z zakresu administracji i zarządzania SO Windows Server, z uwzględnieniem uczestnictwa w warsztatach technicznych.
- 2) Szkolenie z zakresu administracji i zarządzania SO Linux, z uwzględnieniem uczestnictwa w warsztatach technicznych.
- 3) Szkolenie z zakresu administracji i zarządzania systemami wirtualizacji, z uwzględnieniem uczestnictwa w warsztatach technicznych.
- 4) Szkolenie z zakresu administracji i zarządzania rozwiązaniem antywirusowym z Elementami XDR, antyspam, uwierzytelniania wieloskładnikowego.

Część 2 zamówienia:

- 1) Szkolenie z zakresu administracji i zarządzania urządzeniami klasy UTM, z uwzględnieniem uczestnictwa w warsztatach technicznych.

Część 3 zamówienia:

- 1) Szkolenie z zakresu administracji i zarządzania systemem tworzenia i zarządzania kopii zapasowych oraz ich testowania i przywracania.

Część 4 zamówienia:

- 1) Szkolenie w zakresie rozwiązań zarządzania LOG-ami - obsługa, administrowanie i zarządzanie, z uwzględnieniem uczestnictwa w warsztatach technicznych.
- 2) Szkolenie z zakresu administracji sieciami komputerowymi i rozwiązaniami kryptograficznymi, z uwzględnieniem uczestnictwa w warsztatach technicznych.

Część 5 zamówienia:

- 1) Szkolenie w zakresie rozwiązań SIEM - obsługa, administrowanie i zarządzanie, z uwzględnieniem uczestnictwa w warsztatach technicznych.

Część 6 zamówienia:

- 1) Szkolenie z zakresu administracji i zarządzania oprogramowaniem do monitorowania oraz zarządzania siecią, audytowania i inwentaryzacji zasobów.

Część 7 zamówienia:

- 1) Szkolenie dla kadry kierowniczej oraz pracowników w zakresie cyberbezpieczeństwa i bezpieczeństwa informacji.

Kod CPV: 80500000-9 - Usługi szkoleniowe

2. Szczegółowy opis przedmiotu zamówienia został zawarty w **załączniku nr 2** oraz **Załącznikach nr 2a, 2b, 2c, 2d, 2e, 2f, 2g** do zapytania ofertowego.

III. Warunki udziału w postępowaniu i opis sposobu dokonywania oceny ich spełniania

1. O zamówienie mogą ubiegać się wykonawcy, którzy:

- znajdują się w sytuacji ekonomicznej i finansowej zapewniającej wykonanie zamówienia,
- posiadają niezbędną wiedzę i doświadczenie,
- dysponują potencjałem technicznym i osobami zdolnymi do wykonania zamówienia zgodnie z obowiązującymi przepisami prawa,
- nie podlegają wykluczeniu na podstawie art. 7 ust. 1 ustawy sankcyjnej.

W związku z powyższym warunkiem z postępowania o udzielenie zamówienia publicznego wyklucza się:

- a) Wykonawcę wymienionego w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisanego na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ustawy sankcyjnej;
- b) Wykonawcę, którego beneficjentem rzeczywistym w rozumieniu ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (t.j. Dz. U. z 2025 r. poz. 644) jest osoba wymieniona w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisana na listę lub będąca takim beneficjentem rzeczywistym od dnia 24 lutego 2022 r., o ile została wpisana na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ustawy sankcyjnej;
- c) Wykonawcę, którego jednostką dominującą w rozumieniu art. 3 ust. 1 pkt 37 ustawy z dnia 29 września 1994 r. o rachunkowości (t.j. Dz. U. z 2023 r. poz. 120 ze zm.), jest podmiot wymieniony w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisany na listę lub będący taką jednostką dominującą od dnia 24 lutego 2022r., o ile został wpisany na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ustawy sankcyjnej.

Wykluczenie następuje na okres trwania okoliczności określonych w lit a)-c) powyżej.

2. Zamawiający wymaga złożenia oświadczenia dotyczącego spełnienia warunków udziału w postępowaniu zgodnie z **Załącznikiem nr 1 do zapytania ofertowego**.
3. Ocena spełniania ww. warunków dokonana zostanie na podstawie informacji zawartych w przedłożonym **Załączniku nr 1 do zapytania ofertowego**.
4. W celu potwierdzenia braku istnienia okoliczności, o których mowa w ust. 1 tiret czwarty Zamawiający zastrzega możliwość samodzielnego badania ogólnodostępnych rejestrów, w tym Centralnej Ewidencji i Informacji o Działalności Gospodarczej, Krajowego Rejestru Sądowego oraz Centralnego Rejestru Beneficjentów Rzeczywistych.

IV. Kryteria oceny ofert

1. Kryteria, wg których będą rozpatrywane oferty:
 - cena za wykonanie zamówienia - 100%
2. Ilość punktów według kryterium cena przyznawana będzie według wzoru:

$$\text{cena brutto oferty z najniższą kwotą} / \text{cena brutto oferty ocenianej} \times 100 \text{ pkt}$$

3. Spośród ofert niepodlegających odrzuceniu, Zamawiający wybierze najkorzystniejszą cenowo ofertę, która otrzyma największą liczbę punktów.

4. W przypadku złożenia ofert, które uzyskają taką samą liczbę punktów, Zamawiający wezwie wykonawców, którzy złożyli te oferty, do złożenia w terminie określonym przez Zamawiającego ofert dodatkowych. Wykonawca składając oferty dodatkowe, nie może zaoferować cen wyższych niż zaoferowane w złożonych ofertach w postępowaniu.
5. Jeżeli zaoferowana cena lub koszt wydają się rażąco niskie w stosunku do przedmiotu zamówienia, tj. różnią się o więcej niż 30% od średniej arytmetycznej cen wszystkich ważnych ofert niepodlegających odrzuceniu, lub budzą wątpliwości zamawiającego co do możliwości wykonania przedmiotu zamówienia zgodnie z wymaganiami określonymi w zapytaniu ofertowym lub wynikającymi z odrębnych przepisów, zamawiający żąda od wykonawcy złożenia w wyznaczonym terminie wyjaśnień, w tym złożenia dowodów w zakresie wyliczenia ceny lub kosztu. Zamawiający oceni te wyjaśnienia w konsultacji z wykonawcą i może odrzucić tę ofertę wyłącznie w przypadku, gdy złożone wyjaśnienia wraz z dowodami nie uzasadniają podanej ceny lub kosztu w tej ofercie. Obowiązek wykazania, że oferta nie zawiera rażąco niskiej ceny lub kosztu spoczywa na wykonawcy.

V. Informacja o sposobie porozumiewania się z wykonawcami

1. Komunikacja w postępowaniu o udzielenie zamówienia, w tym ogłoszenie zapytania ofertowego, składanie ofert, wymiana informacji między Zamawiającym, a Wykonawcą oraz przekazywanie dokumentów i oświadczeń odbywa się pisemnie za pomocą **BK2021**.
2. Odstąpienie od komunikacji określonej w ust. 1. jest dopuszczalne w zakresie, w jakim nie jest możliwe dotrzymanie sposobu komunikacji w BK2021. W takich przypadkach korespondencja powinna zostać kierowana na adres e-mail: **sekretariat@powiat.pisz.pl** z zastrzeżeniem, że **ofertę** można złożyć wyłącznie za pomocą **BK2021**.
3. Wykonawca może zwrócić się do Zamawiającego o wyjaśnienie treści niniejszego zapytania. Zamawiający udzieli niezwłocznie wyjaśnień, jednak nie później niż na 2 dni przed upływem terminu składania ofert pod warunkiem, że wniosek o wyjaśnienie treści zapytania wpłynął do Zamawiającego nie później niż do końca dnia, w którym upływa połowa wyznaczonego terminu składania ofert.
4. Jeżeli wniosek o wyjaśnienie treści zapytania wpłynie po upływie terminu składania wniosku, o którym mowa w ust. 3 lub dotyczy udzielonych wyjaśnień, Zamawiający może udzielić wyjaśnień albo pozostawić wniosek bez rozpoznania.
5. Treść zapytań wraz z wyjaśnieniami zostanie przekazana Wykonawcom, bez ujawniania źródła zapytania poprzez zamieszczenie odpowiedzi na stronie internetowej, na której udostępnione jest zapytanie ofertowe:
<https://bazakonkurencyjnosci.funduszeuropejskie.gov.pl/>
6. W uzasadnionych przypadkach Zamawiający może przed upływem terminu składania ofert, zmienić treść zapytania ofertowego. Dokonaną zmianę treści Zamawiający udostępni na portalu:
<https://bazakonkurencyjnosci.funduszeuropejskie.gov.pl/>.
7. Wszelkie zmiany treści oraz wyjaśnienia udzielone na zapytania Wykonawców stają się integralną częścią zapytania ofertowego i są wiążące dla Wykonawców.
8. Jeżeli w wyniku zmiany treści zapytania ofertowego będzie niezbędny dodatkowy czas na wprowadzenie zmian w ofertach, Zamawiający przedłuży termin składania ofert i poinformuje o tym Wykonawców poprzez zamieszczenie informacji na portalu:
https://bazakonkurencyjnosci.funduszeuropejskie.gov.pl

VI. Opis sposobu przygotowania oferty

1. Oferta powinna zawierać następujące dokumenty:
 - 1) formularz ofertowy, wg załącznika nr 1a i/lub 1b i/lub 1c i/lub 1d i/lub 1e i/lub 1f i/lub 1g do zapytania ofertowego,
 - 2) oświadczenie o spełnieniu warunków udziału w postępowaniu, wg załącznika nr 1a i/lub 1b i/lub 1c i/lub 1d i/lub 1e i/lub 1f i/lub 1g do zapytania ofertowego,
 - 3) pełnomocnictwo – jeżeli dotyczy
2. Oferta musi być podpisana przez Wykonawcę, tj. osobę (osoby) reprezentującą Wykonawcę, zgodnie z zasadami reprezentacji wskazanymi we właściwym rejestrze lub centralnej ewidencji i informacji o działalności gospodarczej, lub osobę (osoby) upoważnioną do reprezentowania Wykonawcy. Jeżeli z treści dokumentu określającego status prawny Wykonawcy lub pełnomocnictwa wynika, iż do reprezentowania Wykonawcy upoważnionych jest łącznie kilka osób, dokumenty wchodzące w skład oferty muszą być podpisane przez wszystkie te osoby. Podpis powinien być sporządzony w sposób umożliwiający identyfikację osoby podpisującej (np. złożony wraz z imienną pieczętką lub czytelny z podaniem imienia i nazwiska). Jeżeli osoba (osoby) podpisująca ofertę (reprezentująca Wykonawcę lub Wykonawców występujących wspólnie) działa na podstawie pełnomocnictwa, pełnomocnictwo to musi zostać załączone do oferty.
3. Wykonawcy ponoszą wszelkie koszty własne związane z przygotowaniem i złożeniem oferty, niezależnie od wyniku postępowania. Zamawiający w żadnym przypadku nie odpowiada za koszty poniesione przez Wykonawców w związku z przygotowaniem i złożeniem oferty.
4. Oferta powinna być sporządzona w języku polskim.
5. Zamawiający dopuszcza składania ofert częściowych tj. na każdą część Wykonawca może złożyć tylko jedną ofertę. Maksymalna liczba części, na które może zostać udzielone zamówienie jednemu Wykonawcy to 7 części.
6. Zamawiający nie dopuszcza składania ofert wariantowych.

VII. Miejsce, termin i sposób składania ofert

1. Termin składania ofert upływa dnia **22 sierpnia 2025 r.** o godz. 10:00. Oferty złożone po tym terminie nie będą rozpatrywane.
2. Ofertę należy złożyć poprzez portal Baza Konkurencyjności Funduszy Europejskich - **<https://bazakonkurencyjnosci.funduszeuropejskie.gov.pl>**.
3. Instrukcja składania ofert dostępna na stronie:
https://archiwum-bazakonkurencyjnosci.funduszeuropejskie.gov.pl/info/web_instruction
pod nazwą INSTRUKCJA OFERENTA. Ofertę i inne oświadczenia oraz dokumenty za pośrednictwem BK2021 należy złożyć w postaci odwzorowania cyfrowego dokumentu zawierającego własnoręczny podpis wystawcy lub w postaci elektronicznej opatrzonej kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym wystawcy.

VIII. Termin wykonania zamówienia

- Część 1 – 6 zamówienia** - termin realizacji zamówienia od dnia podpisania umowy **do 15 grudnia 2025r.** (formuła on-line)
- Część 7 zamówienia** - termin realizacji zamówienia **od 15 listopada 2025r. do 15 grudnia 2025r.** (stacjonarne w siedzibie zamawiającego tj. Starostwie Powiatowym w Pisz).

IX. Informacja na temat zakazu konfliktu interesów

1. Zamówienia udzielane przez Zamawiającego nie mogą być udzielane podmiotom powiązanim z nim osobowo lub kapitałowo.

Konflikt interesów oznacza każdą sytuację, w której osoby biorące udział w przygotowaniu lub prowadzeniu postępowania o udzielenie zamówienia lub mogące wpłynąć na wynik tego postępowania mają, bezpośrednio lub pośrednio, interes finansowy, ekonomiczny lub inny interes osobisty, który postrzegać można jako zagrażający ich bezstronności i niezależności w związku z przygotowaniem i przeprowadzeniem procedury wyboru wykonawcy, a wykonawcą, polegające w szczególności na:

- uczestniczeniu w spółce jako wspólnik spółki cywilnej lub spółki osobowej, posiadaniu co najmniej 10% udziałów lub akcji (o ile niższy próg nie wynika z przepisów prawa), pełnieniu funkcji członka organu nadzorczego lub zarządzającego, prokurenta, pełnomocnika,
- pozostawaniu w związku małżeńskim, w stosunku pokrewieństwa lub powinowactwa w linii prostej, pokrewieństwa lub powinowactwa w linii bocznej do drugiego stopnia, lub związaniu z tytułu przysposobienia, opieki lub kurateli albo pozostawaniu we wspólnym pożyciu z wykonawcą, jego zastępcą prawnym lub członkami organów zarządzających lub organów nadzorczych wykonawców ubiegających się o udzielenie zamówienia,
- pozostawaniu z Wykonawcą w takim stosunku prawnym lub faktycznym, że istnieje uzasadniona wątpliwość co do ich bezstronności lub niezależności w związku z postępowaniem o udzielenie zamówienia.

