OR.2600.04.2025

Lębork ,dnia 28.01.2025 r.

ZAPYTANIE OFERTOWE

NAZWA ORAZ ADRES ZAMAWIAJĄCEGO
Powiat Lęborski, ul. Czołgistów 5, 84-300 Lębork, tel.: (59) 8632 825, faks: (59) 8632 850, e-mail: sekretariat@starostwolebork.pl, adres strony internetowej: www.powiat-lebork.com

Tryb udzielenia zamówienia
1.Tryb postępowania:
Postępowanie prowadzone będzie w trybie postępowania ofertowego na udzielenie zamówienia publicznego o wartości poniżej 130 000 zł do którego nie stosuje się przepisów ustawy z dnia 11 września 2019 r. Prawo Zamówień Publicznych (tj.Dz. U. z 2024 r. poz.1320), zgodnie z art. 2 ust.1 pkt 1 ustawy.
2. Niniejsze postępowanie jest zgodne z Regulaminem udzielania zamówień publicznych w Starostwie Powiatowym w Lęborku (Uchwała Nr 304/2021 Zarządu Powiatu Lęborskiego z dnia 3 lutego 2021 r. w sprawie wprowadzenia Regulaminu udzielania zamówień publicznych w Starostwie Powiatowym w Lęborku) *oraz Wytycznymi dotyczącymi kwalifikowalności wydatków na lata 2021-2027*

I. OPIS PRZEDMIOTU ZAMÓWIENIA

Przedmiotem zamówienia jest zakup dostępu do platformy szkoleniowej dla pracowników Starostwa Powiatowego w Lęborku oraz przeprowadzenie szkolenia stacjonarnego dla kadry zarządzającej w ramach projektu „Cyberbezpieczny Samorząd" współfinansowanego z Funduszy Europejskich na Rozwój Cyfrowy (FERC) II Zaawansowane usługi cyfrowe, Działanie 2.2. Wzmocnienie krajowego systemu cyberbezpieczeństwa.

Słownik Zamówień (CPV):
80510000-2 Usługi szkolenia specjalistycznego
79632000-3 Szkolenie pracowników

1.1. Dostęp do platformy szkoleniowej dla pracowników Starostwa.
W ramach realizacji zamówienia Wykonawca zobowiązany będzie do zapewnienia pracownikom Zamawiającego **dostępu do platformy szkoleniowej** na 2 cykle szkoleń, każdy cykl prze okres 1 m-ca. Na platformie szkoleniowej (e-learningowej) zamieszczone będą różnorodne materiały szkoleniowe z zakresu cyberbezpieczeństwa. Materiały szkoleniowe muszą być przez Wykonawcę na bieżąco uzupełniane i aktualizowane, w związku z pojawianiem się nowych zagrożeń i podatności, nowych metod ochrony informacji i narzędzie do tego wykorzystywanych oraz zmieniającej się sytuacji geopolitycznej.
Udostępnienie platformy e-learningowej ma umożliwić pracownikom elastyczny dostęp do aktualnych informacji i standardowych praktyk w dogodnym dla nich czasie, co będzie sprzyjać skutecznej nauce, oraz poszerzenia wiedzy o inne tematy związane z cyberbezpieczeństwem.
Liczba użytkowników platformy – 100
Termin udostępnienia platformy (wraz z całością materiału szkoleniowego):

1 cykl : Otrzymanie dostępu do platformy w ciągu 30 dni od podpisania umowy
2 cykl : Otrzymanie dostępu do platformy w ciągu 90 dni od podpisania umowy.

Okres udostępnienia platformy – 2 x 1 miesiąc

1. Platforma musi spełniać następujące wymagania:
Zawierać minimum 45 szkoleń, dostępnych w języku polskim w postaci filmów i prezentacji, zakończonych testami lub quizami sprawdzającymi przyswojenie przedstawianego materiału merytorycznego.

a) szkolenia muszą zapewniać zakres tematyczny co najmniej w ujęciu:

- ✓ Podstawy bezpiecznego internetu
- ✓ Bezpieczeństwo poczty
- ✓ Załączniki w poczcie elektronicznej
- ✓ Phishing
- ✓ Spyware/malware
- ✓ Bezpieczeństwo danych osobowych RODO/GDRP
- ✓ Bezpieczne hasła
- ✓ Menedżery haseł
- ✓ Bezpieczeństwo urządzeń mobilnych
- ✓ Uwierzytelnianie wieloskładnikowe (MFA)
- ✓ Bezpieczna praca zdalna
- ✓ Bezpieczna praca w biurze
- ✓ Sieci społeczne
- ✓ Zakupy w internecie

b) użytkownicy powinni być podzieleni na grupy, dla których będą przygotowane indywidualne harmonogramy szkoleń oraz dedykowane kampanie phishingowe.

c) łączny czas trwania wszystkich materiałów szkoleniowych w każdym cyklu powinien wynosić co najmniej 8 godzin, czyli 2 cykle po 8 godzin, łącznie min. 16 godz.

d) platforma musi być dostosowana do potrzeb osób z niepełnosprawnościami zgodnie ze standardami WCAG 2.1 (w tym osobna wersja kontrastowa – przełączanie co najmniej na stronie startowej).

2. Dedykowaną platformę phishingową pozwalającą na generowanie i wysyłanie spreparowanych maili phishingowych do wszystkich użytkowników usługi oraz na generowanie, co najmniej, poniższych typów wiadomości e-mail:

a) z linkiem prowadzącym do stronnym internetowej,

b) z linkiem do portalu podszywającego się pod usługodawcę i pozwalającego na logowanie (weryfikację, czy użytkownicy są gotowi na fałszywej stronie portalu zalogować się swoim loginem i hasłem); platforma musi zapewniać bezpieczeństwo takiej operacji,

c) z załącznikiem (szyfrowanym i niezaszyfrowanym) zawierającym potencjalnie niebezpieczny kod,

d) z załącznikiem w postaci dokumentu Word lub Excel zawierającym potencjalnie niebezpieczny kod.

W przypadku, gdy użytkownik pozwoli się oszukać, platforma musi posiadać możliwość automatycznego skierowania takiego użytkownika na dodatkowe szkolenie lub ponowne wykonanie jednego z wcześniej ukończonych szkoleń.

3. Dedykowaną platformę dostarczającą raporty obejmujące minimum:

a) status wykonania szkoleń przez użytkowników, z podziałem na grupy i uwzględnieniem terminu wykonania szkoleń oraz wyniku quizów i testów,

b) status kampanii, wraz z raportem o liczbie wysłanych e-maili oraz szczegółach zwierających informację: kto otworzył wiadomość, kto i kiedy pozwolił się oszukać, kto otworzył załącznik, jaka była platforma z jakiej wykonał tę akację oraz szczegółowe daty wykonania tych operacji.

W ramach świadczonej usługi usługodawca musi:

- przygotować platformę do świadczenia usługi, założyć konta dla użytkowników oraz sprawdzić techniczne elementy związane z zapewnieniem dostarczenia wiadomości phishingowych z platformy do użytkowników,
- zaproponować do akceptacji Zamawiającego szczegółowy harmonogram szkoleń dopasowany do okresu świadczenia usługi,
- zaplanować na podstawie harmonogramu całą kampanię szkoleniową i dostarczyć ją użytkownikom za pośrednictwem dedykowanych wiadomości e-mail,
- dostarczać pełny raport z realizacji szkoleń dla użytkowników oraz przeprowadzonych kampanii po zakończeniu każdego modułu szkoleniowego oraz zbiorcze raporty końcowe,
- wprowadzić zmiany w harmonogramie i zakresie szkoleń w przypadku potrzeby modyfikacji, zmian kolejności szkoleń (2 zmiany miesięcznie) lub liczby użytkowników (nie więcej niż 10% zmian w okresie trwania usługi).

Każdy uczestnik szkolenia otrzyma od Wykonawcy imienny certyfikat potwierdzający ukończenie szkolenia.

Wymagania dodatkowe:

Usługa ma być świadczona z centrum danych znajdującym się na terenie Unii Europejskiej. Dostawca platformy musi zapewnić całkowite usunięcie danych użytkowników po zakończeniu realizacji usługi. Wszystkie moduły (platforma szkoleniowa, platforma phishingowa i moduł raportowania) muszą pochodzić od jednego producenta.

Dla zapewnienia wysokiego poziomu usług, podmiot świadczący usługę musi posiadać certyfikat ISO 9001 w zakresie świadczenia usług. Zgłoszenia i komunikacja z usługodawcą będą przyjmowane w języku polskim w trybie 8x5, przez dedykowany portal serwisowy dostępny w sieci internet oraz infolinię w języku polskim 8x5. Czas reakcji usługodawcy nie może być dłuższy niż 1 godzina – reakcja w postaci połączenia telefonicznego lub odpowiedzi w portalu serwisowym.

Do oferty należy załączyć certyfikat ISO 9001.

1.2. Szkolenia dla kadry zarządzającej Starostwa

1.2. W ramach realizacji zamówienia Wykonawca zobowiązany będzie do przeprowadzenia szkolenia specjalistycznego dla kadry zarządzającej w zakresie bezpieczeństwa informacji i wymogów w zakresie cyberbezpieczeństwa w formie stacjonarnej. Liczba osób – ok. 20

- szkolenie obejmować będzie jeden dzień szkoleniowy w wymiarze 8 godzin zegarowych (1 godzina = 60 minut) **w tym dwie przerwy.**
- szkolenie stacjonarne odbywać się będzie w siedzibie Zamawiającego, w wyznaczonym miejscu spełniającym standardy dostępności.
- szkolenie odbywać się będzie w godzinach pracy Zamawiającego.

Przewidywany termin szkolenia – 20.03.2025 r.

Zamawiający zastrzega sobie prawo do zmiany terminu szkolenia, o czym Wykonawca zostanie poinformowany z 5-dniowym wyprzedzeniem.

Wykonawca zapewni uczestnikom szkoleń:
- zatrudnienie osoby prowadzącej szkolenie
- materiały potrzebne do przeprowadzenia szkolenia

Celem szkoleń jest zwiększenie świadomości kadry kierowniczej Starostwa Powiatowego w Lęborku w zakresie problematyki związanej z bezpieczeństwem informacji, rozwinięcie umiejętności strategicznego zarządzania cyberbezpieczeństwem oraz zrozumienie przepisów prawnych i ich implementacji.
Szkolenia powinny być kompleksowym procesem, który umożliwia uczestnikom zdobycie dogłębnej wiedzy na temat wybranych zagadnień. Powinno ono nie tylko dostarczyć podstawowej informacji, ale także omówić zaawansowane aspekty danej tematyki, aby uczestnicy mieli pełniejsze zrozumienie tematu i byli w stanie zastosować zdobytą wiedzę w praktyce. Przekazywanie wiedzy powinno być interaktywne i angażujące, wykorzystując różnorodne metody nauczania, takie jak prezentacje, dyskusje, studia przypadków czy praktyczne ćwiczenia, co pozwoli uczestnikom efektywniej przyswoić omawiany materiał.
W ramach przeprowadzonych szkoleń wykonawca powinien zaprezentować m.in.:
1. Podstawowe informacje o obecnej sytuacji rynkowej powiązanej z tematyką cyberbezpieczeństwa:
- Podstawy i definicje: zapewnienie uczestnikom solidnych podstaw w dziedzinie cyberbezpieczeństwa poprzez omówienie kluczowych pojęć i zasad. Ponadto, zostanie przedstawiona rola menedżera w formowaniu bezpiecznego środowiska cyfrowego, co pozwoli zrozumieć jak ważne jest aktywne zaangażowanie kierownictwa w procesy zapewnienia bezpieczeństwa informacji. W ten sposób uczestnicy będą mieć pełniejsze zrozumienie zarówno teoretycznych, jak i praktycznych aspektów cyberbezpieczeństwa oraz będą lepiej przygotowani do podejmowania decyzji w tym obszarze.
- Statystyki i trendy: skoncentrowanie się na przekazaniu uczestnikom szczegółowej analizy globalnych i lokalnych danych dotyczących cyberataków. Poprzez omówienie ewolucji tych ataków oraz ich metodologii, uczestnicy zyskają wgląd w aktualne trendy i sposoby działania cyberprzestępców. Ponadto, zostaną przedstawione skutki, jakie cyberatak może mieć dla biznesu, co pozwoli uczestnikom lepiej zrozumieć znaczenie inwestycji w bezpieczeństwo informacji oraz skuteczne zarządzanie ryzykiem cybernetycznym dla organizacji. Dzięki temu będą mogli podejmować bardziej świadome decyzje w zakresie ochrony swoich danych i infrastruktury cyfrowej.
2. Omówienie światowych standardów i norm w zakresie cyberbezpieczeństwa i bezpieczeństwa informacji.
- Normy ISO/IEC: Szczegółowe omówienie serii norm: ISO/IEC 27000: (zarysowuje leksykon oraz globalne zasady nadrzędne systemu zarządzania bezpieczeństwem informacji, kreśląc fundament pod szersze zrozumienie oraz efektywniejsze stosowanie pozostałych norm z rodziny 27000), ISO/IEC 27001 (stanowi kanon dotyczący wymagań dla systemów zarządzania bezpieczeństwem informacji, umożliwiając organizacjom zabezpieczenie informacji pod kątem ich poufności, integralności oraz dostępności przez implementację adekwatnych procedur zarządczych), ISO/IEC 27002 (oferuje referencyjny zbiór praktyk dla organizacji dążących do identyfikacji, wdrażania, utrzymania oraz doskonalenia swoich mechanizmów ochrony informacji w kontekście SZBI), ISO/IEC 27004 (dostarcza metodykę do monitorowania, przeglądu, oceny oraz doskonalenia efektywności systemu zarządzania bezpieczeństwem informacji, akcentując znaczenie mierzalnych wskaźników), ISO/IEC 27005 (zawiera wytyczne dotyczące zarządzania ryzykiem w kontekście bezpieczeństwa informacji, nakreślając proces identyfikacji, oceny oraz zarządzania ryzykiem informacyjnym), ISO/IEC 27006 (określa wymogi dla