X. Określenie warunków istotnych zmian umowy zawartej w wyniku przeprowadzonego postępowania o udzielenie zamówienia

Zamawiający przewiduje zmiany postanowień zawartej umowy w stosunku do treści oferty na podstawie której dokonano wyboru Wykonawcy. Szczegółowe informacje zostały zawarte w §7 wzoru umowy stanowiącego załącznik nr 3 do zapytania ofertowego.

XI. Informacja na temat udzielania zamówienia w częściach

Przedmiotowe zamówienie nie będzie realizowany w częściach stanowiących odrębne postępowania.

XII. Opis sposobu obliczenia ceny

1. Cena oferty powinna obejmować wszystkie elementy wyszczególnione przy określeniu przedmiotu zamówienia oraz zawierać podatek VAT.
2. Cena musi być podana w złotych polskich cyfrowo do dwóch miejsc po przecinku.
3. Cena oferty powinna obejmować wszystkie koszty niezbędne do poniesienia dla prawidłowego zrealizowania przedmiotu zamówienia.

XIII. Informacje o formalnościach, jakie powinny zostać dopełnione po wyborze oferty w celu zawarcia umowy w sprawie zamówienia publicznego

1. W przypadku wykonawców ubiegających się wspólnie o udzielenie zamówienia publicznego reprezentowanych przez Pełnomocnika, niezbędne jest przedstawienie pełnomocnictwa do podpisania umowy, o ile załączone do oferty pełnomocnictwo nie uwzględniało tej czynności prawnej.
2. W przypadku wykonawców ubiegających się wspólnie o udzielenie zamówienia, wykonawcy zobowiązani są do przedłożenia zamawiającemu umowy pomiędzy wykonawcami regulującej warunki realizacji zamówienia publicznego.
3. Jeżeli Wykonawca, którego oferta została wybrana, uchyla się od zawarcia umowy w sprawie zamówienia publicznego, Zamawiający może wybrać ofertę najkorzystniejszą spośród pozostałych ofert.

XIV. Przesłanki odrzucenia oferty

Zamawiający odrzuci ofertę złożoną przez Wykonawcę:

- 1) gdy oferta jest niezgodna z wymaganiami określonymi w zapytaniu ofertowym,
- 2) gdy oferta jest nieważna na podstawie odrębnych przepisów,
- 3) który pomimo wezwania do uzupełnienia w terminie wskazanym w wezwaniu nie złożył:
 - a) poprawnych dokumentów potwierdzających warunki udziału w postępowaniu (jeżeli zostały wyznaczone),
 - b) wymaganych pełnomocnictw lub złożył wadliwe pełnomocnictwa,
- 4) gdy oferta zawiera omyłki w obliczeniu ceny, których nie można poprawić jako oczywiste omyłki rachunkowe,
- 5) gdy oferta zawiera omyłki pisarskie bądź inne omyłki, których nie można poprawić jako oczywiste omyłki,
- 6) gdy oferta zawiera rażąco niską cenę w stosunku do przedmiotu zamówienia tzn. różni się o więcej niż 30% od średniej arytmetycznej cen wszystkich ważnych ofert niepodlegających odrzuceniu lub budzi wątpliwości zamawiającego co do możliwości wykonania przedmiotu zamówienia, zgodnie z wymaganiami określonymi w zapytaniu ofertowym lub wynikającymi z odrębnych przepisów,
- 7) który nie udzielił wyjaśnień lub jeżeli dokonana ocena wyjaśnień wraz ze złożonymi dowodami potwierdza, że oferta zawiera rażąco niską cenę w stosunku do przedmiotu zamówienia,
- 8) gdy oferta została złożona przez Wykonawcę wykluczonego z postępowania.

XV. Zawarcie umowy

1. O miejscu i terminie zawarcia umowy wybrany Wykonawca zostanie zawiadomiony drogą elektroniczną lub telefonicznie niezwłocznie po rozstrzygnięciu postępowania.
2. Umowa może zostać podpisana w siedzibie Zamawiającego lub w formie elektronicznej przy wykorzystaniu podpisu kwalifikowanego.
3. W przypadku, gdy podpisanie umowy w wyznaczonym terminie nie będzie możliwe z przyczyn leżących po stronie Wykonawcy, Wykonawca zobowiązany jest do wskazania innego terminu podpisania umowy z zastrzeżeniem, że termin ten nie będzie dłuższy niż 3 dni robocze niż termin pierwotnie wyznaczony przez Zamawiającego.

4. Dopuszcza się tryb obiegowy podpisania umowy. Do zawarcia umowy w trybie obiegowym dochodzi poprzez wymianę dokumentów obejmujących treść oświadczeń woli, z których każdy jest podpisany przez jedną ze Stron.
5. W przypadku, gdy Wykonawca w wyznaczonym terminie:
 - 1) nie podpisze umowy w siedzibie Zamawiającego,
 - 2) nie odeśle podpisanej umowy (w trybie obiegowym),
 - 3) złoży oświadczenie Zamawiającemu o odmowie podpisania umowy,Zamawiający uzna, iż Wykonawca uchyla się od zawarcia umowy z przyczyn leżących po jego stronie.
6. Jeżeli Wykonawca zobowiązany do zawarcia umowy uchyla się od jej zawarcia, Zamawiający może żądać naprawienia szkody, którą poniósł przez to, że liczył na zawarcie umowy.

XVI. Postanowienia końcowe

1. Wykonawca pozostaje związany złożoną ofertą przez okres 30 dni od dnia otwarcia ofert.
2. Zamawiający zastrzega prawo do:
 - a) żądania szczegółowych informacji i wyjaśnień od Wykonawców na każdym etapie postępowania,
 - b) zamknięcia postępowania bez dokonania wyboru oferty,
 - c) zmiany terminów wyznaczonych w zapytaniu ofertowym,
 - d) odwołania postępowania, unieważnienia go w całości lub w części w każdym czasie, w następujących sytuacjach:
 - nie złożono żadnej oraz nie złożono żadnej oferty niepodlegającej odrzuceniu,
 - cena najkorzystniejszej oferty przewyższa kwotę, którą Zamawiający zamierza przeznaczyć na sfinansowanie zamówienia chyba, że Zamawiający może zwiększyć tę kwotę do ceny najkorzystniejszej oferty,
 - wystąpiła istotna zmiana okoliczności powodująca, że prowadzenie postępowania lub wykonanie zamówienia nie leży w interesie Zamawiającego, czego nie można było wcześniej przewidzieć,
 - postępowanie obarczone jest niemożliwą do usunięcia wadą uniemożliwiającą zawarcie Umowy lub prawidłową jej realizację.
3. Wykonawcy uczestniczą w postępowaniu na własny koszt i ryzyko, nie przysługują im żadne roszczenia z tytułu unieważnienia postępowania przez Zamawiającego.

XVII. Informacja o posiadanych danych osobowych i ich przetwarzaniu

W celu wykonania obowiązku nałożonego w drodze art. 13 i 14 RODO, w związku z art. 88 ustawy wdrożeniowej, informujemy o zasadach przetwarzania Państwa danych osobowych:

Administrator danych

Odrębnymi administratorami Państwa danych są:

1. Minister Funduszy i Polityki Regionalnej (dalej jako MFIPR), w zakresie w jakim pełni funkcję Instytucji Zarządzającej (IZ) Funduszami Europejskimi na Rozwój Cyfrowy 2021-2027 (dalej jako FER) z siedzibą przy ul. Wspólnej 2/4, 00-926 Warszawa,
2. Centrum Projektów Polska Cyfrowa (dalej jako CPPC) w zakresie w jakim pełni funkcję Instytucji Pośredniczącej (IP) FER, z siedzibą przy ul. Spokojnej 13A, 01-044 Warszawa,

3. Centrum Projektów Polska Cyfrowa (dalej jako CPPC) w zakresie w jakim pełni funkcje Beneficjenta FERC, z siedzibą przy ul. Spokojnej 13A, 01-044 Warszawa.

Cel przetwarzania danych

Państwa dane osobowe będziemy przetwarzać w związku z realizacją FERC, w szczególności w związku z naborem 2.2 FERC. Podanie danych jest dobrowolne, ale konieczne do realizacji ww. celu. Odmowa ich podania jest równoznaczna z brakiem możliwości podjęcia stosownych działań.

Podstawa przetwarzania

Będziemy przetwarzać Państwa dane osobowe w związku z tym, że:

1. Zobowiązuje nas do tego **prawo** (art. 6 ust. 1 lit. c RODO):
 - 1) art. 87 ustawy wdrożeniowej,
 - 2) art. 61 ustawy z 28 kwietnia 2022 r. o zasadach realizacji zadań finansowanych ze środków europejskich w perspektywie finansowej 2021-2027 (Dz. U. z 2022 r. poz. 1079),
 - 3) ustawa z 14 czerwca 1960 r. - Kodeks postępowania administracyjnego (tekst jednolity Dz.U. z 2023 r. poz. 775 z późn. zm.),
 - 4) art. 206 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (tekst jednolity Dz. U. z 2022 r. poz. 1634, z późn. zm.),
 - 5) Porozumienie trójstronne w sprawie systemu realizacji programu „Fundusze Europejskie na Rozwój Cyfrowy 2021-2027” z 2.02.2023 r.,
 - 6) rozporządzenia Ministra Cyfryzacji z dnia 16 lutego 2023 r. w sprawie udzielania pomocy na rozwój infrastruktury szerokopasmowej w ramach programu Fundusze Europejskie na Rozwój Cyfrowy 2021–2027 (Dz. U. z 2023 r. poz. 405),
2. Wykonujemy zadania w interesie publicznym lub sprawujemy powierzona nam władzę publiczną (art. 6 ust. 1 lit. e RODO),
3. Przygotowujemy i realizujemy **umowy**, których są Państwo stroną, a przetwarzanie danych osobowych jest niezbędne do ich zawarcia i wykonania (art. 6 ust. 1 lit. b RODO).

Rodzaje przetwarzanych danych

Możemy przetwarzać następujące rodzaje Państwa danych:

1. dane identyfikacyjne, wskazane w art. 87 ust. 2 pkt 1 ustawy wdrożeniowej, w tym: imię, nazwisko, adres, adres poczty elektronicznej, numer telefonu, numer faksu, PESEL, REGON, wykształcenie, identyfikatory internetowe,
2. dane związane z zakresem uczestnictwa osób fizycznych w projekcie, wskazane w art. 87 ust. 2 pkt 2 ustawy wdrożeniowej, w tym w szczególności: wynagrodzenie, formę i okres zaangażowania w projekcie,
3. dane osób fizycznych widniejące na dokumentach potwierdzających kwalifikowalność wydatków, wskazane w art. 87 ust. 2 pkt. 3 ustawy wdrożeniowej, m.in. numer rachunku bankowego, doświadczenie zawodowe, numer uprawnień budowlanych, numer księgi wieczystej,
4. dane dotyczące wizerunku i głosu osób uczestniczących w realizacji Programu lub biorących udział w wydarzeniach z nim związanych.

Dane pozyskujemy bezpośrednio od osób, których one dotyczą, albo od instytucji i podmiotów zaangażowanych w realizację FERC w tym w szczególności od wnioskodawców, beneficjentów, partnerów.

Dostęp do danych osobowych

Dostęp do Państwa danych osobowych mają pracownicy i współpracownicy MFIPR oraz CPPC. Ponadto Państwa dane osobowe mogą być powierzane lub udostępniane:

1. podmiotom, w tym ekspertom, o których mowa w art. 80 ustawy wdrożeniowej, którym zlecieliśmy wykonywanie zadań w ramach realizacji FERC,
2. instytucji audytowej, o której mowa w art. 71 rozporządzenie Parlamentu

Europejskiego i Rady (UE) 2021/1060 z dnia 24 czerwca 2021 r. ustanawiające wspólne przepisy dotyczące Europejskiego Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego Plus, Funduszu Spójności, Funduszu na rzecz Sprawiedliwej Transformacji i Europejskiego Funduszu Morskiego, Rybackiego i Akwakultury, a także przepisy finansowe na potrzeby tych funduszy oraz na potrzeby Funduszu Azyłu, Migracji i Integracji, Funduszu Bezpieczeństwa Wewnętrznego i Instrumentu Wsparcia Finansowego na rzecz Zarządzania Granicami i Polityki Wizowej,

3. instytucjom Unii Europejskiej (UE) lub podmiotom, którym UE powierzyła zadania dotyczące wdrażania FERC;
4. podmiotom, które wykonują dla nas usługi związane z obsługą i rozwojem systemów teleinformatycznych, a także zapewnieniem łączności, np. dostawcom rozwiązań IT i operatorom telekomunikacyjnym.

Okres przechowywania danych

Będziemy przechowywać Państwa dane osobowe zgodnie z przepisami o narodowym zasobie archiwalnym i archiwach, do momentu zakończenia realizacji przez IZ/IP/Beneficjenta wszelkich zadań związanych z realizacją i rozliczeniem FERC, z zastrzeżeniem przepisów, które mogą przewidywać dłuższy termin przeprowadzania kontroli, a ponadto przepisów dotyczących pomocy publicznej i pomocy *de minimis* oraz przepisów dotyczących podatku od towarów i usług.