organizacji świadczących usługi certyfikacji systemów zarządzania bezpieczeństwem informacji, wyznaczając ramy dla procesu audytu i certyfikacji), ISO/IEC 27013 (podaje wytyczne integrujące system zarządzania bezpieczeństwem informacji z systemem zarządzania usługami IT, promując koherentną i efektywną infrastrukturę zarządzania), ISO/IEC 27017 (koncentruje się na bezpieczeństwie informacji w chmurze, proponując kontrole oraz wytyczne dla dostawców i użytkowników usług przetwarzania w chmurze), ISO/IEC 27018 (ustanawia kodeks praktyk dla ochrony informacji osobowych w chmurze, zgodnie z wymaganiami prywatności i ochrony danych), ISO/IEC 22301 (specyfikuje wymogi dla systemów zarządzania ciągłością działania, umożliwiając organizacjom przygotowanie na incydenty zakłócające normalne funkcjonowanie), ISO/IEC 24762 (zawiera wytyczne dla usług odzyskiwania po awariach w centrach danych i innych środowiskach IT, podkreślając kluczowe elementy potrzebne do przywrócenia operacji IT po katastrofie, ISO/IEC 27036 (skupia się na zarządzaniu bezpieczeństwem informacji w relacjach między organizacjami, oferując wytyczne dotyczące bezpieczeństwa w outsourcingu i partnerstwach biznesowych), ISO/IEC 31000 (dostarcza wytyczne dotyczące zarządzania ryzykiem ogólnym, promując model zarządzania ryzykiem, który można dostosować do różnych typów organizacji i kontekstów), 13501-2 (norma ta przeprowadza proces kategoryzacji reakcji na ogień wyrobów używanych w budownictwie oraz elementów konstrukcyjnych budowli, określając ich parametry odporności na pożary i zachowanie w ekstremalnych warunkach termicznych), norma 1627 (stanowi kryteria odporne na nieautoryzowany dostęp przez systemy zamykające, jak okna, drzwi oraz osłony, hierarchizując je zgodnie z ich zdolnością do stawiania oporu przy próbach sforsowania), norma 12209-04 (wytycza wymagania techniczne oraz procedury badawcze dla mechanizmów blokujących w obszarze budowlanym, takich jak zamki mechaniczne wraz z ich komponentami, oceniając ich funkcjonalność oraz niezawodność.), norma 50131-1 (określa specyfikacje dla systemów alarmowych przeznaczonych do sygnalizacji prób włamania czy napadu, wyznaczając standardy dotyczące ich skuteczności oraz metodyki testowania).
- Omówienie znaczenia powyższych norm i ich w zapewnianiu wysokiego poziomu bezpieczeństwa informacji oraz praktycznego zastosowania w organizacjach.
- Inne standardy: Przedstawienie i dyskusja na temat innych standardów:

- ramy dotyczące zarządzania ryzykiem cyberbezpieczeństwa - NIST Cybersecurity Framework;
- ramy dotyczące wdrażania, rozwoju i doskonalenia polityki IT – COBIT;
- zbiór praktyk dotyczący zarządzania usługami IT – ITIL;
- akceptowalna polityka szyfrowania SANS;
- techniki kryptograficzne - ENISA ;
- ramy ochrony informacji i zasobów federalnych agencji rządowych USA - 800-53 rev3.

- Rola powyższych zagranicznych standardów w kształtowaniu efektywnych polityk bezpieczeństwa w organizacjach.

3. Omówienie zaawansowanych strategii ochrony organizacji:

- Zarządzanie ryzykiem: Metody identyfikacji, oceny, mitygacji i monitorowania ryzyka cybernetycznego. Wykorzystanie narzędzi i technologii do analizy ryzyka.
- Szczegółowy opis i kroki zarządzania incydentami:

- wykrywanie: inicjacja procesu inicjującego, mającego na celu detekcję niestandardowych aktywności lub zdarzeń infrastrukturalnych, które mogą sygnalizować potencjalne zagrożenia w obszarze cybernetycznym;
- rejestrowanie: operacja dokumentacyjna, polegająca na chronologicznym zapisie zaobserwowanych dysfunkcji w dedykowanych bazach danych, by zapewnić dokumentację dowodową dla późniejszych faz postępowania;
- analizowanie: metodyczne badanie zgromadzonych artefaktów zdarzeń w celu zrozumienia ich genezy, dynamiki oraz wpływu na ekosystem informacyjny;

- klasyfikowanie: systematyzacja incydentów według ustalonego kodu klasyfikacyjnego, uwzględniająca ich naturę, zasięg oraz potencjalne konsekwencje dla organizacji.
- priorytetyzowanie: alokacja zasobów reakcyjnych na bazie oceny krytyczności, która koresponduje z możliwymi konsekwencjami incydentu dla misji instytucji;
- podejmowanie działań naprawczych: inicjowanie interwencji korygujących mających na celu restytucję funkcji systemowych i prewencję przed podobnymi naruszeniami w przyszłości;
- ograniczanie skutków incydentu: implementacja taktyk zaradczych, które mają za zadanie minimalizację negatywnych rezultatów incydentu oraz odbudowę stanu równowagi operacyjnej.

- Priorytetyzacja incydentów na 3 kategorie: krytyczny, wysoki, średni na podstawie poniższych opisów:
  - **Priorytet krytyczny** - Incydent wymaga niezwłocznego działania oraz zgłoszenia do właściwego CSIRT. Procesy wewnętrzne są sparaliżowane lub zakłócone w znaczącym stopniu. Istnieje wysokie ryzyko wycieku danych (np. danych osobowych) oraz utraty poufności, integralności i/lub dostępności informacji.
  - **Priorytet wysoki** - Incydent wymaga szybkiego działania oraz zgłoszenia do właściwego CSIRT w ciągu 24 godzin. Procesy wewnętrzne są częściowo zakłócone lub sparaliżowane. Istnieje niskie ryzyko wycieku danych (np. danych osobowych) oraz utraty poufności, integralności i/lub dostępności informacji.
  - **Priorytet średni** - Incydent prawdopodobnie nie wymaga niezwłocznego działania oraz zgłoszenia do właściwego CSIRT ze względu na brak symptomów działania z zewnątrz. Procesy wewnętrzne nie są sparaliżowane lub zakłócone w żadnym stopniu. Ryzyko wycieku danych (np. danych osobowych) oraz utraty poufności, integralności i/lub dostępności informacji nie występuje.

- Budowanie zespołów ds. bezpieczeństwa: Definicja ról, odpowiedzialności, umiejętności oraz ścieżek rozwoju dla członków zespołu bezpieczeństwa.
- Lista wymaganych kompetencji do omówienia na szkoleniu:
  - Szef działu bezpieczeństwa (kierownik, dyrektor);
  - Pełnomocnik ds. Bezpieczeństwa Informacji;
  - Specjalista ds. Zarządzania Ryzykiem;
  - Specjalista ds. Zgodności;
  - Specjalista ds. Bezpieczeństwa Fizycznego;
  - Architekt Systemów Bezpieczeństwa;
  - Koordynator Programu Bezpieczeństwa;
  - Analityk Bezpieczeństwa (II linia wsparcia);
  - Inżynier ds. Bezpieczeństwa (II linia wsparcia);
  - Administrator Systemów Bezpieczeństwa (II linia wsparcia);

4. Regulacje prawne i compliance:

- Zharmonizowanie działalności Podmiotu z imperatywami Ustawy o Krajowym Systemie Cyberbezpieczeństwa, z naciskiem na implementację procedur i protokołów zapewniających wytrzymałość infrastruktury informatycznej na potencjalne zagrożenia cyfrowe.
- Inicjacja, adaptacja, perpetuacja oraz ewolucja Systemu Zarządzania Bezpieczeństwem Informacji, skonstruowanego na fundamencie czterech norm określonych w paragrafie 20 Krajowego Ramienia Interoperacyjności, stanowiących kamień węgielny dla ochrony danych.
- Egzekwowanie procedury tworzenia redundancji danych dziennikowych poprzez generowanie kopii zapasowych, które będą przechowywane przez okres minimalny dwóch lat, zgodnie z dyrektywą zawartą w paragrafie 21 Krajowego Ramienia Interoperacyjności.

- Implementacja kompleksowej agregacji logów (rejestrowanych zdarzeń) pochodzących z heterogenicznej gamy urządzeń, maszyn i aplikacji działających w ramach infrastruktury teleinformatycznej Podmiotu, umożliwiająca szczegółową analizę i audyt bezpieczeństwa.
- Integracja z zaawansowanym systemem zarządzania cyberbezpieczeństwem S46 (S46-react), celem optymalizacji procesów detekcji, reagowania i prewencji w zakresie incydentów bezpieczeństwa cyfrowego.
- Kodyfikacja programu regularnych audytów wewnętrznych i zewnętrznych, obejmujących spektrum standardów i regulacji (KRI, KSC, ISO, RODO).
- Monitorowanie zdarzeń systemowych w trybie ciągłym, poprzez wykorzystanie mechanizmów korelacji zdarzeń, umożliwiających identyfikację i interpretację wzorców aktywności sugerujących potencjalne scenariusze ataków cybernetycznych.
- Dostosowanie się do rozszerzonego zakresu wymagań wynikających z implementacji Dyrektywy NIS2, która wprowadza nowe, zaostrzone standardy w zakresie cyberbezpieczeństwa, wymagające od organizacji ponownej oceny i ulepszenia istniejących strategii ochrony danych.
- Wyznaczenie dedykowanego Pełnomocnika ds. Systemu Zarządzania Bezpieczeństwem Informacji, którego rola nie będzie interferować ani generować konfliktów interesów z innymi kluczowymi funkcjami w organizacji (np. Inspektorem Ochrony Danych, Informatykiem, Dyrektorem).
- Rekonfiguracja systemów informatycznych oraz protokołów pracy zdalnej w zgodzie ze zmienionymi standardami bezpieczeństwa, uwzględniającymi nowelizację Kodeksu Pracy, w celu zabezpieczenia integralności danych korporacyjnych w rozproszonym środowisku pracy.
- Realizacja oczekiwań organów nadzorczych w kontekście konstruowania oraz utrzymywania zaawansowanych systemów cyberbezpieczeństwa, zdolnych do przeciwdziałania współczesnym zagrożeniom w przestrzeni cyfrowej.
- Implementacja rygorystycznych protokołów ochrony danych osobowych, mających na celu eliminację ryzyka wycieków informacji, spowodowanych przez nieświadome bądź intencjonalne działania personelu organizacji.
- Automatyzacja procesów aktualizacji oprogramowania w celu zapewnienia najwyższego poziom

5. Zarządzanie bezpieczeństwem w praktyce:

- Zrozumienie znaczenia typów licencji względem konieczności ich testowania:

- Licencje niewyłączne, w których udzielający licencji może zezwolić na korzystanie z utworu wielu osobom równocześnie, które nie muszą mieć formy pisemnej.
- Licencje wyłączne, spotykane głównie w przypadku oprogramowania pisanego na zamówienie (np. strona www), w tym przypadku zwykle umowa licencyjna wynika z umowy o dzieło, na podstawie której firma wykonująca oprogramowanie wykonuje zamówioną aplikację, umowa taka wymaga formy pisemnej pod rygorem nieważności.
- Sublicencja, w której licencjobiorca może udzielić dalszej licencji, pod warunkiem wszakże takiego upoważnienia w jego umowie licencyjnej.
- OEM, to programy sprzedawane wraz ze sprzętem komputerowym (przypisane do konkretnego komputera), po wymianie sprzętu na nowszy, nie można ich przenieść na nowy komputer tylko trzeba ponownie je zakupić.
- BOX, to programy, które można przenosić na kolejne komputery jednak pod warunkiem, że zawsze zainstalowany jest tylko na jednym komputerze. Legalny jest tylko program ostatnio zainstalowany.
- Open Source (otwarte oprogramowanie) to alternatywa dla Freeware (wolne oprogramowanie), którego celem jest istnienie swobodnego dostępu do oprogramowania dla wszystkich jego uczestników. Zapewnia swoim użytkownikom prawo do legalnego oraz darmowe.