Prawa osób, których dane dotyczą

Przysługują Państwu następujące prawa:

1. dostępu do swoich danych osobowych oraz otrzymania ich kopii (art. 15 RODO),
2. do sprostowania swoich danych (art. 16 RODO),
3. do usunięcia swoich danych (art. 17 RODO) - jeśli dotyczy,
4. do żądania od administratora ograniczenia przetwarzania swoich danych (art. 18 RODO),
5. wniesienia sprzeciwu – wobec przetwarzania swoich danych (art. 21 RODO) - jeśli przetwarzanie odbywa się w celu wykonywania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej, powierzonej administratorowi (tj. w celu, o którym mowa w art. 6 ust. 1 lit. e RODO,
6. wniesienia skargi do organu nadzorczego (art. 77 RODO), tj. Prezesa Urzędu Ochrony Danych Osobowych, w przypadku uznania, że przetwarzanie danych osobowych narusza przepisy RODO lub inne przepisy prawa regulujące kwestię ochrony danych osobowych.

Zautomatyzowane podejmowanie decyzji

Dane osobowe nie będą podlegały zautomatyzowanemu podejmowaniu decyzji, w tym profilowaniu.

Przekazywanie danych do państwa trzeciego

Nie zamierzamy przekazywać Państwa danych osobowych do państwa trzeciego lub organizacji międzynarodowej innej niż Unia Europejska. W przypadku konieczności przekazania Państwa danych osobowych do państwa trzeciego lub organizacji międzynarodowej zapewniamy, że odbędzie się to z zachowaniem warunków określonych w art. 45 lub 46 RODO.

Kontakt z administratorem danych i Inspektorem Ochrony Danych

Jeśli mają Państwo pytania dotyczące przetwarzania przez CPPC danych osobowych, prosimy kontaktować z Inspektorami Ochrony Danych Osobowych (dalej jako IOD) w następujący sposób:

1. IOD MFIPR:
 - 1) pocztą tradycyjną kierując korespondencję na adres: ul. Wspólna 2/4, 00-926 Warszawa,
 - 2) elektronicznie na adres e-mail: IOD@mfipr.gov.pl,
2. IOD CPPC:
 - 1) pocztą tradycyjną kierując korespondencję na adres: ul. Spokojna 13A, 01-044 Warszawa,
 - 2) elektronicznie na adres e-mail: bezpieczenstwo@cppc.gov.pl.

Podstawa prawna:

1. ustawa wdrożeniowa - ustawa z 28 kwietnia 2022 r. o zasadach realizacji zadań finansowanych ze środków europejskich w perspektywie finansowej 2021-2027 (Dz. U. z 2022 r., poz. 1079),
2. RODO - rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (Dz. Urz. UE L 119 z 4 maja 2016 r., s.1-88; Dz. Urz. UE L 127 z 23 maja 2018, str. 2 oraz Dz. Urz. UE L 74 z 4 marca 2021, str. 35).

STAROSTA

/-/ mgr Andrzej Nowicki

Załączniki:

- Formularz ofertowy dla Części 1 – załącznik nr 1a
- Formularz ofertowy dla Części 2 – załącznik nr 1b
- Formularz ofertowy dla Części 3 – załącznik nr 1c
- Formularz ofertowy dla Części 4 – załącznik nr 1d
- Formularz ofertowy dla Części 5 – załącznik nr 1e
- Formularz ofertowy dla Części 6 – załącznik nr 1f
- Formularz ofertowy dla Części 7 – załącznik nr 1g
- Opis przedmiotu zamówienia – załącznik nr 2
- Opis przedmiotu zamówienia dla Części 1 – załącznik nr 2a
- Opis przedmiotu zamówienia dla Części 2 – załącznik nr 2b
- Opis przedmiotu zamówienia dla Części 3 – załącznik nr 2c
- Opis przedmiotu zamówienia dla Części 4 – załącznik nr 2d
- Opis przedmiotu zamówienia dla Części 5 – załącznik nr 2e
- Opis przedmiotu zamówienia dla Części 6 – załącznik nr 2f
- Opis przedmiotu zamówienia dla Części 7 – załącznik nr 2g
- Wzór umowy – załącznik nr 3

Załącznik nr 1a

.....
/Nazwa i adres Wykonawcy/

.....
/miejscowość i data/

Tel. wykonawcy:

adres e-mail wykonawcy:

Powiat Piski
ul. Warszawska 1
12-200 Pisz

FORMULARZ OFERTOWY

Odpowiadając na zaproszenie do wzięcia udziału w zapytaniu ofertowym nr Or.272.2.17.2025 na Usługi przeprowadzenia szkoleń określone w **Część 1 zamówienia**, oferujemy realizację przedmiotu zamówienia za:

cenę brutto zł

w tym podatek VAT w wysokości% wynosi zł

Nazwa szkolenia	Czas trwania 1 szkolenia	Ilość szkoleń	Cena jednostkowa netto za 1 szkolenie	Wartość netto (3x4)
1	2	3	4	5
Szkolenie z zakresu administracji i zarządzania SO Windows Server	5 dni tj. łącznie 30 godz.	2		
Szkolenie z zakresu administracji i zarządzania SO Linux	3 dni tj. łącznie 21 godz.	2		
Szkolenie z zakresu administracji i zarządzania systemami wirtualizacji, Vmware vSphere	2 dni tj. łącznie 14 godz.	2		
Szkolenie z zakresu administracji i zarządzania rozwiązaniem antywirusowym z Elementami XDR, antyspam	3 dni tj. łącznie 21 godz.	2		
Wartość netto				
Podatek VAT w zł				
Wartość brutto				

- Przedmiot zamówienia realizować będziemy w okresie wskazanym w warunkach zapytania ofertowego.
- Oświadczamy, że zapoznaliśmy się z warunkami zapytania ofertowego (w tym ze wzorem umowy) i nie wnosimy do niej zastrzeżeń oraz przyjmujemy warunki w nich zawarte.
- Oświadczamy, że uważamy się za związanych niniejszą ofertą na okres wskazany w warunkach zapytania ofertowego.
- Oświadczamy, że:
 - nie podlegamy wykluczeniu z postępowania na podstawie art. 7 ust. 1 ustawy sankcyjnej,

- 2) znajdujemy się w sytuacji ekonomicznej i finansowej zapewniającej wykonanie zamówienia,
- 3) posiadamy niezbędną wiedzę i doświadczeni do wykonania zamówienia,
- 4) dysponujemy potencjałem technicznym i osobami zdolnymi do wykonywania zamówienia.
5. Oświadczam, że nie jestem powiązany osobowo lub kapitałowo z Zamawiającym w sytuacjach, o których mowa w Sekcji 3.2.2 pkt 8) wytycznych.
6. Oświadczamy, że przedmiot zamówienia zamierzamy powierzyć niżej wymienionym podwykonawcom do wykonania niżej wymienione części zamówienia..... (jeżeli dotyczy)
7. Oświadczamy, że wypełniliśmy obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskaliśmy w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu.
8. Oświadczamy, że oferta nie zawiera/zawiera* informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji.

* niepotrzebne skreślić

.....
podpis Wykonawcy

Załącznik nr 1b

.....
/Nazwa i adres Wykonawcy/

.....
/miejscowość i data/

Tel. wykonawcy:

adres e-mail wykonawcy:

Powiat Piski
ul. Warszawska 1
12-200 Pisz

FORMULARZ OFERTOWY

Odpowiadając na zaproszenie do wzięcia udziału w zapytaniu ofertowym nr Or.272.2.17.2025 na Usługi przeprowadzenia szkoleń określone w **Część 2 zamówienia**, oferujemy realizację przedmiotu zamówienia za:

cenę brutto zł

w tym podatek VAT w wysokości% wynosi zł

Nazwa szkolenia	Czas trwania 1 szkolenia	Ilość szkoleń	Cena jednostkowa netto za 1 szkolenie	Wartość netto (3x4)
1	2	3	4	5
Szkolenie w zakresie administracji i zarządzania urządzeniami UTM oraz sieciami komputerowymi, Fortigate	3 dni, tj. łącznie 24 godz.	2		
Wartość netto				
Podatek VAT w zł				
Wartość brutto				

1. Przedmiot zamówienia realizować będziemy w okresie wskazanym w warunkach zapytania ofertowego.
2. Oświadczamy, że zapoznaliśmy się z warunkami zapytania ofertowego (w tym ze wzorem umowy) i nie wnosimy do niej zastrzeżeń oraz przyjmujemy warunki w nich zawarte.
3. Oświadczamy, że uważamy się za związanych niniejszą ofertą na okres wskazany w warunkach zapytania ofertowego.
4. Oświadczamy, że:
 - 1) nie podlegamy wykluczeniu z postępowania na podstawie art. 7 ust. 1 ustawy sankcyjnej,
 - 2) znajdujemy się w sytuacji ekonomicznej i finansowej zapewniającej wykonanie zamówienia,
 - 3) posiadamy niezbędną wiedzę i doświadczeni do wykonania zamówienia,
 - 4) dysponujemy potencjałem technicznym i osobami zdolnymi do wykonywania zamówienia.
5. Oświadczam, że nie jestem powiązany osobowo lub kapitałowo z Zamawiającym w sytuacjach, o których mowa w Sekcji 3.2.2 pkt 8) wytycznych.

6. Oświadczamy, że przedmiot zamówienia zamierzamy powierzyć niżej wymienionym podwykonawcom do wykonania niżej wymienione części zamówienia..... *(jeżeli dotyczy)*
7. Oświadczamy, że wypełniliśmy obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskaliśmy w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu.
8. Oświadczamy, że oferta nie zawiera/zawiera* informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji.

* niepotrzebne skreślić

.....
podpis Wykonawcy

.....
/Nazwa i adres Wykonawcy/

.....
/miejscowość i data/

Tel. wykonawcy:

adres e-mail wykonawcy:

Powiat Piski
ul. Warszawska 1
12-200 Pisz

FORMULARZ OFERTOWY

Odpowiadając na zaproszenie do wzięcia udziału w zapytaniu ofertowym nr Or.272.2.17.2025 na Usługi przeprowadzenia szkoleń określone w **Część 3 zamówienia**, oferujemy realizację przedmiotu zamówienia za:

cenę brutto **zł**

w tym podatek VAT w wysokości% wynosi **zł**

Nazwa szkolenia	Czas trwania 1 szkolenia	Ilość szkoleń	Cena jednostkowa netto za 1 szkolenie	Wartość netto (3x4)
1	2	3	4	5
Szkolenie z zakresu administracji i zarządzania systemem tworzenia i zarządzania kopii zapasowych oraz ich testowania i przywracania, Veeam® Backup & Replication™	4 dni, tj. łącznie 32 godz.	2		
Wartość netto				
Podatek VAT w zł				
Wartość brutto				

1. Przedmiot zamówienia realizować będziemy w okresie wskazanym w warunkach zapytania ofertowego.
2. Oświadczamy, że zapoznaliśmy się z warunkami zapytania ofertowego (w tym ze wzorem umowy) i nie wnosimy do niej zastrzeżeń oraz przyjmujemy warunki w nich zawarte.
3. Oświadczamy, że uważamy się za związanych niniejszą ofertą na okres wskazany w warunkach zapytania ofertowego.
4. Oświadczamy, że:
 - 1) nie podlegamy wykluczeniu z postępowania na podstawie art. 7 ust. 1 ustawy sankcyjnej,
 - 2) znajdujemy się w sytuacji ekonomicznej i finansowej zapewniającej wykonanie zamówienia,
 - 3) posiadamy niezbędną wiedzę i doświadczeni do wykonania zamówienia,
 - 4) dysponujemy potencjałem technicznym i osobami zdolnymi do wykonywania zamówienia.
5. Oświadczam, że nie jestem powiązany osobowo lub kapitałowo z Zamawiającym w sytuacjach, o których mowa w Sekcji 3.2.2 pkt 8) wytycznych.

6. Oświadczamy, że przedmiot zamówienia zamierzamy powierzyć niżej wymienionym podwykonawcom do wykonania niżej wymienione części zamówienia..... *(jeżeli dotyczy)*
7. Oświadczamy, że wypełniliśmy obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałismy w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu.
8. Oświadczamy, że oferta nie zawiera/zawiera* informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji.

* niepotrzebne skreślić

.....
podpis Wykonawcy

.....
/Nazwa i adres Wykonawcy/

.....
/miejscowość i data/

Tel. wykonawcy:

adres e-mail wykonawcy:

Powiat Piski
ul. Warszawska 1
12-200 Pisz

FORMULARZ OFERTOWY

Odpowiadając na zaproszenie do wzięcia udziału w zapytaniu ofertowym nr Or.272.2.17.2025 na Usługi przeprowadzenia szkoleń określone w **Część 4 zamówienia**, oferujemy realizację przedmiotu zamówienia za:

cenę brutto **zł**

w tym podatek VAT w wysokości% wynosi **zł**

Nazwa szkolenia	Czas trwania 1 szkolenia	Ilość szkoleń	Cena jednostkowa netto za 1 szkolenie	Wartość netto (3x4)
1	2	3	4	5
Szkolenie w zakresie rozwiązań zarządzania LOG-ami - obsługa, administrowanie i zarządzanie	1 dzień, tj. łącznie 7 godzin	2		
Szkolenie z zakresu administracji sieciami komputerowymi i rozwiązaniami kryptograficznymi, z uwzględnieniem uczestnictwa w warsztatach technicznych	2 dni, tj. łącznie 16 godzin	2		
Wartość netto				
Podatek VAT w zł				
Wartość brutto				

- Przedmiot zamówienia realizować będziemy w okresie wskazanym w warunkach zapytania ofertowego.
- Oświadczamy, że zapoznaliśmy się z warunkami zapytania ofertowego (w tym ze wzorem umowy) i nie wnosimy do niej zastrzeżeń oraz przyjmujemy warunki w nich zawarte.
- Oświadczamy, że uważamy się za związanych niniejszą ofertą na okres wskazany w warunkach zapytania ofertowego.
- Oświadczamy, że:
 - nie podlegamy wykluczeniu z postępowania na podstawie art. 7 ust. 1 ustawy sankcyjnej,
 - znajdujemy się w sytuacji ekonomicznej i finansowej zapewniającej wykonanie zamówienia,
 - posiadamy niezbędną wiedzę i doświadczeni do wykonania zamówienia,
 - dysponujemy potencjałem technicznym i osobami zdolnymi do wykonywania zamówienia.