Z przeprowadzonego szkolenia Wykonawca musi przedstawić **listę obecności** z podpisami uczestników szkolenia oraz program szkolenia. Każdy uczestnik szkolenia otrzyma od Wykonawcy imienny certyfikat potwierdzający ukończenie szkolenia.

Szkolenie musi być zakończone ankietą **oceniającą szkolenie**, jego przydatność, zakres przekazanych informacji, adekwatności przekazanych informacji do potrzeb uczestnika, formy prezentacji i komunikatywności prowadzącego szkolenie.

INFORMACJE OGÓLNE DO SZKOLEŃ

1. Wykonawca zobowiązuje się do odpowiedniego oznaczenia wszystkich miejsc i dokumentów bezpośrednio związanych z realizacją przedmiotu umowy, zgodnie z „Podręcznikiem wnioskodawcy i beneficjenta programów polityki spójności 2021-2027 w zakresie informacji i promocji".
2. Wykonawca zobowiązuje się do realizacji przedmiotu zamówienia zgodnie z zasadami horyzontalnymi, to jest: zasadą równości szans i niedyskryminacji, konwencją o prawach osób niepełnosprawnych, zasadą równości kobiet i mężczyzn, zasadą zrównoważonego rozwoju, w tym DNSH (zasada "nie czyń poważnych szkód"), Kartą praw podstawowych Unii Europejskiej, zgodnie z określonymi Wytycznymi, w szczególności Wytycznymi dotyczącymi realizacji zasad równościowych w ramach funduszy unijnych na lata 2021-2027 oraz Wytycznych w zakresie w realizacji zasady równości szans i niedyskryminacji, w tym dostępności dla osób z niepełnosprawnościami i zasady równości szans kobiet i mężczyzn w ramach funduszy unijnych na lata 2021-2027.
3. Podczas realizacji przedmiotu zamówienia Wykonawca podejmie odpowiednie kroki w celu zapobiegania wszelkiej dyskryminacji ze względu na płeć, rasę lub pochodzenie etniczne, religię lub światopogląd, niepełnosprawność, wiek lub orientację seksualną. W procesie przygotowywania i realizacji szkoleń należy w szczególności wziąć pod uwagę zapewnienie dostępności dla osób z niepełnosprawnościami.
4. W przypadku szkoleń online, e-learningu (dostęp do platformy szkoleniowej) wymagane będzie spełnienie przez wykonawcę wymogów dostępności oraz WCAG 2.1 dla narzędzi/platform które zostaną wykorzystane do szkoleń. W sytuacji kiedy szkolenia będą prowadzone w formie stacjonarnej wykonawca będzie musiał zapewnić materiał szkoleniowy z większym rozmiarem czcionki (w zależności od potrzeb uczestników szkolenia). W ramach grup szkoleniowych przewidziana jest równa dostępność dla kobiet i mężczyzn oraz osób niepełnosprawnych. Opracowane dokumentacje będą musiały być dostarczone w formie papierowej i elektronicznej z możliwością powiększania treści.
   Wykonawca zamówienia będzie zobowiązany do podpisania oświadczenia potwierdzającego przestrzeganie powyższych zasad.

<u>Warunki płatności:</u>

1. Płatność wynagrodzenia będzie dokonywana w transzach:

a) za udostępnienie platformy online, po każdym cyklu szkolenia.
b) za przeszkolenie kadry zarządzającej do dnia 30.06.2025 r. (szkolenie stacjonarnie – planowane na dzień 20.03.2025 r.)

na podstawie prawidłowo sporządzonych faktur VAT/rachunków, wystawionej po wykonaniu części zamówienia, płatne w terminie do 14 dni od dnia wpływu do Zmawiającego, z załączeniem protokołu częściowego i protokołem końcowym.

2. Wykonawca oświadcza, że wynagrodzenie obejmuje wszelkie koszty niezbędne do prawidłowego wykonania przedmiotu umowy.

II. WARUNKI UDZIAŁU W POSTĘPOWANIU

1. Wykonawca powinien spełniać warunek dotyczący zdolności technicznej lub zawodowej, jeżeli wykaże, że

a) dysponuje lub będzie dysponował następującą /-cymi osobą /-ami skierowanymi przez Wykonawcę do realizacji zamówienia publicznego, która/-e posiadają stosowną wiedzę popartą certyfikatami lub równoważnym dokumentami oraz m.in. 2 letnie doświadczenie w przygotowaniu i przeprowadzeniu szkoleń budujących i wzmacniających świadomość cyberzagrożeń.

b) Wykonawca, który przeprowadza szkolenie posiada stosowną wiedzę popartą certyfikatami lub równoważnymi dokumentami, m.in. 2 letnie doświadczenie we wnioskowanym zakresie i szkolenie jest dedykowane JST

2. posiada certyfikat ISO 9001 w zakresie świadczenia usług.

W celu weryfikacji ww. warunków, określonych w pkt 1, należy złożyć stosowne oświadczenie – załącznik nr 3, załącznik nr 4, a także załączyć stosowne kserokopie certyfikatów lub równoważne poświadczenia (np. Kwalifikację zawodową).

Wykonawcy, którzy nie wykażą spełnienia warunków udziału w postępowaniu podlegać będą wykluczeniu z udziału w postępowaniu.

III. INFORMACJA NA TEMAT ZAKRESU WYKLUCZENIA

1. O udzielenie zamówienia nie może ubiegać się Wykonawca:

1) jeżeli w stosunku do niego zachodzi którakolwiek z okoliczności, o których mowa w art. 7 ust. 1 ustawy 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 2024 r. poz. 507).

2) który jest powiązany z Beneficjentem lub osobami upoważnionymi do zaciągania zobowiązań w imieniu Beneficjenta lub osobami wykonującymi w imieniu Beneficjenta czynności związane z przygotowaniem i przeprowadzeniem procedury wyboru wykonawcy osobowo lub kapitałowo, polegających na:

a) 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,

b) 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, jego zastępcą prawnym lub członkami organów zarządzających lub organów nadzorczych Beneficjenta udzielającego zamówienie,

c) pozostawaniu z Beneficjentem w takim stosunku prawnym lub faktycznym, że istnieje uzasadniona wątpliwość co do ich bezstronności lub niezależności w związku z postępowaniem o udzielenie zamówienia.

2. W celu potwierdzenia braku podstaw do wykluczenia Wykonawcy wskazanych w ust. 1 pkt 1 i 2, Wykonawca zobowiązany jest złożyć wraz z ofertą oświadczenia, zgodne ze wzorami oświadczeń, stanowiących Załącznik nr 2 do Zapytania ofertowego.

3. Zamawiający wykluczy Wykonawcę z postępowania o udzielenie zamówienia, w stosunku do którego zachodzi którakolwiek z okoliczności, o których mowa w ust. 1 pkt 1 lub pkt 2.

4. Do udziału w postępowaniu dopuszczeni zostaną Wykonawcy, którzy spełnią wszystkie warunki udziału w postępowaniu. Ocena spełnienia warunków odbywać się będzie na zasadzie „spełnia/nie spełnia".

IV. TERMIN WYKONANIA ZAMÓWIENIA

Dostęp do platformy szkoleniowej dla pracowników Starostwa: od dnia podpisania umowy do dnia 30.06.2025 r.

1 cykl : Otrzymanie dostępu do platformy w ciągu 30 dni od podpisania umowy.
2 cykl : Otrzymanie dostępu do platformy w ciągu 90 dni od podpisania umowy.

Okres udostępnienia platformy – 2x 1 m-c

Szkolenie dla Kadry Zarządzającej Starostwa:
Planowany termin szkolenia stacjonarnego na dzień 20.03.2025 r.

Zamawiający zastrzega sobie prawo do zmiany terminu szkolenia, o czym Wykonawca zostanie poinformowany z 5-dniowym wyprzedzeniem.

UWAGA! Harmonogram wsparcia zostanie ustalony pomiędzy Zamawiającym a Wykonawcą po podpisaniu umowy.

V. KRYTERIUM WYBORU OFERTY

1. Przy wyborze najkorzystniejszej oferty Zamawiający będzie się kierował następującymi kryteriami oceny ofert

1) Kryterium 1 (K1) Cena oferty brutto – 60 %
2) Kryterium 2 (K2) Doświadczenie osoby wyznaczonej do przeprowadzenia przedmiotu zamówienia - 40%

2. Sposób oceny ofert w poszczególnych kryteriach:

1) Kryterium oceny ofert - cena oferty brutto – 60%

$$K = \frac{\text{Cena minimalna (najniższa spośród złożonych ofert)}}{\text{Cena przedstawiona w ofercie}} \times 60$$

a) Podstawą przyznania punktów w kryterium „cena" będzie cena ofertowa brutto podana przez Wykonawcę w Formularzu Ofertowym.
b) Cena ofertowa brutto musi uwzględniać wszelkie koszty jakie Wykonawca poniesie w związku z realizacją przedmiotu zamówienia.

2) Kryterium Doświadczenie osoby wyznaczonej do przeprowadzenia przedmiotu zamówienia – 40% = max. 40 pkt

K2= Liczba punktów uzyskanych przez osobę/-y wyznaczoną/-e do wykonania przedmiotu zamówienia zgodnie z poniższą skalą (max. 40 punktów)

a) posiadane m.in. 2 letnie doświadczenie w przygotowaniu i przeprowadzeniu szkoleń budujących i wzmacniających świadomość cyberzagrożeń – 0 pkt.

b) posiadane doświadczenie od 2 lat do łącznie 2 lat i 6 miesięcy doświadczenia w przygotowaniu i przeprowadzeniu szkoleń budujących i wzmacniających świadomość cyberzagrożeń – 10 pkt.
c) posiadane od 2 lat i 7 miesięcy do łącznie 3 lat doświadczenia w przygotowaniu i przeprowadzeniu szkoleń budujących i wzmacniających świadomość cyberzagrożeń – 20 pkt.
d) posiadane od 3 lat do łącznie 3 lat i 6 miesięcy doświadczenia w przygotowaniu i przeprowadzeniu szkoleń budujących i wzmacniających świadomość cyberzagrożeń – 30 pkt.
e) posiadane powyżej 3 lat i 7 miesięcy doświadczenia w przygotowaniu i przeprowadzeniu szkoleń budujących i wzmacniających świadomość cyberzagrożeń – 40 pkt.

Do oferty należy dołączyć dokumenty potwierdzające posiadane doświadczenie.
Ocena ogólna poszczególnych ofert dokonywana będzie w oparciu o poniższy wzór:
O=K1+K2
gdzie:
O – oznacza łączną ocenę, jako sumę punktów w poszczególnych kryteriach
K1 – liczba punktów uzyskanych w kryterium „cena"
K2 – liczba punktów uzyskana w kryterium „doświadczenie osoby wyznaczonej do przeprowadzenia przedmiotu zamówienia"

UWAGA: Wykonawca może posługiwać się przy realizacji zamówienia większą liczbą osób zdolnych do wykonania zamówienia. Punkty za powyższe kryterium „Doświadczenie osoby wyznaczonej do przeprowadzenia przedmiotu zamówienia" zostaną przyznane w skali 0-40 punktowej

3. Oferty złożone w odpowiedzi na niniejsze zamówienie ocenione będą w oparciu o ww. kryteria z dokładnością do dwóch miejsc po przecinku.
4. Oferty oceniane będą punktowo. Maksymalna liczba punktów, jaką może uzyskać oferta wynosi 100,00 pkt.
5. Oferta, która otrzyma największą, łączną ilość punktów uznana zostanie za najkorzystniejszą.
6. Jeżeli nie będzie można dokonać wyboru najkorzystniejszej oferty z uwagi na to, że zostały złożone oferty o takiej samej cenie, Zamawiający wezwie Wykonawców, którzy złożyli te oferty, do złożenia w terminie określonym przez Zamawiającego ofert dodatkowych zawierających nową cenę.
7. Zamawiający udzieli zamówienia Wykonawcy, którego oferta zostanie uznana za najkorzystniejszą.