5. Oświadczam, że nie jestem powiązany osobowo lub kapitałowo z Zamawiającym w sytuacjach, o których mowa w Sekcji 3.2.2 pkt 8) wytycznych.
6. Oświadczamy, że przedmiot zamówienia zamierzamy powierzyć niżej wymienionym podwykonawcom do wykonania niżej wymienione części zamówienia..... *(jeżeli dotyczy)*
7. Oświadczamy, że wypełniliśmy obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskaliśmy w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu.
8. Oświadczamy, że oferta nie zawiera/zawiera* informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji.

* niepotrzebne skreślić

.....
podpis Wykonawcy

.....
/Nazwa i adres Wykonawcy/

.....
/miejscowość i data/

Tel. wykonawcy:

adres e-mail wykonawcy:

Powiat Piski
ul. Warszawska 1
12-200 Pisz

FORMULARZ OFERTOWY

Odpowiadając na zaproszenie do wzięcia udziału w zapytaniu ofertowym nr Or.272.2.17.2025 na Usługi przeprowadzenia szkoleń określone w **Część 5 zamówienia**, oferujemy realizację przedmiotu zamówienia za:

cenę brutto **zł**

w tym podatek VAT w wysokości% wynosi **zł**

Nazwa szkolenia	Czas trwania 1 szkolenia	Ilość szkoleń	Cena jednostkowa netto za 1 szkolenie	Wartość netto (3x4)
1	2	3	4	5
Szkolenie w zakresie rozwiązań SIEM - obsługa, administrowanie i zarządzanie SIEM WAZUH	3 dni, tj. łącznie 24 godz.	2		
Wartość netto				
Podatek VAT w zł				
Wartość brutto				

- Przedmiot zamówienia realizować będziemy w okresie wskazanym w warunkach zapytania ofertowego.
- Oświadczamy, że zapoznaliśmy się z warunkami zapytania ofertowego (w tym ze wzorem umowy) i nie wnosimy do niej zastrzeżeń oraz przyjmujemy warunki w nich zawarte.
- Oświadczamy, że uważamy się za związanych niniejszą ofertą na okres wskazany w warunkach zapytania ofertowego.
- Oświadczamy, że:
 - nie podlegamy wykluczeniu z postępowania na podstawie art. 7 ust. 1 ustawy sankcyjnej,
 - znajdujemy się w sytuacji ekonomicznej i finansowej zapewniającej wykonanie zamówienia,
 - posiadamy niezbędną wiedzę i doświadczeni do wykonania zamówienia,
 - dysponujemy potencjałem technicznym i osobami zdolnymi do wykonywania zamówienia.
- Oświadczam, że nie jestem powiązany osobowo lub kapitałowo z Zamawiającym w sytuacjach, o których mowa w Sekcji 3.2.2 pkt 8) wytycznych.

6. Oświadczamy, że przedmiot zamówienia zamierzamy powierzyć niżej wymienionym podwykonawcom do wykonania niżej wymienione części zamówienia..... *(jeżeli dotyczy)*
7. Oświadczamy, że wypełniliśmy obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskaliśmy w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu.
8. Oświadczamy, że oferta nie zawiera/zawiera* informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji.

* niepotrzebne skreślić

.....
podpis Wykonawcy

.....
/Nazwa i adres Wykonawcy/

.....
/miejscowość i data/

Tel. wykonawcy:

adres e-mail wykonawcy:

Powiat Piski
ul. Warszawska 1
12-200 Pisz

FORMULARZ OFERTOWY

Odpowiadając na zaproszenie do wzięcia udziału w zapytaniu ofertowym nr Or.272.2.17.2025 na Usługi przeprowadzenia szkoleń określone w **Część 6 zamówienia**, oferujemy realizację przedmiotu zamówienia za:

cenę brutto zł

w tym podatek VAT w wysokości% wynosi zł

Nazwa szkolenia	Czas trwania 1 szkolenia	Ilość szkoleń	Cena jednostkowa netto za 1 szkolenie	Wartość netto (3x4)
1	2	3	4	5
Szkolenie z zakresu administracji i zarządzania oprogramowaniem do monitorowania oraz zarządzania siecią, audytowania i inwentaryzacji zasobów	1 dzień, tj. łącznie 8 godziny	2		
Wartość netto				
Podatek VAT w zł				
Wartość brutto				

1. Przedmiot zamówienia realizować będziemy w okresie wskazanym w warunkach zapytania ofertowego.
2. Oświadczamy, że zapoznaliśmy się z warunkami zapytania ofertowego (w tym ze wzorem umowy) i nie wnosimy do niej zastrzeżeń oraz przyjmujemy warunki w nich zawarte.
3. Oświadczamy, że uważamy się za związanych niniejszą ofertą na okres wskazany w warunkach zapytania ofertowego.
4. Oświadczamy, że:
 - 1) nie podlegamy wykluczeniu z postępowania na podstawie art. 7 ust. 1 ustawy sankcyjnej,
 - 2) znajdujemy się w sytuacji ekonomicznej i finansowej zapewniającej wykonanie zamówienia,
 - 3) posiadamy niezbędną wiedzę i doświadczeni do wykonania zamówienia,
 - 4) dysponujemy potencjałem technicznym i osobami zdolnymi do wykonywania zamówienia.
5. Oświadczam, że nie jestem powiązany osobowo lub kapitałowo z Zamawiającym w sytuacjach, o których mowa w Sekcji 3.2.2 pkt 8) wytycznych.

6. Oświadczamy, że przedmiot zamówienia zamierzamy powierzyć niżej wymienionym podwykonawcom do wykonania niżej wymienione części zamówienia..... *(jeżeli dotyczy)*
7. Oświadczamy, że wypełniliśmy obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskaliśmy w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu.
8. Oświadczamy, że oferta nie zawiera/zawiera* informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji.

* niepotrzebne skreślić

.....
podpis Wykonawcy

Załącznik nr 1g

.....
/Nazwa i adres Wykonawcy/

.....
/miejscowość i data/

Tel wykonawcy:

adres e-mail wykonawcy:

Powiat Piski
ul. Warszawska 1
12-200 Pisz

FORMULARZ OFERTOWY

Odpowiadając na zaproszenie do wzięcia udziału w zapytaniu ofertowym nr Or.272.2.17.2025 na Usługi przeprowadzenia szkoleń określone w **Część 7 zamówienia**, oferujemy realizację przedmiotu zamówienia za:

cenę brutto zł

w tym podatek VAT w wysokości% wynosi zł

Nazwa szkolenia	Czas trwania 1 szkolenia	Ilość szkoleń	Cena jednostkowa netto za 1 szkolenie	Wartość netto (3x4)
1	2	3	4	5
Szkolenie dla kadry kierowniczej oraz pracowników w zakresie cyberbezpieczeństwa i bezpieczeństwa informacji.	1 dzień, tj. łącznie 6 godz.	2		
Wartość netto				
Podatek VAT w zł				
Wartość brutto				

- Przedmiot zamówienia realizować będziemy w okresie wskazanym w warunkach zapytania ofertowego.
- Oświadczamy, że zapoznaliśmy się z warunkami zapytania ofertowego (w tym ze wzorem umowy) i nie wnosimy do niej zastrzeżeń oraz przyjmujemy warunki w nich zawarte.
- Oświadczamy, że uważamy się za związanych niniejszą ofertą na okres wskazany w warunkach zapytania ofertowego.
- Oświadczamy, że:
 - nie podlegamy wykluczeniu z postępowania na podstawie art. 7 ust. 1 ustawy sankcyjnej,
 - znajdujemy się w sytuacji ekonomicznej i finansowej zapewniającej wykonanie zamówienia,
 - posiadamy niezbędną wiedzę i doświadczeni do wykonania zamówienia,
 - dysponujemy potencjałem technicznym i osobami zdolnymi do wykonywania zamówienia.
- Oświadczam, że nie jestem powiązany osobowo lub kapitałowo z Zamawiającym w sytuacjach, o których mowa w Sekcji 3.2.2 pkt 8) wytycznych.

6. Oświadczamy, że przedmiot zamówienia zamierzamy powierzyć niżej wymienionym podwykonawcom do wykonania niżej wymienione części zamówienia..... *(jeżeli dotyczy)*
7. Oświadczamy, że wypełniliśmy obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskaliśmy w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu.
8. Oświadczamy, że oferta nie zawiera/zawiera* informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji.

* niepotrzebne skreślić

.....
podpis Wykonawcy

Opis przedmiotu zamówienia

1. Część 1 – 6 termin realizacji zamówienia do 15 grudnia 2025r. realizowane w formule on-line.
2. Część 7 termin realizacji zamówienia od 15 listopada 2025r. do 15 grudnia 2025r. stacjonarnie w siedzibie Zamawiającego tj. Starostwie Powiatowym w Pisz, ul. Warszawska 1, 12-200 Pisz.
3. Szkolenie/szkolenia odbędą się zgodnie z harmonogramem, który zostanie przedstawionym przez Wykonawcę w terminie do 7 dni od dnia podpisania umowy. Dla każdego szkolenia (o jednej tematyce) Wykonawca zaproponuje co najmniej trzy różne, niepokrywające się terminy do wyboru przez Zamawiającego. Zamawiający (dla szkolenia o jednej tematyce) dokona wyboru dwóch z proponowanych terminów w ciągu 7 dni od otrzymania harmonogramu.
4. Szkolenia muszą odbywać się w języku polskim, dostępne materiały szkoleniowe w języku polskim lub angielskim.
5. Opis poruszanej tematyki jest zakresem minimalnym jaki winien być zrealizowany w toku przeprowadzanego szkolenia.
6. Wskazany czas trwania szkolenia jest czasem minimalnym w jakim powinno odbyć się szkolenie.
7. Jeżeli w zapytaniu ofertowym zamawiający opisał przedmiot zamówienia z zastosowaniem konkretnych metod lub rozwiązań dopuszcza się metody lub rozwiązania równoważne opisywanym.

Opis przedmiotu zamówienia

Część 1 zamówienia:

1. Szkolenie z zakresu administracji i zarządzania SO Windows Server, z uwzględnieniem uczestnictwa w warsztatach technicznych.
 - a) Szkolenie prowadzone przez autoryzowanego trenera Microsoft (MCT)
 - b) Czas trwania 1 szkolenia: **5 dni**, tj. łącznie 30 godzin
 - c) Ilość szkoleń: **2**
 - d) MS 55371 Administrowanie systemem Windows Server
 - e) Szkolenie mające na celu zdobycie takich umiejętności jak:
 1. Korzystanie z technik i narzędzi administracyjnych w systemie Windows Server,
 2. Wdrażanie usługi zarządzania tożsamością,
 3. Zarządzanie usługami infrastruktury sieciowej,
 4. Konfigurowanie serwerów plików i pamięci masowej,
 5. Zarządzanie maszynami wirtualnymi z wykorzystaniem wirtualizacji Hyper-V i kontenerów,
 6. Wdrażanie rozwiązania wysokiej dostępności i odzyskiwania danych po awarii,
 7. Stosowanie zabezpieczeń w celu ochrony kluczowych zasobów,
 8. Konfigurowanie usług zdalnego pulpitu,
 9. Konfigurowanie wdrożenia infrastruktury pulpitów opartej na maszynach wirtualnych,
 10. Wdrażanie dostępu zdalnego i usług internetowych,
 11. Wdrażanie monitorowania usług i wydajności oraz rozwiązywanie problemów,
 12. Wykonywanie aktualizacji i migracji związanych z AD DS, oraz pamięcią masową.

Opis:

Moduł 1: Wprowadzenie do administracji systemu Windows Server

- Wprowadzenie do systemu Windows Server
- Wprowadzenie do systemu Windows Server Core
- Wprowadzenie do zasad i narzędzi administracyjnych systemu Windows Server
- **Ćwiczenie:** Wdrażanie i konfiguracja systemu Windows Server
 - Wdrażanie i konfiguracja systemu Server Core
 - Wdrażanie i stosowanie zdalnej administracji serwerami

Po ukończeniu tego modułu uczestnicy będą w stanie:

- Opisać system Windows Server, a także techniki wdrażania, serwisowania i aktywacji,
- Opisać system Windows Server Core, przedstawić jego specyfikę i sposoby administrowania nim.

Moduł 2: Usługi zarządzania tożsamością w systemie Windows Server

- Wprowadzenie do AD DS
- Wdrażanie kontrolerów domeny Windows Server
- Wprowadzenie do usługi Azure AD

- Wdrażanie zasad grupy
- Wprowadzenie do usług certyfikatów Active Directory
- **Ćwiczenie:** Wdrażanie usług zarządzania tożsamością i zasad grupy
 - Wdrażanie nowego kontrolera domeny w systemie Server Core
 - Konfigurowanie zasad grupy
 - Wdrażanie i korzystanie z usług certyfikatów
 - Wyjaśnienie podstaw zasad grupy i konfiguracja GPO w środowisku domenowym
 - Opis roli usług certyfikatów Active Directory i korzystanie z certyfikatów

Po ukończeniu tego modułu uczestnicy będą w stanie:

- Opisać AD DS w środowisku systemu Windows Server,
- Wdrażać kontrolery domeny w AD DS,
- Opisać Azure AD i korzyści płynące z integracji Azure AD z AD DS.

Moduł 3: Usługi infrastruktury sieciowej w systemie Windows Server

- Wdrażanie i zarządzanie protokołem DHCP
- Wdrażanie i zarządzanie systemem DNS
- Wdrażanie i zarządzanie systemem IPAM
- Usługi dostępu zdalnego w systemie Windows Server
- **Ćwiczenie:** Wdrażanie i konfiguracja usług infrastruktury sieciowej w systemie Windows Server
 - Wdrażanie i konfiguracja protokołu DHCP
 - Wdrażanie i konfiguracja systemu DNS
 - Wdrażanie serwera proxy aplikacji sieci WWW

Po ukończeniu tego modułu uczestnicy będą w stanie:

- Opisać, wdrożyć i skonfigurować usługę DHCP,
- Wdrażać, konfigurować i zarządzać systemem DNS,
- Opisać, wdrożyć i zarządzać systemem IPAM.

Moduł 4: Serwery plików i zarządzanie pamięcią masową w systemie Windows Server

- Woluminy i systemy plików w systemie Windows Server
- Wdrażanie udostępniania w systemie Windows Server
- Wdrażanie rozwiązania Storage Spaces (przestrzeni dyskowych) w systemie Windows Server
- Wdrażanie deduplikacji danych
- Wdrażanie interfejsu iSCSI
- Wdrażanie rozproszonego systemu plików
- **Ćwiczenie:** Wdrażanie rozwiązań pamięci masowej w systemie Windows Server
 - Wdrażanie deduplikacji danych
 - Konfiguracja magazynu iSCSI
 - Konfiguracja nadmiarowych przestrzeni dyskowych
 - Wdrażanie Storage Spaces Direct

Po ukończeniu tego modułu uczestnicy będą w stanie:

- Wdrażać udostępnianie w systemie Windows Server,
- Wdrożyć technologię Storage Spaces,
- Wdrażać funkcję deduplikacji danych,
- Wdrażać pamięć masową opartą na iSCSI,

- Wdrożyć i zarządzać rozproszonym systemem plików (DFS - Distributed File System).

Moduł 5: Wirtualizacja Hyper-V i kontenery w systemie Windows Server

- Hyper-V w systemie Windows Server
- Konfiguracja maszyn wirtualnych /li>
- Zabezpieczanie wirtualizacji w systemie Windows Server
- Kontenery w systemie Windows Server
- Wprowadzenie do platformy Kubernetes
- **Ćwiczenie:** Wdrażanie i konfiguracja wirtualizacji w systemie Windows Server
 - Tworzenie i konfigurowanie maszyn wirtualnych
 - Instalacja i konfiguracja kontenerów

Po ukończeniu tego modułu uczestnicy będą w stanie:

- Opisać kluczowe cechy Hyper-V w systemie Windows Server,
- Opisać ustawienia maszyn wirtualnych oraz wdrożyć i skonfigurować maszyny wirtualne w Hyper-V,
- Wyjaśnić zastosowanie technologii bezpieczeństwa w wirtualizacji,
- Opisać i wdrożyć kontenery w systemie Windows Server,
- Wyjaśnić zastosowanie platformy Kubernetes w systemie Windows.

Moduł 6: Wysoka dostępność w systemie Windows Server

- Planowanie wdrożenia klastra pracy awaryjnej
- Tworzenie i konfiguracja klastra pracy awaryjnej
- Wprowadzenie do rozciągniętych klastrów
- Planowanie rozwiązań w zakresie wysokiej dostępności i odzyskiwania danych po awarii z wykorzystaniem maszyn wirtualnych funkcji Hyper-V
- **Ćwiczenie:** Wdrażanie klastra pracy awaryjnej
 - Konfiguracja pamięci masowej i tworzenie klastra
 - Wdrażanie i konfiguracja serwera plików o wysokiej dostępności
 - Sprawdzanie poprawności wdrożenia serwera plików o wysokiej dostępności

Po ukończeniu tego modułu uczestnicy będą w stanie:

- Opisać klastry pracy awaryjnej i warunki jego wdrożenia,
- Tworzyć i konfigurować klastry pracy awaryjnej,
- Opisać klastry rozciągnięte,
- Opisać opcje osiągania wysokiej dostępności za pomocą maszyn wirtualnych Hyper-V.

Moduł 7: Odzyskiwanie danych po awarii w systemie Windows Server

- Funkcja Hyper-V Replica
- Tworzenie kopii zapasowych i przywracanie infrastruktury w systemie Windows Server
- **Ćwiczenie:** Wdrażanie funkcji Hyper-V Replica i Windows Server Backup
 - Wdrażanie funkcji Hyper-V Replica
 - Wdrażanie tworzenia kopii zapasowych i przywracania za pomocą narzędzia Windows Server Backup

Po ukończeniu tego modułu uczestnicy będą w stanie:

- Opisać i wdrożyć funkcję Hyper-V Replica,

- Opisać usługę Azure Site Recovery,
- Opisać i wdrożyć narzędzie Windows Server Backup,
- Opisać usługę Azure Backup.

Moduł 8: Bezpieczeństwo systemu Windows Server

- Ochrona danych uwierzytelniających i dostępu uprzywilejowanego
- Hardening systemu Windows Server
- JEA w systemie Windows Server
- Zabezpieczanie i analiza ruchu w SMB
- Zarządzanie aktualizacjami w systemie Windows Server
- **Ćwiczenie:** Konfiguracja zabezpieczeń w systemie Windows Server
 - Konfiguracja funkcji Windows Defender Credential Guard
 - Lokalizowanie problematycznych kont
 - Wdrażanie rozwiązania LAPS

Po ukończeniu tego modułu uczestnicy będą w stanie:

- Opisać dane uwierzytelniające wykorzystywane w systemie Windows Server,
- Wyjaśnić, jak wdrożyć zabezpieczenia dostępu uprzywilejowanego,
- Opisać metody i technologie hardeningu zabezpieczeń w systemie Windows Server,
- Opisać i skonfigurować usługę Just Enough Administration (JEA),
- Zabezpieczyć ruch SMB w systemie Windows Server,
- Opisać usługę Windows Update oraz jej opcje wdrażania i zarządzania.

Moduł 9: RDS (usługi pulpitu zdalnego) w systemie Windows Server

- Wprowadzenie do RDS
- Konfiguracja wdrażania pulpitu opartego na sesji
- Wprowadzenie do osobistych i połączonych pulpitów wirtualnych
- **Ćwiczenie:** Wdrażanie RDS w systemie Windows Server
 - Wdrażanie RDS
 - Konfigurowanie ustawień kolekcji sesji i wykorzystywanie RDC
 - Konfiguracja szablonu pulpitu wirtualnego

Po ukończeniu tego modułu uczestnicy będą w stanie:

- Opisać usługi Remote Desktop Services (RDS - usługi pulpitu zdalnego) w systemie Windows Server,
- Opisać i wdrożyć pulpity oparte na sesji,
- Opisać osobiste i połączone pulpity wirtualne.

Moduł 10: Dostęp zdalny i usługi internetowe w systemie Windows Server

- Wdrażanie sieci VPN
- Wdrażanie usługi Always On VPN
- Wdrażanie systemu NPS
- Wdrażanie serwera WWW w systemie Windows Server
- **Ćwiczenie:** Wdrażanie obciążeń sieciowych
 - Wdrażanie sieci VPN w systemie Windows Server
 - Wdrażanie i konfiguracja serwera WWW

Po ukończeniu tego modułu uczestnicy będą w stanie:

- Opisać opcje sieci VPN w systemie Windows Server,
- Opisać funkcję Always On VPN,
- Opisać i skonfigurować NPS,
- Opisać i skonfigurować serwer WWW (IIS).

Moduł 11: Monitorowanie serwera i wydajności w systemie Windows Server

- Wprowadzenie do narzędzi do monitorowania systemu Windows Server
- Korzystanie z monitora wydajności
- Monitorowanie dzienników zdarzeń w celu rozwiązywania problemów
- **Ćwiczenie:** Monitorowanie i rozwiązywanie problemów z systemem Windows Server
 - Ustanowienie bazowego poziomu wydajności
 - Identyfikacja źródła problemu z wydajnością

Po ukończeniu tego modułu uczestnicy będą w stanie:

- Opisać narzędzia monitorujące w systemie Windows Server,
- Opisać monitorowanie wydajności i wykorzystać je w systemie Windows Server,
- Opisać rejestrowanie zdarzeń i monitorować rejestrowanie zdarzeń dla celów rozwiązywania problemów.

Moduł 12: Aktualizacja i migracja w systemie Windows Server

- Migracja AD DS
- Usługa migracji pamięci masowej
- Narzędzia do migracji systemu Windows Server
- **Ćwiczenie:** Migracja obciążeń serwera
 - Wdrażanie usługi migracji pamięci masowej

Po ukończeniu tego modułu uczestnicy będą w stanie:

- Opisać narzędzia, których należy użyć do migracji AD DS,
- Opisać usługę migracji pamięci masowej,
- Opisać narzędzia do migracji Windows Server i scenariusze ich użycia.

2. Szkolenie z zakresu administracji i zarządzania SO Linux, z uwzględnieniem uczestnictwa w warsztatach technicznych.

Linux LPIC-1 Certyfikowany administrator systemu Linux 101-500.

Czas trwania 1 szkolenia: 3 dni, tj. łącznie 21 godzin

Ilość szkoleń: 2

1. Architektura systemu

- a. Określenie i konfiguracja ustawień sprzętu
- b. Uruchamianie systemu
- c. Poziomy pracy, zamykanie lub uruchamianie ponownie systemu

2. Instalacja systemu Linux i zarządzanie pakietami

- a. Układ dysku twardego
- b. Instalacja menedżera rozruchu
- c. Zarządzanie bibliotekami współdzielonymi
- d. Zarządzanie pakietami Debiana
- e. Zarządzane pakietami RPM i YUM

3. Polecenia GNU i Unix

- a. Praca w wierszu poleceń
- b. Przetwarzanie strumieni tekstowe za pomocą filtrów
- c. Podstawowe zarządzanie plikami
- d. Strumienie, potoki i przekierowania
- e. Monitorowanie i zarządzanie procesami
- f. Modyfikacja priorytetów wykonywania procesów
- g. Przeszukiwanie plików tekstowych za pomocą wyrażeń regularnych
- h. Podstawowe operacje edycji plików za pomocą vi

4. Urządzenia, systemy plików Linux, Standard hierarchii systemów plików

- a. Partycje i systemy plików
- b. Integralność systemów plików
- c. Montowanie i odmontowywanie systemów plików
- d. Zarządzanie limitami dysków
- e. Zarządzanie uprawnieniami do plików i własnością

3. Szkolenie z zakresu administracji i zarządzania systemami wirtualizacji, z uwzględnieniem Uczestnictwa w warsztatach technicznych

Vmware vSphere: Instalacja, konfiguracja i zarządzanie

Czas trwania 1 szkolenia: 2 dni, tj. łącznie 14 godzin

Ilość szkoleń: 2

1. Przegląd vSphere i Wirtualizacji
 - a) Podstawy wirtualizacji: Wprowadzenie do koncepcji i znaczenia wirtualizacji.
 - b) vSphere i jego komponenty: Szczegółowe omówienie vSphere i jego elementów.
 - c) Zastosowania i korzyści: Przedstawienie korzyści płynących z wykorzystania wirtualnych maszyn.
 - d) Architektura i terminologia: Wyjaśnienie kluczowych terminów i struktury systemu.
2. Instalacja i konfiguracja ESXi
 - a) Wprowadzenie do ESXi: Podstawy i znaczenie ESXi w środowisku VMware.
 - b) Wymagania i instalacja: Przegląd wymagań i procesu instalacji ESXi.
 - c) Konfiguracja hosta ESXi: Szczegółowe kroki konfiguracji hosta.
 - d) Laboratoria i demonstracje: Praktyczne ćwiczenia z instalacji i konfiguracji.
3. Wdrażanie i konfiguracja vCenter
 - a) Zarządzanie scentralizowane z vCenter: Rola i znaczenie vCenter w zarządzaniu środowiskiem VMware.
 - b) Architektura i usługi vCenter: Przegląd komponentów i usług vCenter.
 - c) Licencjonowanie i skalowalność: Omówienie licencji i możliwości skalowania.
 - d) Zarządzanie inwentarzem vCenter: Techniki i narzędzia do zarządzania zasobami.
 - e) Role i uprawnienia: Zarządzanie dostępem i uprawnieniami użytkowników.
4. Konfiguracja sieci vSphere
 - a) Podstawy sieci wirtualnych: Wprowadzenie do sieci wirtualnych i ich typów.
 - b) Standardowe i rozproszone przełączniki: Porównanie i konfiguracja różnych typów przełączników.
 - c) Laboratoria praktyczne: Ćwiczenia z konfiguracji i zarządzania siecią w środowisku vSphere.
5. Konfiguracja przechowywania danych w vSphere
 - a) Podstawy przechowywania danych: Wprowadzenie do koncepcji i typów przechowywania danych.
 - b) VMFS i NFS Datastores: Konfiguracja i zarządzanie magazynami danych.
 - c) Fibre Channel i iSCSI Storage: Omówienie i konfiguracja różnych typów przechowywania.
 - d) Laboratoria i ćwiczenia praktyczne: Praktyczne zastosowanie wiedzy o przechowywaniu danych.
6. Wdrażanie maszyn wirtualnych
 - a) Tworzenie i zarządzanie VM: Proces tworzenia i konfiguracji maszyn wirtualnych.
 - b) Szablony i biblioteki zawartości: Wykorzystanie szablonów i zarządzanie bibliotekami.
 - c) Narzędzia VMware i sprzęt wirtualny: Instalacja i aktualizacja narzędzi VMware, zarządzanie sprzętem wirtualnym.
 - d) Laboratoria i symulacje: Praktyczne ćwiczenia z tworzenia i zarządzania VM.
7. Zarządzanie Maszynami Wirtualnymi
 - a) Migracja Maszyn Wirtualnych: Omówienie różnych typów migracji, w tym vSphere vMotion.
 - b) Zarządzanie Snapshots : Techniki zarządzania snapshotami
8. Wdrażanie i Konfiguracja Klastrow vSphere
 - a) Przegląd Klastrow vSphere: Podstawy tworzenia i zarządzania klastrami vSphere.