VI. OPIS SPOSOBU PRZYGOTOWANIA OFERTY

1. Oferta powinna zostać przygotowana i złożona Zamawiającemu na Formularzu Ofertowym, stanowiącym załącznik nr 1 niniejszego zapytania.
2. Oferta musi zawierać wszystkie niezbędne formularze i dokumenty wymagane przez Zamawiającego.
3. Jeżeli oferta i załączniki zostaną podpisane przez upoważnionego przedstawiciela, Oferent jest zobowiązany do przedłożenia w załączeniu do oferty właściwego pełnomocnictwa lub umocowania prawnego.
4. Oferta musi być sporządzona w języku polskim, w formie zapewniającej pełną czytelność jej treści.
5. Każdy Wykonawca może złożyć tylko jedną ofertę.
6. Jeżeli do oferty Wykonawca nie złoży wymaganych oświadczeń i dokumentów co uniemożliwiłoby wybranie oferty złożonej przez Wykonawcę, Zamawiający może wezwać Wykonawcę do uzupełnienia lub wyjaśnienia.
7. Zamawiający nie dopuszcza możliwości składania ofert częściowych ani wariantowych. Oferty częściowe i wariantowe nie będą brane pod uwagę.
8. Oferta jest jawna, z wyjątkiem informacji stanowiących tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji, a Wykonawca składając ofertę zastrzegł

w odniesieniu do tych informacji, że nie mogą one być udostępnione przez innym uczestnikom postępowania.
9. Złożona oferta wiąże Wykonawcę przez 30 dni od dnia upływu terminu składania ofert.
10. Wykonawca ponosi wszystkie koszty związane z przygotowaniem oferty.
11. Zamawiający zastrzega sobie prawo do zmiany warunków określonych w niniejszym Zapytaniu ofertowym.

VII. MIEJSCE, TERMIN I SPOSÓB SKŁADANIA OFERTY

1. Ofertę należy składać wyłącznie drogą elektroniczną za pośrednictwem aplikacji Baza Konkurencyjności (https://bazakonkurencyjnosci.funduszeeuropejskie.gov.pl/).
2. Termin składania ofert: 12.02.2025 r., do godz. 09:00
3. O terminie złożenia oferty decyduje data złożenia oferty za pomocą Bazy Konkurencyjności.
4. Otwarcie Ofert nastąpi w dniu 12.02. 2025 roku o godz.09:10

VIII. OFERTA ZOSTANIE ODRZUCONA, GDY:

1. Zawiera omyłki rachunkowe w obliczeniu ceny, których nie można poprawić na zasadzie oczywistych omyłek rachunkowych bądź błędów rachunkowych. Zamawiający odrzuci ofertę, jeżeli jej treść nie odpowiada treści niniejszego zapytania ofertowego.
2. Została złożona po wyznaczonym terminie lub/i niewłaściwej formie.
3. Została złożona przez Wykonawcę wykluczonego.

IX. UNIEWAŻNIENIE POSTĘPOWANIA

Zamawiający zastrzega sobie prawo unieważnienia postępowania w przypadku wystąpienia okoliczności nie dających się przewidzieć, a mających wpływ na prowadzone postępowanie, na każdym etapie bez podania przyczyny. Zamawiający unieważni postępowanie w całości lub w części, jeżeli:
1. Nie złożono żadnej oferty niepodlegającej odrzuceniu,
2. Cena najkorzystniejszej oferty przewyższy kwotę, którą Zamawiający zamierza przeznaczyć na sfinansowanie zamówienia.
3. Wystąpiła istotna zmiana okoliczności powodująca, że prowadzenie postepowania lub wykonanie zamówienia nie leży w interesie publicznym, czego nie można było wcześniej przewidzieć.
4. Postępowanie obarczone jest niemożliwą do usunięcia wadą uniemożliwiającą zawarcie niepodlegającej unieważnieniu umowy w sprawie zamówienia publicznego.
5. W wyniku dogrywki zostały złożone oferty dodatkowe, o takim samym bilansie ceny lub kosztu.

W przypadku zaistnienia powyższych okoliczności, Wykonawcom nie przysługują żadne roszczenia w stosunku do Zamawiającego.

X. KOMUNIKACJA POMIĘDZY ZAMAWIAJĄCYM, A WYKONAWCĄ

1. Wszelka komunikacja w postępowaniu o udzielenie zamówienia, w tym ogłoszenie zapytania ofertowego, składanie ofert, wymiana informacji między zamawiającym a wykonawcami oraz przekazywanie dokumentów i oświadczeń odbywa się za pomocą aplikacji Baza Konkurencyjności(BK2021).
2. Ewentualne pytania dotyczące przedmiotu niniejszego zapytania ofertowego należy składać za pośrednictwem Bazy Konkurencyjności: (https://bazakonkurencyjnosci.funduszeeuropejskie.gov.pl)

3. Zamawiający i Wykonawca będą komunikować się za pomocą ww. aplikacji – komunikacja za pośrednictwem BK2021 jest obowiązkowa od momentu opublikowania postępowania do upływu terminu składania ofert (np. wyjaśnienie treści ogłoszenia). Po upływie terminu składania ofert, komunikacja między Zamawiający a Wykonawcą za pośrednictwem BK2021 nie jest wymagana. Na tym etapie można się kontaktować z Wykonawcą np. za pomocą danych kontaktowych dostępnych w sekcji „Osoby do kontaktu "w ogłoszeniu.

XI. INFORMACJA O WYNIKACH POSTĘPOWANIA

Zamawiający niezwłocznie zawiadomi wszystkich Wykonawców, którzy złożyli oferty o:
1. Wyborze najkorzystniejszej oferty,
2. Wykonawcach, których oferty zostały odrzucone
3. Unieważnieniu postępowania.

Informacja o wynikach postępowania Zamawiający zamieści w aplikacji Baza Konkurencyjności.

XII. DODATKOWE INFORMACJE

1. Planowany termin zawarcia umowy: luty 2025 r. wg wzoru – załącznik nr 5 do zapytania ofertowego.
2. Istotne postanowienia umowne, w tym w szczególności zapisy dotyczące warunków płatności, kar umownych innych warunków realizacji niniejszego zamówienia, określone zostały w załączniku nr 5 do zapytania ofertowego – Projekt Umowy.
3. Zamawiający dopuszcza możliwość zmiany umowy w zakresie i na zasadach ustalonych w załączniku nr 5 do zapytania ofertowego – Projekt Umowy.
4. Jeżeli Wykonawca, którego oferta została wybrana uchyla się od zawarcia umowy, Zamawiający może wybrać kolejną ofertę, najkorzystniejszą spośród pozostałych ofert.
5. Zamawiający oceni i porówna jedynie te oferty, które odpowiadają zasadom określonym w zapytaniu.
6. Jeżeli Zamawiający otrzyma oferty, w których zaoferowane ceny przewyższają kwotę, którą Zamawiający zamierza przeznaczyć na realizacje zamówienia, nie przewiduje się prowadzenie negocjacji z Wykonawcą, którego oferta została wybrana, jako najkorzystniejsza (otrzymał najwyższą ilość punktów).
7. W toku badania i oceny ofert Zamawiający zastrzega sobie prawo do wezwania Wykonawcy do korekty błędów lub wyjaśnień treści złożonych ofert. W powyższym celu Zamawiający wyznaczy zakres wymaganych korekt i wyjaśnień oraz odpowiedni termin na ich dokonanie. Niedotrzymanie tego terminu będzie skutkować odrzuceniem oferty i wykluczeniem z postępowania.
8. 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 wezwie Wykonawcę złożenia w wyznaczonym terminie wyjaśnień, w tym złożenia dowodów w zakresie wyliczenia ceny lub kosztu. Zamawiający oceni złożone wyjaśnienia w konsultacji z Wykonawcą i może odrzucić ofertę wyłącznie w przypadku, gdy złożone wyjaśnienia wraz z dowodami nie uzasadniają podanej ceny lub kosztu w tej ofercie.
9. Zamawiający zastrzega sobie prawo do zmiany warunków określonych w niniejszym Zapytaniu ofertowym lub unieważnieniu niniejszego postępowania na każdym etapie postępowania bez podania przyczyny.