- b) vSphere Distributed Resource Scheduler (DRS): Konfiguracja i zarządzanie DRS w klastrach.
- c) vSphere High Availability (HA): Wprowadzenie do HA i scenariusze awarii.
- d) Architektura vSphere HA: Szczegółowe omówienie architektury i komunikacji w HA.
- e) Konfiguracja vSphere HA: Praktyczne wskazówki dotyczące konfiguracji i zarządzania HA.

4. Szkolenie z zakresu administracji i zarządzania rozwiązaniem antywirusowym z Elementami XDR, antyspam, uwierzytelniania wieloskładnikowego.

ESET Client & Network Security Administrator

ESET Inspect - Administrator XDR

Czas trwania 1 szkolenia: 3 dni, tj. łącznie 21 godzin

Ilość szkoleń: 2

1. Różnice pomiędzy ESET PROTECT ON-PREM i ESET PROTECT,
2. Różnice pomiędzy EEA i EES,
3. Przydatne strony WWW,
4. ESET PROTECT Hub – licencjonowanie (ćwiczenie),
5. ESET PROTECT ON-PREM - architektura i omówienie komponentów,
6. Instalacja i aktualizacja serwera ESET PROTECT ON-PREM (ćwiczenie),
7. ESET PROTECT ON-PREM - omówienie funkcji serwera,
8. Zarządzanie administratorami i ich uprawnieniami (ćwiczenie),
9. Zdalna instalacja i omówienie możliwości wdrażania komponentów ESET (ćwiczenie),
10. Grupy statyczne i dynamiczne,
11. Zadania klienta, serwera oraz wyzwalacze,
12. Typowe scenariusze (ćwiczenia),
13. Omówienie funkcji podstawowych i zaawansowanych klienta EES,
14. Ochrona antywirusowa,
15. Zarządzanie aktualizacją,
16. Polityki i dziedziczenie (ćwiczenie),
17. ESET Bridge,
18. Zapora osobista (ćwiczenie),
19. Typowe scenariusze (ćwiczenia),
20. Moduł antyspamowy,
21. Powiadomienia,
22. Raportowanie (ćwiczenie),
23. Kontrola dostępu do stron internetowych (ćwiczenie),
24. Kontrola dostępu do urządzeń (ćwiczenie),
25. Migracja ESET PROTECT ON-PREM do ESET PROTECT (ćwiczenie),
26. Wdrożenie klienta ESET Endpoint Security for Android (ćwiczenie),
27. Omówienie pojęcia Extended Detection & Respond (XDR),
28. Architektura produktu ESET INSPECT ON-PREM,
29. Wdrożenie serwera ESET INSPECT ON-PREM (ćwiczenie),
30. Wdrożenie i konfiguracja ESET INSPECT CONNECTOR (ćwiczenie),
31. Omówienie funkcji ESET INSPECT ON-PREM,
32. Generowanie detekcji i ich analiza (ćwiczenie),
33. Reguły i automatyzacja (ćwiczenie),
34. Raportowanie, powiadomienia i zarządzanie uprawnieniami,

- 35. Rozwiązywanie problemów,
- 36. Dobre praktyki,
- 37. Pytania i odpowiedzi.

Opis przedmiotu zamówienia

Część 2 zamówienia:

1. Szkolenie z zakresu administracji i zarządzania urządzeniami klasy UTM, z uwzględnieniem uczestnictwa w warsztatach technicznych.

FORTIGATE -kompleksowe bezpieczeństwo sieci komputerowej wraz z zaawansowaną konfiguracją urządzenia.

Czas trwania 1 szkolenia: **3 dni**, tj. łącznie 24 godziny

Ilość szkoleń: **2**

1. **Fizyczna budowa urządzeń FortiGate**
2. **Wstępna konfiguracja urządzenia FortiGate**
 - a. Tryby pracy NAT/Transparent
 - b. Konfiguracja sieci i routingu
 - c. System Dashboard i moduły systemu
 - d. Administracja urządzeniem (WWW, CLI)
3. **Polityki zapory sieciowej**
 - a. Koncepcja firewall w urządzeniach FortiGate
 - b. Tworzenie obiektów dla reguł firewall
 - c. Translacja adresów NAT i Virtual IP
 - d. Internet Service Database
4. **Inspekcja ruchu SSL i metody dystrybucji certyfikatów**
5. **Omówienie trybów pracy urządzenia –Proxy i Flow**
6. **Logowanie i powiadomienia**
7. **Korzystanie z FortiCloud**
8. **FortiView**
9. **Wprowadzenie do Security Fabric**
 - a. FabricConnectors
10. **Konfiguracja funkcji ochronnych (profile bezpieczeństwa)**Ochrona antywirusowa i integracja z FortiSandbox
 - a. Filtrowanie antyspamowe
 - b. System IPS / DoSPolicy
 - c. Kontrola ruchu WWW / blokowanie URL / DNS Filter
 - d. Kontrola aplikacji
 - e. Reputacja klienta
 - f. Web Application Firewall (WAF)
11. **Optymalizacja ruchu sieciowego (kształtowanie pasma)**
12. **Konfiguracja połączeń SSL VPN**
13. **Konserwacja i bieżąca obsługa systemu**
14. **Architektura urządzenia**
15. **VDOM -Wirtualizacja w obrębie urządzenia**
 - a. Wykorzystanie trybów pracy NAT / Transparent
16. **Zaawansowana konfiguracja sieci i routingu**
 - a. Tworzenie sieci VLAN
 - b. Routing dynamiczny
 - c. Pojęcie Policy Routingu
 - d. SD-WAN -LoadBalancing oraz redundancja łącz Internetowych

17. **Uwierzytelnianie użytkowników**
 - a. Integracja z usługami katalogowymi –FSSO
 - b. Tworzenie reguł firewall w oparciu o grupy użytkowników
 - c. Konta użytkowników gości
 - d. Dwuskładnikowa autoryzacja –FortiToken
18. **Identyfikacja urządzeń**
19. **EndpointControl**
 - a. Integracja z aplikacją FortiClient
20. **CooperativeSecurity Fabric**
 - a. Integracja urządzeń z portfolio Fortinet
 - b. Automatyzacja
21. **Wirtualne sieci prywatne -VPN**
 - a. IPSecVPN site-to-site, client-to-site
 - b. VXLAN
 - c. ADVPN
22. **Diagnostyka i rozwiązywanie problemów**
23. **Konfiguracja urządzeń do pracy w klastrze HA**
 - a. Tryby pracy klastra
 - b. Topologia połączeń i konfiguracja urządzeń

Opis przedmiotu zamówienia

Część 3 zamówienia:

1. Szkolenie z zakresu administracji i zarządzania systemem tworzenia i zarządzania kopii zapasowych oraz ich testowania i przywracania.

Veeam® Backup & Replication™ konfiguracja, zarządzanie oraz przywracanie

Czas trwania 1 szkolenia: **4 dni**, tj. łącznie 32 godziny

Ilość szkoleń: **2**

Strategie ochrony danych

Przegląd kluczowych strategii ochrony danych, zapewniających bezpieczeństwo przechowywanych informacji.

Scenariusze ryzyka

Analiza różnych scenariuszy ryzyka, z jakimi można spotykać się na co dzień w środowisku IT i jakie zagrożenia mogą wpłynąć na bezpieczeństwo danych.

Podstawowe komponenty

Przegląd składników Veeam Backup & Replication wymaganych w większości wdrożeń, ich funkcje oraz minimalne wymagania systemowe.

Początkowe rozważania bezpieczeństwa

Opis strategii oraz narzędzi zabezpieczających serwer kopii zapasowych Veeam przed nieautoryzowanym dostępem i potencjalnymi wyciekami danych.

Kopia zapasowa maszyn wirtualnych

Skuteczna ochrona maszyn wirtualnych VMware i Hyper-V, zapewniająca zgodność z umowami SLA, poprzez tworzenie zadań kopii zapasowych.

Kopia zapasowa agenta

Zastosowanie grup ochrony do automatycznej instalacji agentów Veeam i ochrony obciążeń za pomocą zadań backupowych realizowanych przez agentów.

Kopia zapasowa danych nieustrukturalizowanych

Wymagane składniki oraz funkcjonalności służące do ochrony danych nieustrukturalizowanych, takich jak pliki czy dane multimedialne.

Optymalizacje kopii zapasowych

Analiza opcji i ustawień umożliwiających optymalizację przechowywania danych w kopiach zapasowych, przyspieszenie procesu backupu oraz zapewnienie spójności danych.

Niezmienność i wzmocnione repozytoria

Opis mechanizmów ochrony danych backupowych przed przedwczesnym usunięciem oraz nieautoryzowanymi modyfikacjami. Omówienie cech i etapów wdrożenia wzmocnionych repozytoriów Linux w celu zapewnienia niezmienności danych kopii zapasowych.

Magazyn obiektowy

Analiza korzyści płynących z przechowywania kopii zapasowych w magazynie obiektowym, dostępnych rozwiązań oraz uwag związanych z konfiguracją repozytoriów obiektowych.

Tryby transportu

Omówienie różnych metod transportu danych z środowiska produkcyjnego, ich zalet oraz specyficznych kwestii, które należy uwzględnić przy wyborze metody.

Kopie zapasowe

Zabezpieczenie procesów odzyskiwania danych oraz przestrzeganie zasady 3-2-1 poprzez zastosowanie zadań tworzenia kopii zapasowych.

Scale-out Backup Repository™

Opis architektury oraz zasad zarządzania Scale-out Backup Repository, w tym polityki rozmieszczania danych, warstwy danych oraz zarządzanie repozytoriami.

Migracja lub kopiowanie kopii zapasowych

Identyfikacja przypadków użycia migracji obciążeń i kopii zapasowych przy użyciu narzędzia VeeamMover.

Replikacja

Opis przypadków użycia oraz architektury zadań replikacji oraz polityk Continuous Data Protection (CDP) w kontekście ochrony danych.

Weryfikacja odzyskiwalności

Tworzenie zautomatyzowanych testów w celu zapewnienia odzyskiwalności danych z kopii zapasowych i replik.

Veeam Backup Enterprise Manager

Opis przypadków użycia dla narzędzia Veeam Backup Enterprise Manager, w tym jego funkcjonalności i zalet w zarządzaniu infrastrukturą backupową.

Planowanie odpowiedzi na incydenty

Integracja rozwiązania Veeam Backup & Replication w ramach planu reagowania na incydenty IT.

Scenariusze odzyskiwania i funkcje

Analiza różnych metod odzyskiwania danych oraz wpływ wyboru odpowiedniego scenariusza odzyskiwania na całość procesu.

Przeprowadzanie odzyskiwania

Ćwiczenie procesu odzyskiwania danych przy użyciu różnych metod i typów danych w oparciu o scenariusze awaryjne.

Veeam Data Platform

Identyfikacja i wyjaśnienie celu oraz funkcji każdego z głównych produktów w ramach platformy Veeam Data, wraz z przykładowymi przypadkami użycia tych rozwiązań.

Opis przedmiotu zamówienia

Część 4 zamówienia:

1. Szkolenie w zakresie rozwiązań zarządzania LOG-ami - obsługa, administrowanie i zarządzanie, z uwzględnieniem uczestnictwa w warsztatach technicznych.

Analiza Logów i ruchu sieciowego. IT Monitoring & Hardening

Czas trwania 1 szkolenia: **1 dzień**, tj. 7 godzin

Ilość szkoleń: **2**

Wprowadzenie

- Znaczenie monitorowania systemów informatycznych
- Logi w kontekście cyberbezpieczeństwa
- Wykrywanie nieautoryzowanego dostępu
- Monitorowanie aplikacji
- Reakcje na zdarzenia

Windows – Monitorowanie i analiza logów

- Wprowadzenie do systemu Windows w kontekście bezpieczeństwa
- Monitorowanie aktywności użytkowników i aplikacji w systemie Windows
- Analiza logów w Windows Event Viewer: Security Logs, Application Logs
- Podstawowe komendy systemowe, cmd & powershell
- Analiza zdarzeń związanych z bezpieczeństwem
- Lab

Linux – Monitorowanie i analiza logów

- Wprowadzenie do systemu Linux z perspektywy bezpieczeństwa
- Analiza podstawowych logów systemowych: /var/log/auth.log, /var/log/syslog
- Monitorowanie działań użytkowników w systemie Linux
- Podstawowe komendy systemowe i narzędzia analityczne w Linuxie
- Lab

Hardening systemów

- Wprowadzenie do hardeningu systemów Windows i Linux
- Zasady zabezpieczania systemów operacyjnych i usług
- Podstawowe komendy sieciowe (ping, tracer, nslookup, netstat, tcpdump i inne).
- Analiza ruchu sieciowego - Wireshark
- Najlepsze praktyki w zakresie zabezpieczania systemów przed atakami
- Lab

AV/EDR – Analiza logów i wykrywanie zagrożeń

- Wprowadzenie do ESET Inspect jako narzędzia EDR (Endpoint Detection and Response)
- Analiza logów z ESET Inspect: wykrywanie podejrzanych działań
- Interpretacja zdarzeń bezpieczeństwa w logach antywirusowych
- Praktyczne ćwiczenia w analizie logów ESET i identyfikacji zagrożeń

2. Szkolenie z zakresu administracji sieciami komputerowymi i rozwiązaniami kryptograficznymi, z uwzględnieniem uczestnictwa w warsztatach technicznych.