XIII. RODO

1. Administratorem Państwa danych osobowych jest Starostwo Powiatowe w Lęborku reprezentowane przez Starostę Lęborskiego z siedzibą w Lęborku, 84-300, ul. Czołgistów 5.
2. Nadzór nad prawidłowym przetwarzaniem danych osobowych w Starostwie Powiatowym w Lęborku sprawuje Inspektor Ochrony Danych: Marek Czechowski - e-mail: iodo@starostwolebork.pl lub korespondencyjnie na adres Administratora Danych Osobowych.
3. Państwa dane osobowe są przetwarzane w formie papierowej oraz elektronicznej.
4. Państwa dane osobowe zostały pozyskane w związku z zawarciem lub zamiarem zawarcia umowy z Administratorem i zostały pozyskane bezpośrednio od Państwa albo zostały podane przez Państwa pracodawcę/zleceniodawcę w związku z wykonywanymi obowiązkami wynikającymi ze stosunku pracy/umowy cywilnoprawnej.
5. Administrator będzie przetwarzał Państwa dane osobowe, które są niezbędne do realizacji niżej wymienionych celów, jakimi mogą być:
a. Przeprowadzenie postępowania o udzielenie zamówienia publicznego na podstawie art. art. 6 ust. 1 lit. c RODO
b. spełnienia obowiązków prawnych Zleceniodawcy/Zamawiającego wynikających z właściwych przepisów prawa na podstawie art. 6 ust. 1 lit c) i art. 9 ust. 2 lit. b) RODO;
c. spełnienie obowiązków prawnych wynikających z właściwych przepisów prawa np. wydawanie upoważnień lub zachowanie potwierdzenia spełnienia obowiązku informacyjnego na podstawie art. 6 ust. 1 lit. c) RODO;
d. ustalenie, dochodzenie lub obrona roszczeń na podstawie art. 6 ust. 1 lit. f) RODO prawnie uzasadniony interes administratora, dochodzenie i obrona roszczeń w stosunku do Państwa lub podmiotów zewnętrznych;
e. zawarcie i wykonanie umowy na podstawie art. 6 ust. 1 lit. b) RODO;
f. zapewnienie bezpieczeństwa osób i mienia poprzez monitoring wizyjny na podstawie art. 6 ust. 1 lit. f) RODO;
g. spełnienie obowiązku prawnego związanego z możliwością nadania uprawnienia dostępu do informacji niejawnych na podstawie art. 6 ust. 1 lit. c) RODO ;
h. spełnienie obowiązków podatkowych oraz rachunkowości na podstawie art. 6 ust. 1 lit. c) RODO;
i. spełnienie obowiązków BHP na podstawie art. 6 ust. 1 lit. c) RODO.
j. bieżąca komunikacja wewnątrz i na zewnątrz Starostwa Powiatowego na podstawie art. 6 ust. 1 lit. f) RODO – prawnie uzasadniony interes Administratora w postaci kontaktowania się z Państwem oraz Państwa z innymi osobami w ramach wykonywania obowiązków służbowych – dane będą przechowywane do czasu ustania potrzeby kontaktu.
6. Państwa dane osobowe będą przechowywane przez okres wynikający z przepisów prawa nakładających na Administratora obowiązek przechowywania danych na potrzeby archiwizacji, podatkowe, księgowe, BHP, wynikające z przepisów bezwzględnie obowiązującego prawa w tym prawa pracy, a także z uwagi na przedawnienie roszczeń w stosunku do Administratora.
7. Państwa dane osobowe mogą być udostępniane właściwym organom uprawnionym na podstawie przepisów prawa oraz w ramach udzielania informacji publicznej w przypadku Państwa udziału w zamówieniach publicznych, a także podmiotom, z którymi Administrator zawarł umowę powierzenia przetwarzania danych osobowych w związku z realizacją usług na rzecz Administratora, w zakresie swoich obowiązków służbowych, na podstawie upoważnienia, np. kancelarii prawnej, dostawcom oprogramowania, zewnętrznym audytorom, zleceniobiorcom świadczącym usługi związane z przetwarzaniem danych osobowych, a także bankom, kurierom, podmiotowi świadczącemu usługi pocztowe, ubezpieczycielom.
8. Państwa dane osobowe nie będą przekazywane do państwa trzeciego ani do organizacji międzynarodowej.

9. Państwa dane osobowe nie będą przetwarzane w sposób zautomatyzowany.
10. Posiadają Państwo prawo dostępu do treści swoich danych osobowych oraz prawo do ich sprostowania, usunięcia lub ograniczenia przetwarzania, a także prawo do wniesienia sprzeciwu wobec ich przetwarzania, a także prawo do przenoszenia danych – w przypadkach i na zasadach określonych w przepisach RODO.
11. Posiadają Państwo prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych z siedzibą w Warszawie (00–193) przy ul. Stawki 2, gdy uznają Państwo, że przetwarzanie ich danych osobowych narusza obowiązujące przepisy prawa.
12. Podanie danych osobowych jest wymogiem umownym, a konsekwencją ich nie podania będzie brak możliwości zrealizowania współpracy z Administratorem.

XIV. WYKAZ ZAŁĄCZNIKÓW DO NINIEJSZEGO OGŁOSZENIA

1. Formularz ofertowy - załącznik nr 1
2. Oświadczenie o braku podstaw do wykluczenia - załącznik nr 2
3. Oświadczenie o posiadanym doświadczeniu – załącznik nr 3
4. Wykaz usług - załącznik nr 4
5. Wzór/projekt umowy – załącznik nr 5

28.01.25 STAROSTA Tomasz Litwin

(data i podpis Starosty lub innej osoby upoważnionej)