System zabezpieczeń infrastruktury teleinformatycznej

Czas trwania 1 szkolenia: 2 dni, tj. łącznie 16 godzin

Ilość szkoleń: 2

Zapoznanie z elementami podatnymi na niebezpieczeństwo oraz metodami ich wykorzystywania przez intruza

Przewidywanie zagrożeń bezpieczeństwa na podstawie modelu STRIDE

- tworzenie planu zarządzania ryzykiem
- projektowanie zabezpieczeń dla zasobów fizycznych
- wyznaczenie zagrożeń i analiza ryzyka w sieci

Wyznaczenie zagrożeń i analiza ryzyka dla kont w organizacji

- projektowanie zabezpieczeń kont – polityki blokowania konta, granularne zasady haseł
- wyznaczenie zagrożeń i analiza ryzyka dla procesu uwierzytelniania

Typowe zagrożenia usług katalogowych i DNS oraz zastosowanie metod zabezpieczających te usługi

- znaczenie i ograniczenia funkcjonalności Credential Guard w systemach Windows
- działanie i konfiguracja DNSSEC

Wyznaczenie zagrożeń, projektowanie zabezpieczeń i analiza ryzyka dla danych

- implementacja i konfiguracja Encrypted File System i Bitlocker w oparciu o dobre praktyki

Wyznaczenie zagrożeń, projektowanie zabezpieczeń i analiza ryzyka dla transmisji danych

Projektowanie polis inspekcji dostępu do zasobów

Analiza ryzyka tworzonego przez użytkowników sieci, projektowanie polityki bezpiecznego używania komputera

Analiza ryzyka zarządzania siecią, projektowanie polityki bezpieczeństwa dla zarządzania siecią

Elementy kryptografii

- sposoby wykorzystania kryptografii do zabezpieczania informacji
- metody szyfrowania
- zabezpieczanie informacji w organizacji przy użyciu uwierzytelniania oraz kontroli dostępu

Dystrybucja i zarządzanie certyfikatami, tworzenie struktury PKI

- zabezpieczanie transmisji danych (SSL/TLS)
- implementacja zabezpieczeń dla typowych metod transmisji danych (IPSec), i uwierzytelniania do sieci bezprzewodowych (RADIUS/WPA2-Enterprise)
- dystrybucja i wykorzystanie kart inteligentnych w środowisku Windows

Identyfikacja, odpowiedź na incydenty oraz asystowanie przy formalnym śledztwie w przypadku włamania

Opis przedmiotu zamówienia

Część 5 zamówienia:

1. Szkolenie w zakresie rozwiązań SIEM - obsługa, administrowanie i zarządzanie, z uwzględnieniem uczestnictwa w warsztatach technicznych.

SIEM WAZUH

Czas trwania 1 szkolenia: **3 dni**, tj. łącznie 24 godziny

Ilość szkoleń: **2**

1. Wprowadzenie do Wazuha:
 - a) Co to jest Wazuh i jakie problemy rozwiązuje.
2. Przegląd architektury Wazuha.
 - a) Przygotowanie środowiska:
 - b) Wymagania systemowe.
 - c) Przygotowanie maszyny wirtualnej i fizycznej z systemem Linux.
3. Instalacja Wazuha:
 - a) Pobieranie i instalacja serwera Wazuh.
 - b) Konfiguracja bazowa i instalacja dodatków.
4. Podstawowa konfiguracja:
 - a) Konfiguracja agenta Wazuh na systemach Linux i Windows.
 - b) Testowanie połączenia, tuning bazowy.
 - c) Konfiguracja agenta w trybie Agentless (Syslog oraz SSH)
5. Zaawansowana konfiguracja:
 - a) Konfiguracja reguł i polityk bezpieczeństwa.
 - b) Tworzenie i modyfikacja dekodów.
6. Troubleshooting:
 - a) Rozwiązywanie typowych problemów z instalacją i konfiguracją.
 - b) Analiza logów i błędów.
7. Zarządzanie użytkownikami:
 - a) Tworzenie kont użytkowników i zarządzanie nimi w Wazuhu.
 - b) Konfiguracja ról i uprawnień użytkowników.
 - c) Implementacja polityk bezpieczeństwa dla użytkowników.
 - d) Audyt i monitorowanie działań użytkowników.
8. Bezpieczeństwo systemu:
 - a) Zabezpieczenie komunikacji między komponentami Wazuha (SSL/TLS).
 - b) Konfiguracja i zarządzanie zaporami sieciowymi.
 - c) Implementacja polityk bezpieczeństwa systemu operacyjnego.
 - d) Monitorowanie i reakcja na próby naruszenia bezpieczeństwa.
9. Backup i przywracanie danych:
 - a) Strategie tworzenia kopii zapasowych dla Wazuha.
 - b) Konfiguracja automatycznego backupu.
 - c) Procedury przywracania danych w przypadku awarii.
10. Analiza i raportowanie:

- a) Tworzenie niestandardowych raportów bezpieczeństwa.
 - b) Konfiguracja powiadomień i alertów dotyczących naruszeń bezpieczeństwa.
 - c) Analiza logów pod kątem wykrywania potencjalnych zagrożeń.
11. Wprowadzenie do podstawowych pojęć i zagrożeń.
 12. Wykrywanie i reagowanie na incydenty:
 - a) Tworzenie reguł detekcji i zarządzanie nimi.
 - b) Analiza i reagowanie na alerty.
 13. Symulacja ataku i analiza jego skutków za pomocą Wazuha.
 14. Przykłady realnych incydentów i reagowania na nie.
 15. Prezentacja modułu zarządzania podatnościami - Wazuh Cyber Threat Intelligence [CTI].
 16. Wprowadzenie do instalacji klastrowej:
 - a) Korzyści z użycia klastra.
 - b) Przegląd architektury klastrowej.
 17. Instalacja klastra:
 - a) Konfiguracja węzłów klastra.
 - b) Load balancing i redundancja.
 18. Skalowanie i optymalizacja:
 - a) Monitorowanie wydajności.
 - b) Optymalizacja konfiguracji pod kątem wydajności.
 19. Integracja z usługami zewnętrznymi:
 - a) Wykrywanie sygnatur za pomocą YARA
 - b) Wzbogacanie komunikatów za pomocą LLM / AI
 - c) Automatyzacja za pomocą Ansible
 - d) Integracja innych rozwiązań za pomocą API
 20. Integracja Wazuha z lokalnym LLM
 21. Monitorowanie zdarzeń w kontenerach
 22. Monitorowanie infrastruktury chmurowej
 23. Aktualizacja agentów przez polityki GPO
 24. Monitorowanie wydajności, metryk i procesów
 25. Optymalizacja indeksów i zapytań
 26. Dobre praktyki utrzymania klastra w dobrym stanie
 27. Implementacja Cross-Cluster Search
 28. Optymalizacja retencji danych i zarządzanie logami
 29. Integracja z Grafana
 30. Integracja z MISP
 31. Integracja z Suricata
 32. Integracja z Zabbix
 33. Integracja z Git
 34. Integracja z Graylog
 35. Integracja z nmap i ChatGPT
 36. Integracja z CDB AlienVault
 37. Integracja z Atlassian Jira
 38. Integracja z Sysmon

Opis przedmiotu zamówienia

Część 6 zamówienia:

1. Szkolenie z zakresu administracji i zarządzania oprogramowaniem do monitorowania oraz zarządzania siecią, audytowania i inwentaryzacji zasobów.

Zarządzanie oprogramowaniem do monitorowania oraz zarządzania siecią, audytowaniem i inwentaryzacją zasobów.

Czas trwania 1 szkolenia: **1 dzień**, tj. 8 godzin

Ilość szkoleń: **2**

- monitorowanie sieci – cele, znaczenie, korzyści
- mapowanie i proaktywne monitorowanie sieci
- jak najlepiej wykorzystać możliwości technologiczne nowoczesnych rozwiązań bezpieczeństwa ICT
- audyt IT – dlaczego warto cyklicznie przeprowadzać audyt bezpieczeństwa teleinformatycznego
- narzędzia wspomagające zarządzanie oprogramowaniem
- inwentaryzacja sprzętu i oprogramowania; efektywne zarządzanie licencjami
- wymogi prawne monitorowania użytkowników, obowiązki i uprawnienia administratora
- kontrolowanie użytkownika aplikacji, monitorowanie dostępu do Internetu
- metody kontroli użytkowników, zbieranie dowodów elektronicznych
- monitorowanie odwiedzanych stron WWW i ich blokowanie
- monitorowanie wiadomości e-mailowych
- ochrona danych przed wyciekiem (zarządzanie urządzeniami przenośnymi oraz portami)
- ochrona przed szkodliwym oprogramowaniem przenoszonym na nośnikach danych (blokowanie portów i nośników).

Opis przedmiotu zamówienia

Część 7 zamówienia:

1. Szkolenie dla kadry kierowniczej oraz pracowników w zakresie cyberbezpieczeństwa i bezpieczeństwa informacji.

Czas trwania 1 szkolenia: **1 dzień**, tj. 6 godzin (w siedzibie Zamawiającego)

Ilość szkoleń: **2**

- podstawy cyberbezpieczeństwa
- grupy cyberprzestępcze i ich działanie
- zagrożenia ze strony cyberprzestępców
- co dają cyberprzestępcom dane użytkowników
- rodzaje ataków na pracowników biurowych
- straty dla firmy pod względem cyberataków
- sieci typu botnet
- metody ochrony przed cyberatakami
- sztuczna inteligencja (AI) w atakach
- zagadnienia: SPAM, Phishing
- ataki: DDoS, DoS, 0-day
- poczta elektroniczna i załączniki
- bezpieczeństwo haseł
- metody socjotechniczne
- kradzież tożsamości
- bezpieczeństwo fizyczne w miejscu pracy
- pamięci przenośne "znalezione" w pobliżu miejsca pracy lub pozyskane w inny sposób
- sprzęt firmowy oraz prywatny - różnice
- pytania słuchaczy i odpowiedzi

Umowa (wzór)

Nr

zawarta w dniu w Pisz, pomiędzy Powiatem Piskim, z siedzibą ul. Warszawska 1, 12-200 Pisz, zwanym dalej „Zamawiającym”, reprezentowanym przez:

...

a

...

zwanym dalej „Wykonawcą” reprezentowanym przez:

...

Na podstawie dokonanego przez Zamawiającego wyboru oferty złożonej w zapytaniu ofertowym na usługę przeprowadzenia szkoleń w ramach realizacji projektu pn. „Wzmocnienie Systemu Cyberbezpieczeństwa w Starostwie Powiatowym w Pisz, uwzględniając rozwiązania organizacyjne, kompetencyjne i techniczne”, który otrzymał dofinansowanie z Programu Operacyjnego Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. - Wzmocnienie krajowego systemu cyberbezpieczeństwa w ramach konkursu grantowego „Cyberbezpieczny Samorząd” o nr FERC.02.02-CS.01-001/23, zawarto umowę o następującej treści:

§1 PRZEDMIOT UMOWY

1. Przedmiotem umowy jest:

Usługa przeprowadzenia szkoleń w formie on-line:

– **Część 1** w następującym zakresie:

- Szkolenie z zakresu administracji i zarządzania SO Windows Server, z uwzględnieniem uczestnictwa w warsztatach technicznych;
- Szkolenie z zakresu administracji i zarządzania SO Linux, z uwzględnieniem uczestnictwa w warsztatach technicznych, zgodnie z załącznikiem;
- Szkolenie z zakresu administracji i zarządzania systemami wirtualizacji, z uwzględnieniem Uczestnictwa w warsztatach technicznych;
- Szkolenie z zakresu administracji i zarządzania rozwiązaniem antywirusowym z Elementami XDR, antyspam, uwierzytelniania wieloskładnikowego, zgodnie z załącznikiem nr **2a** zapytania ofertowego,

– **Część 2** w następującym zakresie,

- Szkolenie z zakresu administracji i zarządzania urządzeniami klasy UTM, z uwzględnieniem uczestnictwa w warsztatach technicznych, zgodnie z załącznikiem nr **2b** zapytania ofertowego;
- **Część 3** w następującym zakresie,
 - Szkolenie z zakresu administracji i zarządzania systemem tworzenia i zarządzania kopii zapasowych oraz ich testowania i przywracania, zgodnie z załącznikiem nr **2c** zapytania ofertowego;
- **Część 4** w następującym zakresie,
 - Szkolenie w zakresie rozwiązań zarządzania LOG-ami - obsługa, administrowanie i zarządzanie, z uwzględnieniem uczestnictwa w warsztatach technicznych,
 - Szkolenie z zakresu administracji sieciami komputerowymi i rozwiązaniami kryptograficznymi, z uwzględnieniem uczestnictwa w warsztatach technicznych, zgodnie z załącznikiem nr **2d** zapytania ofertowego;
- **Część 5** w następującym zakresie,
 - Szkolenie w zakresie rozwiązań SIEM - obsługa, administrowanie i zarządzanie, z uwzględnieniem uczestnictwa w warsztatach technicznych, zgodnie z załącznikiem nr **2e** zapytania ofertowego;
- **Część 6** w następującym zakresie,
 - Szkolenie z zakresu administracji i zarządzania oprogramowaniem do monitorowania oraz zarządzania siecią, audytowania i inwentaryzacji zasobów, zgodnie z załącznikiem nr **2f** zapytania ofertowego;

oraz stacjonarnie w siedzibie Zamawiającego:

- **Część 7** w następującym zakresie,
 - Szkolenie dla kadry kierowniczej oraz pracowników w zakresie cyberbezpieczeństwa i bezpieczeństwa informacji, zgodnie z załącznikiem nr **2g** zapytania ofertowego.
2. Wykonawca oświadcza, że posiada uprawnienia, niezbędną wiedzę, kwalifikacje i doświadczenie do należytego przeprowadzenia szkolenia będącego przedmiotem niniejszej umowy. Wykonawca oświadcza, że dysponuje potencjałem technicznym i osobami z odpowiednimi uprawnieniami zdolnymi do prawidłowej realizacji przedmiotu umowy.
 3. Szkolenie/szkolenia odbędą się zgodnie z harmonogramem, który zostanie przedstawionym przez Wykonawcę w terminie do 7 dni od dnia podpisania umowy. Dla każdego szkolenia (o jednej tematyce) Wykonawca proponuje co najmniej trzy różne, niepokrywające się terminy do wyboru przez Zamawiającego. Zamawiający (dla szkolenia o jednej tematyce) dokona wyboru dwóch z proponowanych terminów w ciągu 7 dni od otrzymania harmonogramu.
 4. Wykonawca oświadcza, że jest autorem materiałów dydaktycznych będących utworami w rozumieniu ustawy o prawie autorskim i prawach pokrewnych, wytworzonymi w ramach realizacji niniejszej umowy i przysługują mu wyłączne i nieograniczone autorskie prawa majątkowe do tych utworów.

5. Wykonawca zobowiązuje się, że realizując przedmiot Umowy nie naruszy praw majątkowych osób trzecich.
6. Oferta wykonawcy z dnia stanowi **załącznik nr 1** do niniejszej umowy i jednocześnie jej integralną część.

§ 2 WYNAGRODZENIE

1. Za wykonanie przedmiotu umowy Zamawiający zapłaci Wykonawcy wynagrodzenie w kwocie (słownie:) złotych brutto, w tym:
 - Część 1 -zł brutto
 - Część 2 -zł brutto
 - Część 3 -zł brutto
 - Część 4 -zł brutto
 - Część 5 -zł brutto
 - Część 6 -zł brutto
 - Część 7 -zł brutto
2. Wynagrodzenie wskazane w ustępie poprzedzającym jest ostateczne i nie podlega żadnym zmianom oraz zawiera wszelkie koszty Wykonawcy związane z realizacją przedmiotu umowy.
3. Wynagrodzenie zostanie wypłacone przelewem na wskazany rachunek bankowy, w terminie 14 dni od daty otrzymania przez zamawiającego faktury.
4. Wykonawca oświadcza, że wskazany na fakturze rachunek bankowy jest jego rachunkiem rozliczeniowym, służącym wyłącznie do celów rozliczeń z tytułu prowadzonej przez niego działalności gospodarczej oraz rachunek ten znajduje się w elektronicznym wykazie podmiotów prowadzonym przez szefa Krajowej Administracji Skarbowej (biała lista), o którym mowa w art. 96 b ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług.
5. Niespełnienie warunku, o którym mowa powyżej spowoduje wydłużenie terminu zapłaty faktury o liczbę dni liczoną od dnia stwierdzenia braku numeru rachunku w elektronicznym wykazie podmiotów prowadzonym przez szefa Krajowej Administracji Skarbowej (biała lista) do dnia jego faktycznego umieszczenia w tym wykazie w wyniku odpowiednich działań Wykonawcy, w sposób umożliwiający jego potwierdzenie. Powyższe stanowi okoliczność leżącą po stronie Wykonawcy i jest równoznaczne ze zwłoką wierzyciela.
6. Zamawiający oświadcza, że będzie realizować płatności za faktury z zastosowaniem mechanizmu podzielonej płatności, tzw. split payment.
7. Podzieloną płatność, tzw. split payment stosuje się wyłącznie przy płatnościach bezgotówkowych, realizowanych za pośrednictwem polecenia przelewu lub polecenia zapłaty dla czynnych podatników VAT. Mechanizm podzielonej płatności nie będzie wykorzystywany

do zapłaty za czynności lub zdarzenia pozostające poza zakresem VAT (np. zapłata odszkodowania), a także za świadczenia zwolnione z VAT, opodatkowane stawką 0%.

8. Wykonawca oświadcza, że przyjmuje do wiadomości dokonywanie przez Zamawiającego płatności w systemie podzielonej płatności.
9. Wykonawca oświadcza, że numer rachunku rozliczeniowego wskazany we wszystkich fakturach, które będą wystawione w jego imieniu, jest rachunkiem dla którego zgodnie z rozdziałem 3a ustawy z dnia 29 sierpnia 1997 r. - Prawo bankowe prowadzony jest rachunek VAT.
10. Za datę zapłaty przyjmuje się datę obciążenia rachunku zamawiającego.
11. Za nieterminowe płatności faktur wykonawca ma prawo naliczyć odsetki ustawowe za opóźnienie.

§3 WARUNKI I TERMIN REALIZACJI USŁUGI

1. Przedmiot umowy wskazany w §1 ust. 1 zostanie zrealizowany w terminie do **15.12.2025 r.**
2. Prawidłowe wykonanie przedmiotu umowy zostanie potwierdzone przez Strony podpisanym protokołem odpowiadającym realizowanej części zamówienia.
3. Jeżeli podczas czynności potwierdzenia realizacji usługi Zamawiający stwierdzi wady lub niezgodność co do treści realizowanej usługi odmówi czynności potwierdzenia realizacji usługi i wyznaczy Wykonawcy dodatkowy, 2-dniowy termin na wykonanie przedmiotu umowy, co nie wyłącza prawa Zamawiającego do naliczenia kar umownych z tytułu opóźnienia Wykonawcy w realizacji umowy. W takim wypadku zostanie sporządzony protokół, w którym Strony opiszą stwierdzone uchybienia i wady oraz potwierdzą dodatkowy termin wyznaczony przez Zamawiającego zgodnie ze zdaniem poprzedzającym.
4. Upoważnionymi do dokonania czynności potwierdzenia realizacji usługi są:
 - 1) po stronie Zamawiającego:, nr tel.:, e-mail:
 - 2) po stronie Wykonawcy:, nr tel.:, e-mail:

§4 ODSTĄPIENIE OD UMOWY

1. Zamawiający ma prawo odstąpić od umowy jeżeli Wykonawca nie wykona usługi lub nie usunie wad i uchybień stwierdzonych w toku czynności potwierdzenia realizacji usługi zgodnie z §3 ust. 3 – w terminie 7 dni od dnia upływu wyznaczonego terminu dodatkowego.
2. Oświadczenie o odstąpieniu od umowy wymaga formy pisemnej pod rygorem nieważności.
3. Poza przypadkami określonymi w Kodeksie Cywilnym Zamawiający może odstąpić od umowy, jeżeli:
 - 1) wystąpią istotne zmiany powodujące, że wykonanie zamówienia nie leży w interesie publicznym, czego nie można było przewidzieć w chwili zawarcia umowy

- 2) wykonawca przystąpił do likwidacji swojej firmy, z wyjątkiem likwidacji przeprowadzanej w celu przekształcenia – zamawiający może odstąpić od umowy w terminie 10 dni od dnia powzięcia informacji o tych okolicznościach.
- 3) wykonawca pomimo uprzednich pisemnych zastrzeżeń Zamawiającego nie wykonuje przedmiotu Umowy zgodnie z warunkami umownymi lub w rażący sposób zaniedbuje zobowiązania umowne - zamawiający może odstąpić od umowy w terminie 10 dni od dnia doręczenia pisemnych zastrzeżeń Wykonawcy.
4. W razie istotnej zmiany okoliczności powodującej, że wykonanie umowy nie leży w interesie publicznym, czego nie można było przewidzieć w chwili zawarcia umowy, Zamawiający może odstąpić od umowy w terminie 30 dni od powzięcia wiadomości o tych okolicznościach.

§5 KARY UMOWNE

1. Wykonawca zapłaci Zamawiającemu karę umową w następujących przypadkach i wysokościach:
 - 1) za każdy dzień opóźnienia w wykonaniu umowy ponad termin wskazany w §3 ust. 1, w wysokości 0,5 % wynagrodzenia brutto umowy, o którym mowa w § 2 ust. 1, za każdy rozpoczęty dzień zwłoki,
 - 2) za naruszenie przez Wykonawcę obowiązków, o których mowa w §6 niniejszej umowy, w wysokości 1 000 zł, za każdy stwierdzony przypadek naruszenia.
 - 3) w przypadku odstąpienia Zamawiającego lub Wykonawcy od umowy z przyczyn leżących po stronie Wykonawcy, w wysokości 5% wynagrodzenia brutto umowy, o którym mowa w § 2 ust. 1.
2. W przypadku, gdy powstała szkoda przewyższa ustanowioną karę umowną, Zamawiający ma prawo żądać odszkodowania uzupełniającego na zasadach ogólnych.

§6 OCHRONA TAJEMNICY PRZEDSIĘBIORSTWA

1. Strony zobowiązują się do utrzymania w tajemnicy i nie przekazywania osobom trzecim informacji poufnych.
2. W razie wątpliwości, czy określona informacja stanowi informację poufną, zainteresowany zobowiązany jest zwrócić się do drugiej strony o wyjaśnienie takiej wątpliwości.
3. Obowiązek zachowania tajemnicy nie dotyczy obowiązku ujawniania informacji poufnych, wynikającego z bezwzględnie obowiązujących przepisów prawa. W przypadku konieczności ujawnienia informacji poufnej, strona zobowiązana do jej ujawnienia zgodnie z niniejszym ustępem, zawiadomi drugą stronę o zakresie i warunkach takiego ujawnienia.
4. Obowiązek zachowania tajemnicy informacji poufnych obciąża strony przez okres obowiązywania umowy, a także po jej wygaśnięciu, przez okres 5 (pięć) lat.

5. Każda ze stron obowiązana jest zorganizować i utrzymywać takie środki bezpieczeństwa i sposoby postępowania, jakie w praktyce będą możliwe i rozsądne, dla zapewnienia bezpiecznego przechowywania informacji poufnych otrzymanych od drugiej strony, a także dołożyć wszelkich starań by zapobiec jakimkolwiek nieautoryzowanemu wykorzystaniu, ujawnieniu, czy dostępowi do tych informacji poufnych.

§7 ZMIANY POSTANOWIEŃ UMOWY

1. W przypadkach przewidzianych w umowie dopuszcza się wprowadzenie zmian za zgodą Zamawiającego. Zmiany przewidziane w umowie mogą być inicjowane przez strony umowy.
2. Zmiany, o których mowa w ust. 1 mogą dotyczyć:
 - a) wstrzymania wykonania całości lub części usług na skutek wystąpienia okoliczności niezależnych od Wykonawcy,
 - b) zmiany dopuszczającej do realizacji części zamówienia podwykonawcy w sytuacji nieprzewidzianej, po wcześniejszym uzgodnieniu z Zamawiającym,
 - c) zmiany spowodowanej okolicznościami siły wyższej lub powstałej z winy osób trzecich,
 - d) zmiany w przepisach ustawowych i aktach wykonawczych związanych z przedmiotem zamówienia, które nastąpiły po dniu zawarcia umowy, w tym zmiany stawki podatku VAT.
3. Zmiana postanowień umowy w stosunku do treści oferty Wykonawcy jest możliwa poprzez przedłużenie terminu zakończenia zamówienia o okres odpowiadający wstrzymaniu lub opóźnieniu realizacji usługi w przypadku:
 - a) działania siły wyższej (np. klęski żywiołowe, strajki generalne lub lokalne, działań wojennych), mające bezpośredni wpływ na terminowość zakończenia usług,
 - b) wystąpienia okoliczności, których strony umowy nie były w stanie przewidzieć, pomimo zachowania należytej staranności,
 - c) działań osób trzecich lub organów władzy publicznej, które spowodują przerwanie lub czasowe zawieszenie realizacji zamówienia.
4. Zmiana postanowień umowy w stosunku do treści oferty Wykonawcy jest możliwa poprzez zmianę sposobu wykonania przedmiotu umowy w przypadku:
 - a) konieczności zrealizowania jakiegokolwiek części usługi, objętej przedmiotem umowy, przy zastosowaniu odmiennych rozwiązań, niż wskazane w zapytaniu ofertowym.
 - b) zaistnienia innych okoliczności prawnych, ekonomicznych lub technicznych, skutkujących niemożliwością wykonania lub należytego wykonania umowy zgodnie z jej postanowieniami.
5. Dokonanie zmian wymaga podpisania przez strony aneksu do umowy.
6. Zamawiający przewiduje możliwość zmiany harmonogramu, o którym mowa w §1 ust. 3 umowy. Zmiana harmonogramu nie wymaga podpisania aneksu do umowy.

§8 POSTANOWIENIA KOŃCOWE

1. Ewentualne spory, wynikłe w związku z realizacją przedmiotu umowy, strony zobowiązują się rozwiązywać na drodze wspólnych negocjacji, a przypadku niemożności ustalenia kompromisu spory będą rozstrzygane przez Sąd Powszechny właściwy dla siedziby Zamawiającego.
2. Wszelkie polecenia wydawane Wykonawcy przez Zamawiającego, jak również zapytania i odpowiedzi dotyczące realizacji niniejszej umowy wymagają formy pisemnej.
3. W sprawach nie uregulowanych niniejszą umową mają zastosowanie przepisy kodeksu cywilnego.
4. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach, po 1 dla każdej ze stron.

WYKONAWCA

ZAMAWIAJĄCY